Geevarghese Cheria

[Geevarghese Cheria](https://community.cisco.com/t5/user/viewprofilepage/user-id/292721) Cisco Employee

Cisco Employee

[Options](https://community.cisco.com/t5/security-knowledge-base/connect-and-secure-with-meraki/ta-p/4722928)

on ‎11-16-2022 08:37 PM

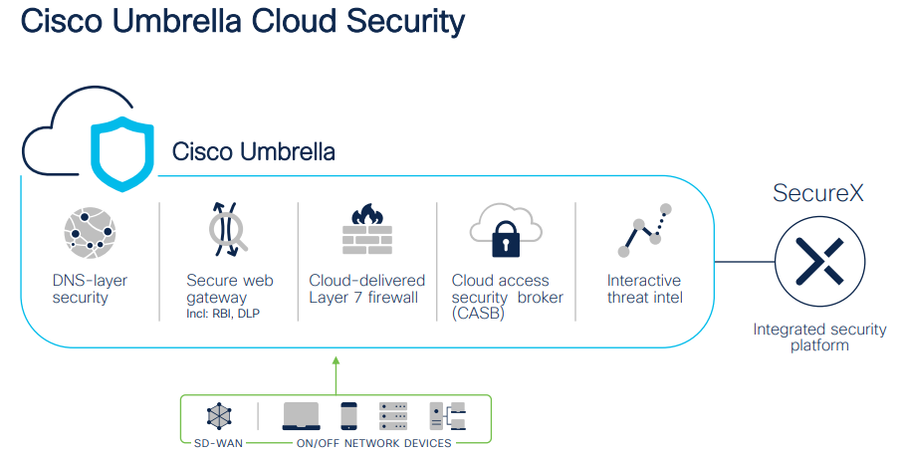
In today’s world, employees work from anywhere around the world and are using an ever-increasing number of applications that are moving to the cloud. Many businesses cannot afford to run networks that were not built for these new digital demands. Cisco Meraki equips IT organizations of any size with the capabilities to securely connect users and applications anywhere. In this article we will have a quick walk-through on the following topics:

* SASE – Secure Access Service Edge – Its basically the convergence of your network as a service along with security into a unified converged cloud platform.
* • Meraki Umbrella SD-WAN Connector
* • Cisco+ Secure Connect Now

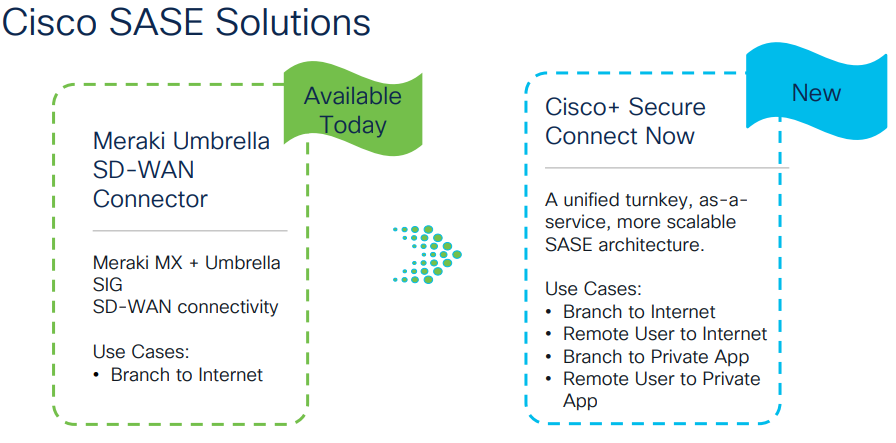
Applications are hyper-distributed across a diverse IT landscape. IDG Communications’ 2022 State of the CIO research report highlights the shift in IT priorities and the increasing involvement of CIOs in ensuring cybersecurity and increasing operational efficiency. The report captures inputs from IT leaders and line of business (LOB) participants who confirm the shift in IT priorities. Eighty five percent of CIOs say it’s important to maintain security, control, and governance across user devices, networks, clouds, and applications. Sixty nine percent of CIOs believe insights will be more important than ever to deliver a seamless consumer experience.

[Source: <https://wire19.com/84-cios-now-focusing-on-functional-activities/>]

Gartner MQ report for WAN Edge Infrastructure, Sep-2021 states that Cisco has a strong vision to deliver a fully integrated SASE solution, as well as the financial resources to execute the vision. For the Cisco on network part, we have MERAKI, the most trusted & simplified cloud managed platform, which is born in the cloud, growing daily, and trusted everywhere. We also have Cisco Umbrella, which is a cloud-based Domain Name Service (DNS) Security Solution that offers a variety of internet gateway services. It’s the ‘first line of defense’ against internet-sourced threats such as malware, ransomware and phishing campaigns.



Now let’s see how Cisco Meraki and Cisco umbrella are converged together to form a SASE solution. The project was started with Meraki Umbrella SD-WAN connector for branch to access the Internet as a use case. Now Meraki has more use cases from the same connected security fabric that includes remote user to Internet, branch to private app, etc.



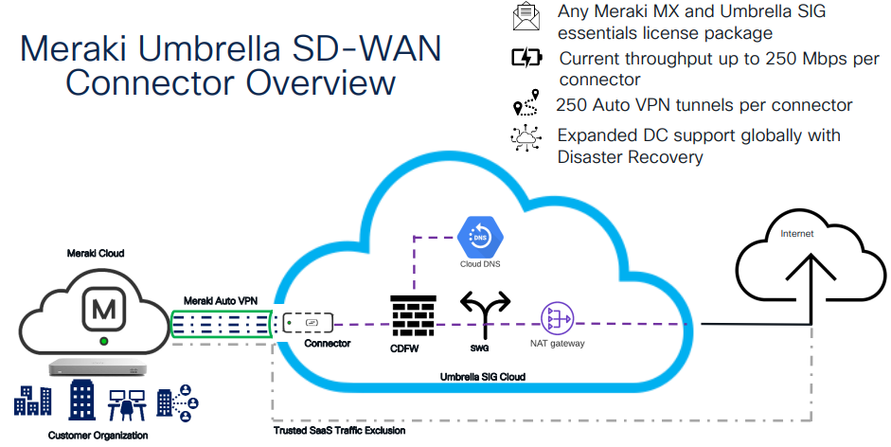
So, let’s start with Meraki Umbrella SD-WAN connector. This is possible with the help of the Meraki Auto VPN solution which is known for its intelligent path selection.



Auto VPN will set the entire network management through Meraki cloud, so that all features available with Meraki can be used for SD-WAN branch integration. Integrating Umbrella SIG (Secure Internet Gateway) with Meraki MX by connecting Meraki SD-WAN fabric to Umbrella cloud security services. It reduces the complexity in securing the network WAN edge. Umbrella's unified cloud platform simplifies managing and designing security policies for all sites within the Meraki SD-WAN fabric.



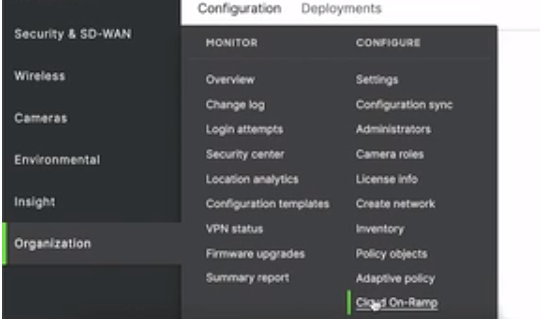
Let’s take a use case for a  chain of restaurants where credit card transactions need to be secured. In this scenario you need to first choose the data centers based on the geographical location to deploy the connectors. Then connect all the restaurants via Meraki Auto VPN to the connector. This deploys all the Secure Internet Gateway policies across all the sites.



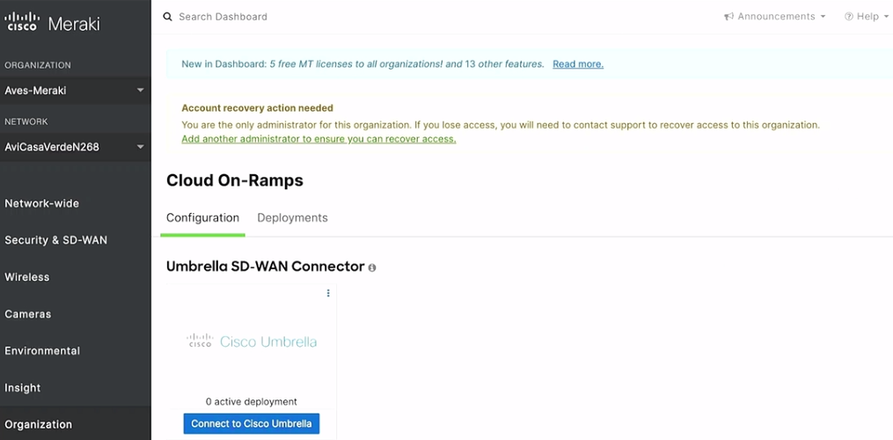
If you don’t want all the traffic tunneled via Secure Internet Gateway, then use Auto VPN’s other feature, known as trusted SaaS Traffic Exclusion. You can filter out the high bandwidth consuming traffic and exclude it. Per connector you have 250Mbps of throughput and can have 250 tunnels per connector.

**First lets checkout how to get connectivity to the cloud network from Meraki Dashboard.**

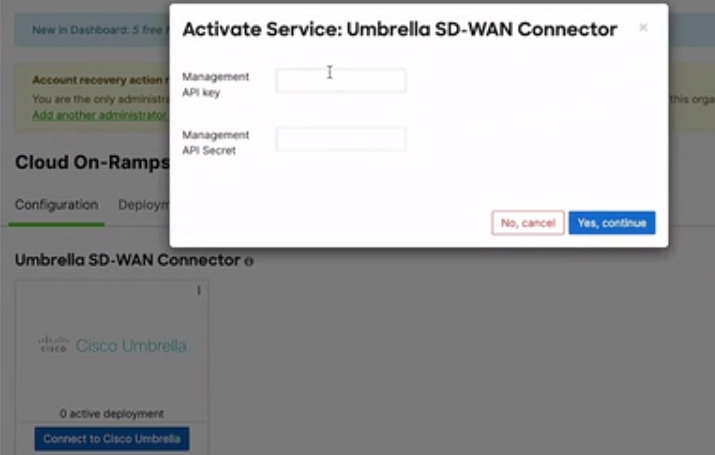
If we navigate to the organization -> Cloud On-Ramp



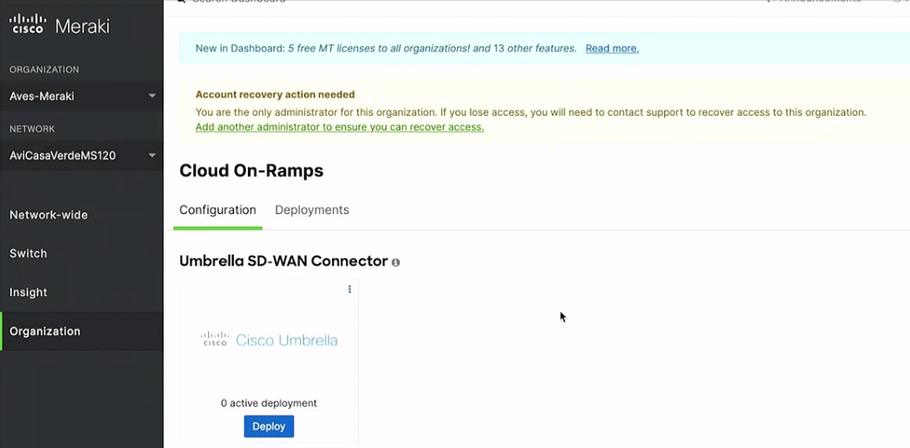
We will see a page as shown below.



If you have Cisco Umbrella license, then when you click on the blue button ‘Connect to Cisco Umbrella’ it will prompt for the API keys which you can get from the API keys menu under the Admin.



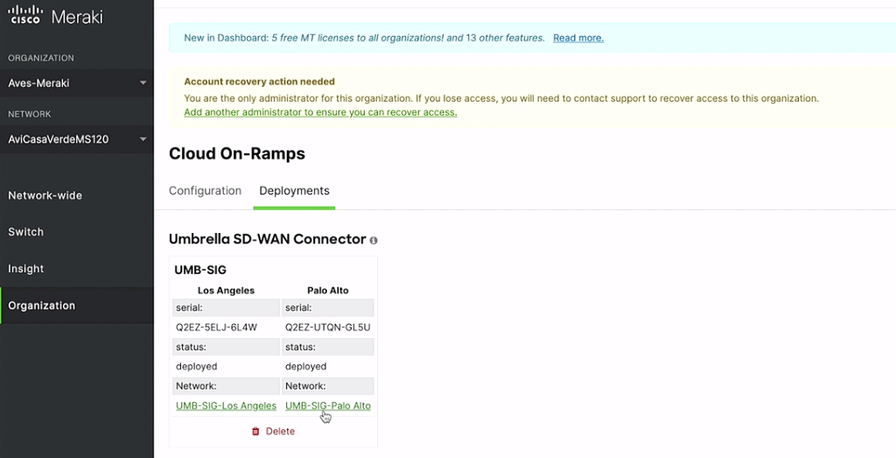
Once you enter the values you will see the following page displayed.



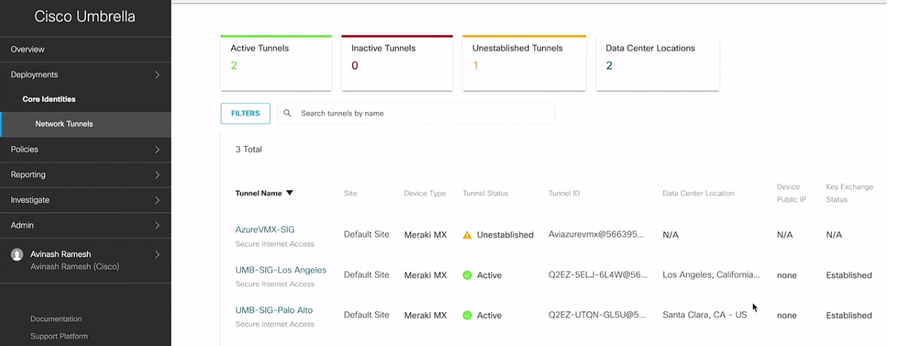
When you click on ‘Deploy’ it will prompt you to enter the network name and then you need to select the data center from the drop-down menu. The menu will display the list of available data centers.



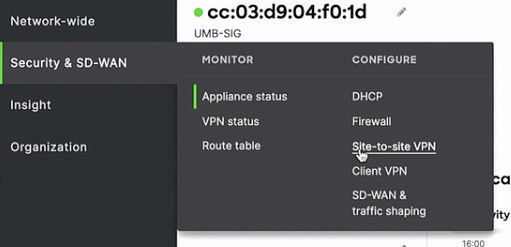
Once you click the button ‘Yes, continue’ it may take around five minutes for the deployment to happen and the details can be seen as below.



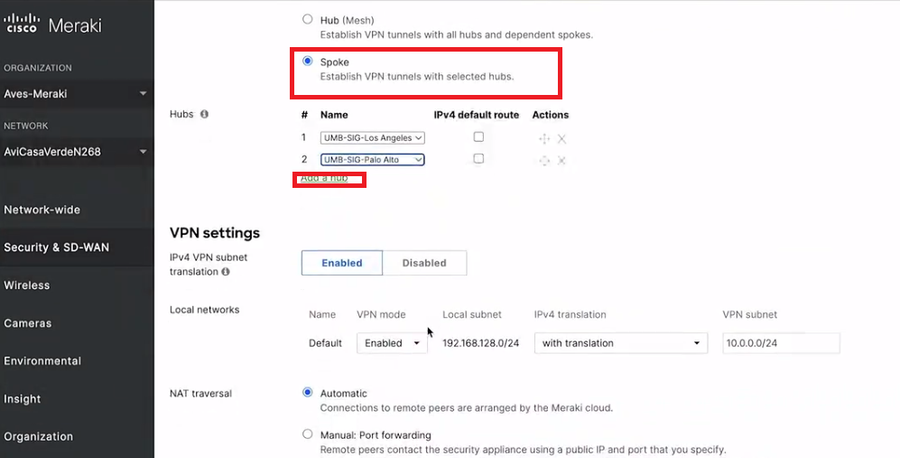
To verify, you may navigate to the ‘Network Tunnels’ under ‘Deployments’ where you can see the tunnels are active.



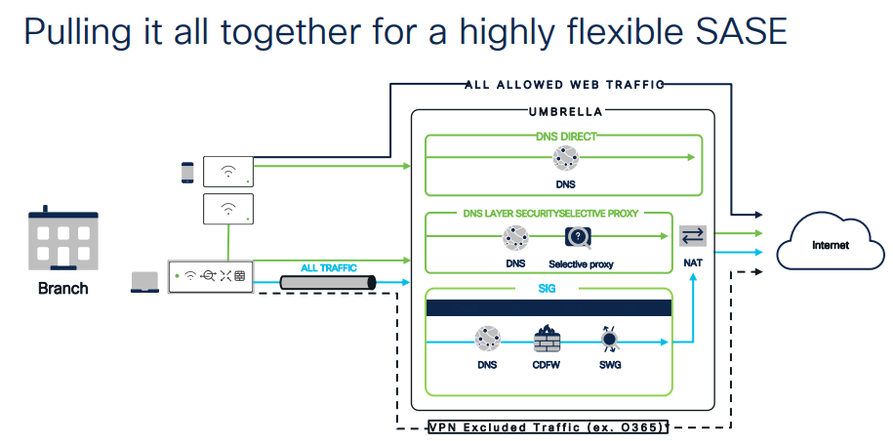
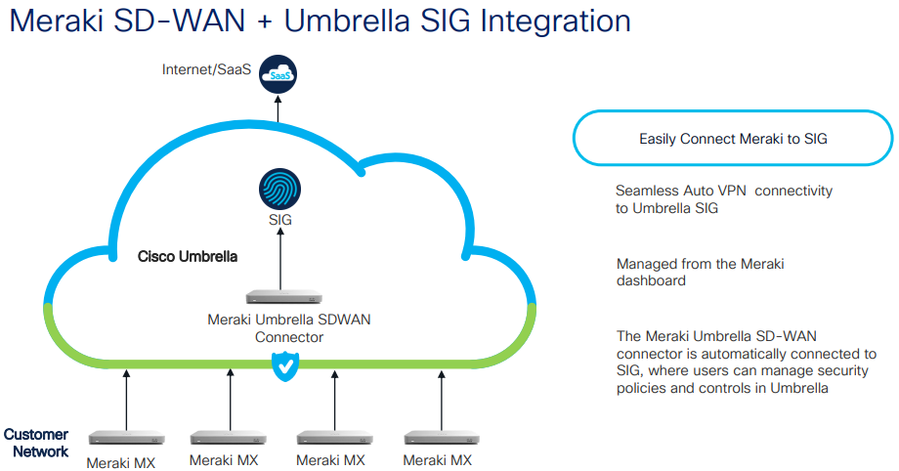
Each connector is deployed as a HUB on Data Center which will be having the default route to the Umbrella. Let’s navigate to the option ‘Site-to-Site VPN’ under the ‘Security & SD-WAN’ menu.



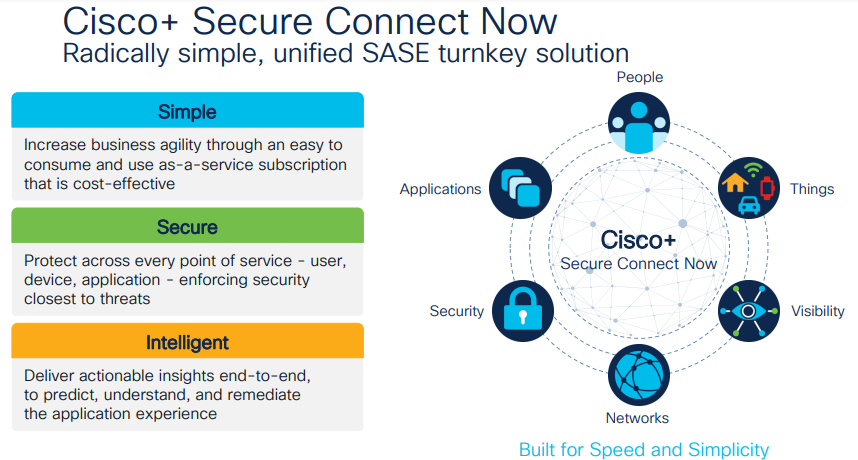
Here, on the page displayed, let’s select the ‘Spoke’ radio button and click on ‘Add a hub’ link whereby we are adding the network as shown below.



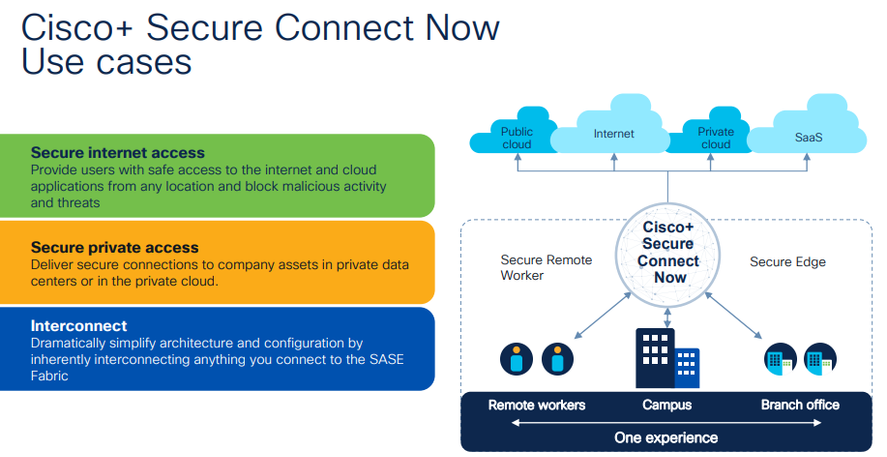
This is how you can have Umbrella security policies setup across the networks at different locations. If needed, you can have specific security policies for each network using the Meraki Dashboard.



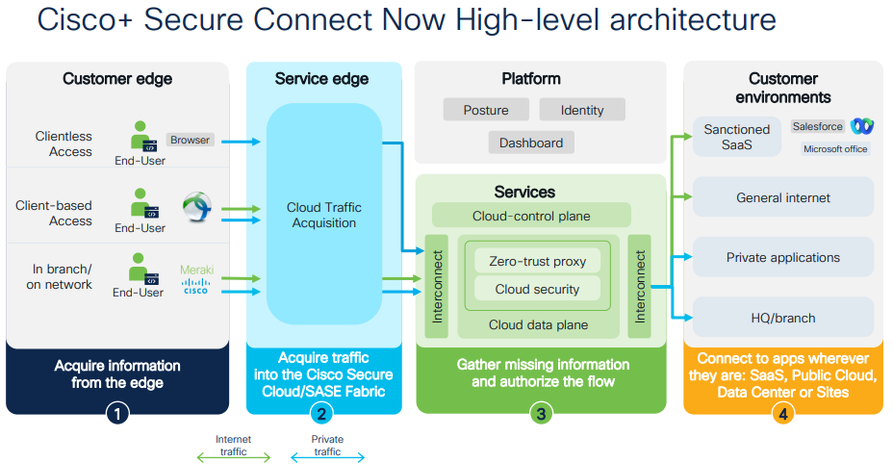
Next Let’s see another SASE solution which is named as **Cisco+ Secure Connect Now**. The product combines all the factors that you may come across in any application and make the connectivity based on these three pillars namely - simple, secure, and Intelligent.



Here are some of the use cases using Cisco+ Secure Connect Now. A remote user will be accessing an application which could be on cloud or Internet or anywhere from any location. In this case, the first option will be to establish a secure connection with the power of cloud umbrella. As there are lots of applications on public/private cloud, your second option will be to establish secure private access. Then, the third, is interconnect, which is the magic on helping on talking to applications at hybrid platforms through the SASE fabric.

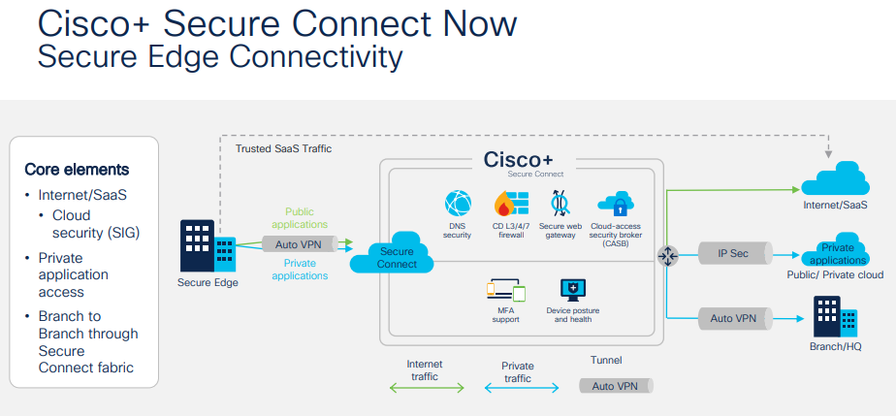


Let’s deep dive into the architecture of Cisco+ Secure Connect Now. For anyone connecting from the branch office via VPN, they will be using a software like cisco AnyConnect. If the user wants to access the network from the browser without VPN, Cisco+ Secure Connect Now will cater to that service also.



Now moving to traffic, what is done is that the traffic from the customer is taken to the service edge. Next comes the magic were the platform that combines the security and networking features as a service has been provided. It is via zero-trust proxy that the customers are provided with clientless access without any VPN to access a private application. Finally comes the customer environment where the customer would like to reach out. This could be any app like something directly accessing via the Internet or reaching out to any private application or accessing an application at the headquarters or branch office.

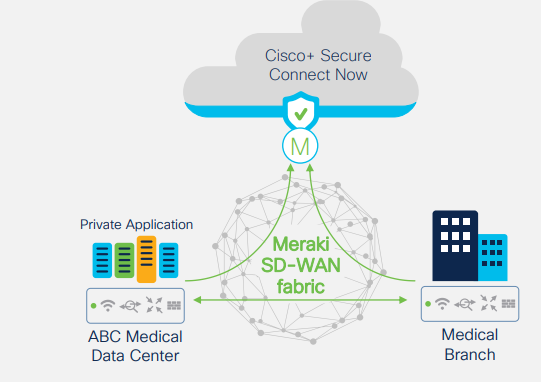
If you happen to be on the Secure Edge and want to connect to Meraki cloud, where the branches are using the Meraki technology, in that case, you will be using the Auto VPN tunnel, which is the Cisco proprietary technology to connect with just a single click from the Meraki dashboard.



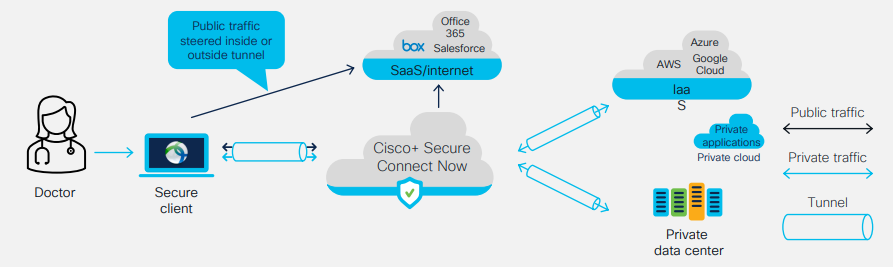
Depending upon the use case, you can have lots of flexibility that can be controlled from the dashboard.  Next, in the case of the user working remotely, the user will reach the client-based network via any connect line and can reach the Internet/SAAS applications. In the case of a clientless/browser based access, all that is needed is an HTTPS session. You will be getting all the capabilities of the cloud-based Umbrella security solution along with Meraki authentication in the solution. This will help to add the users to cloud authentication database very quickly by spinning up a Meraki authentication instance.



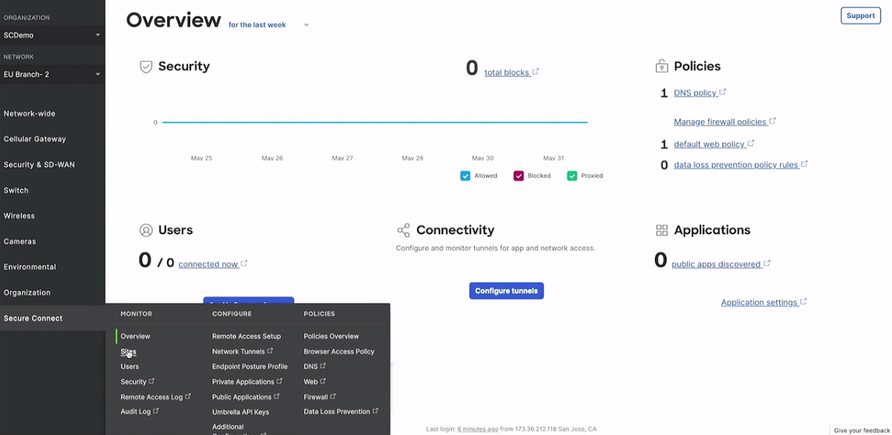
Now let’s take a use case were a medical company wants to connect the Cisco+ Secure Connect Now via Meraki SD-WAN fabric.



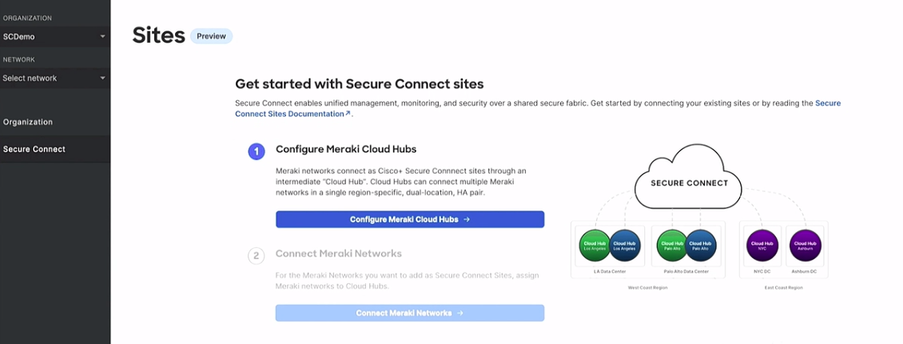
If the doctor want to access an MRI scan report which is been located on AWS or on private cloud then as per the topology diagram shown below it could be accessed directly from Cisco+ Secure Connect Now.



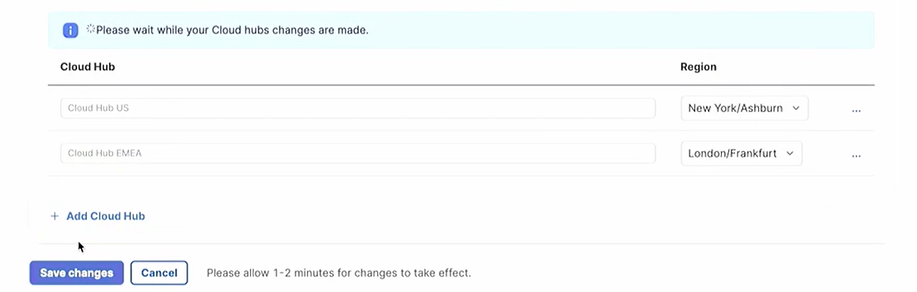
The configurations that need to be done to setup the connectivity of the above scenario is as shown below.Looking into the dashboard, where it’s a green field deployment, navigate to ‘Secure Connect’ and pick up ‘Sites’.



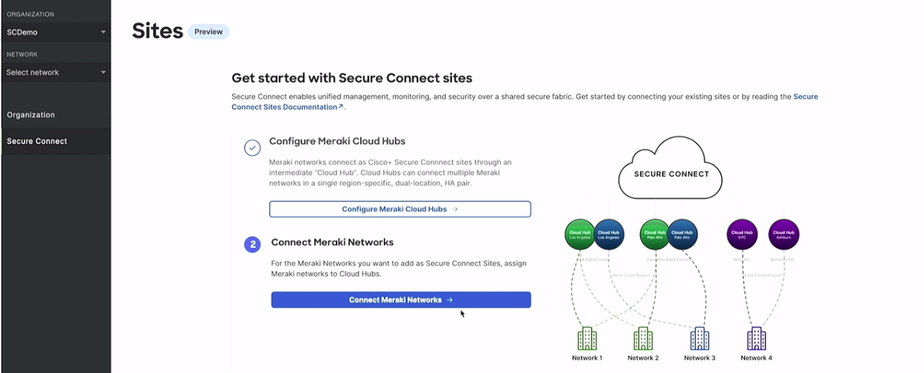
This will open up a window where you are going to add sites.



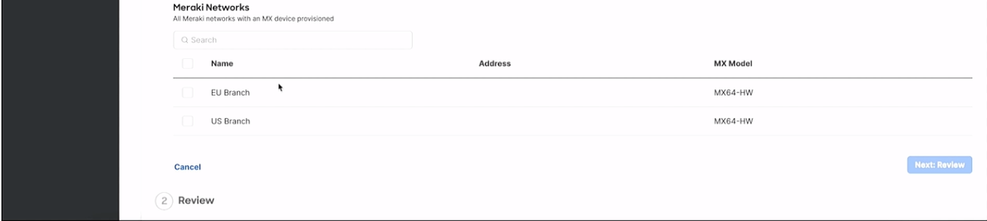
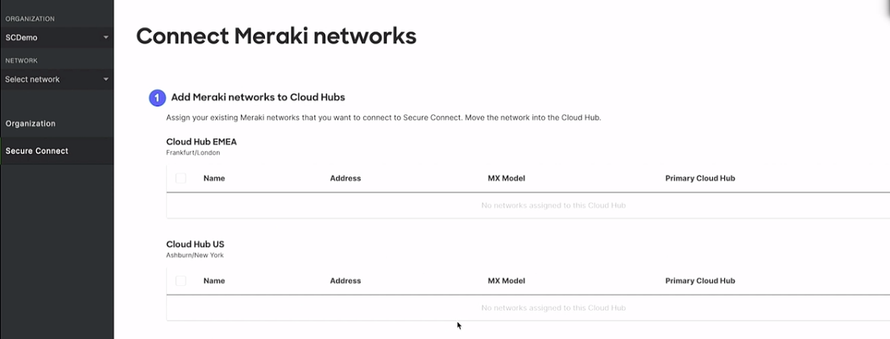
When you click on the ‘Configure Meraki Cloud Hubs’ button, a window as shown below will get opened where you need to click on the ‘+Add Cloud Hub’ and give the details as shown below with the Region. Here we have selected two different locations were the connectivity between happens automatically just in few clicks.



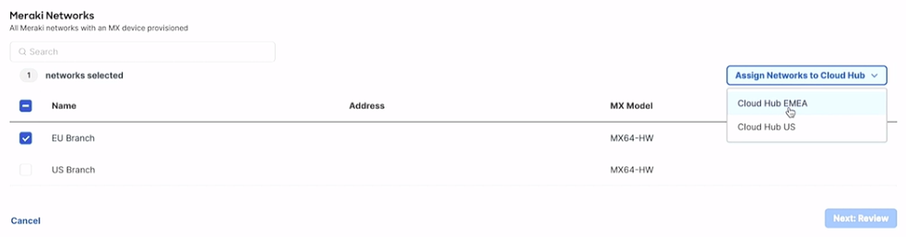
Once you click on Save changes button, it will open up as shown below where you need to click on the ‘Connect Meraki Networks’ button.



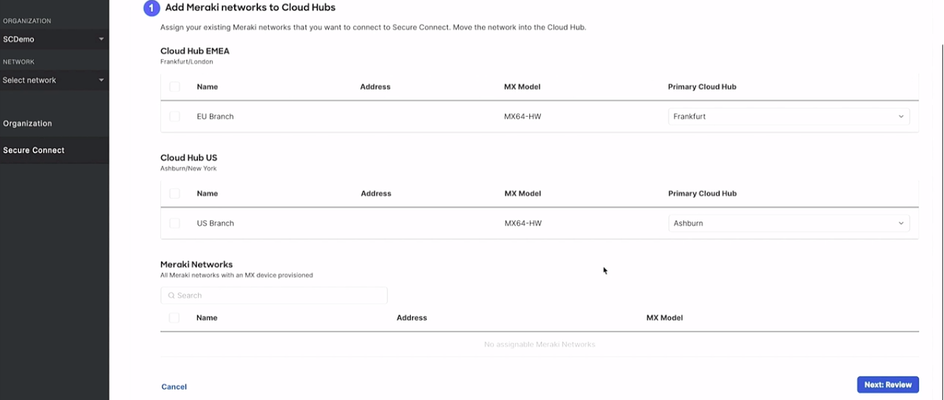
On the window that pops up, you need to add the Meraki network to the hubs which you have just spun up.



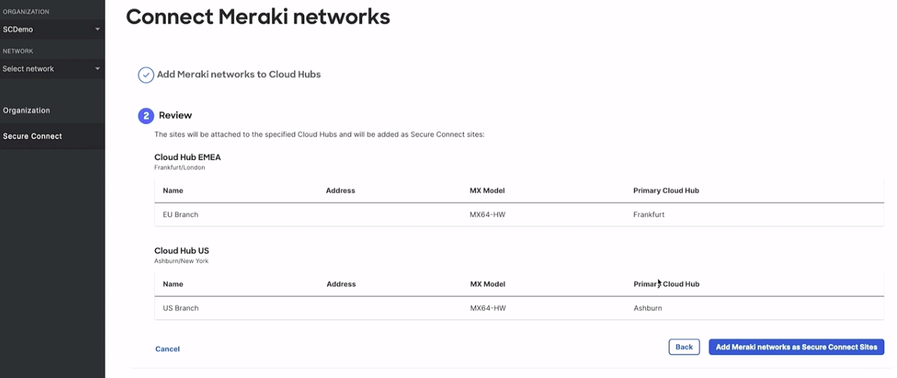
All you must do is select the branch and correspondingly select the hub as shown below.



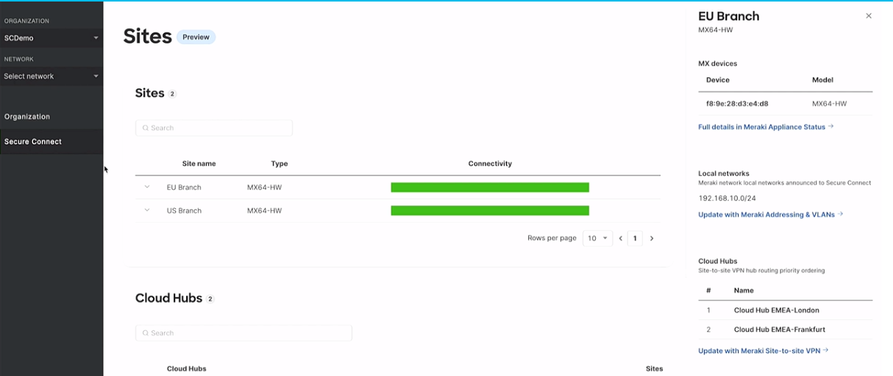
Now you can see the Branch got added to the hub location.



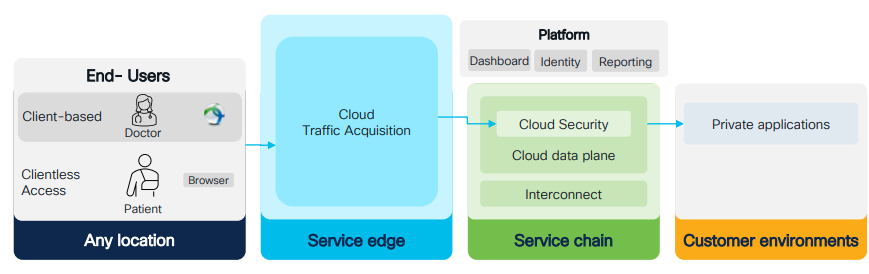
Click on Next button, which will open up a window as below



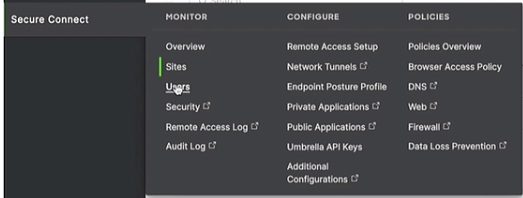
Here, when you click on the button ‘Add Meraki networks as Secure Connect Sites’ it will open up a window where you can see the sites got added.



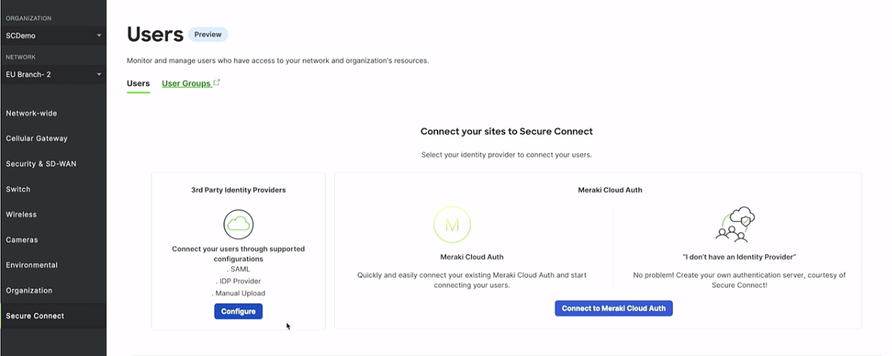
Next, use case is if you are a Patient, you won’t be using AnyConnect but will be using the clientless browser-based access only, while the Doctor will have AnyConnect; in that case also the workflow remains the same as shown below.



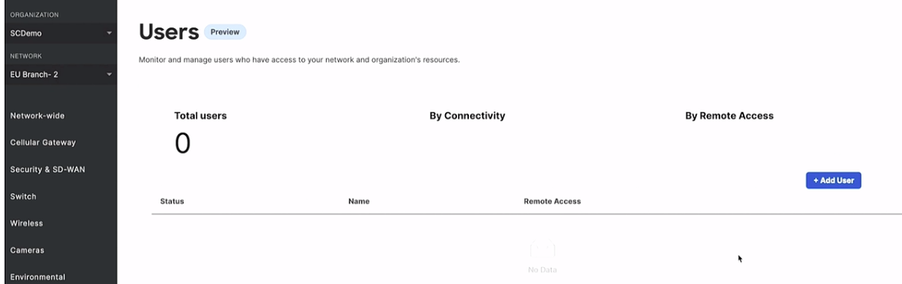
Let’s check out how to setup the user options. For that select the ‘Users’ option from the Secure Connect menu.



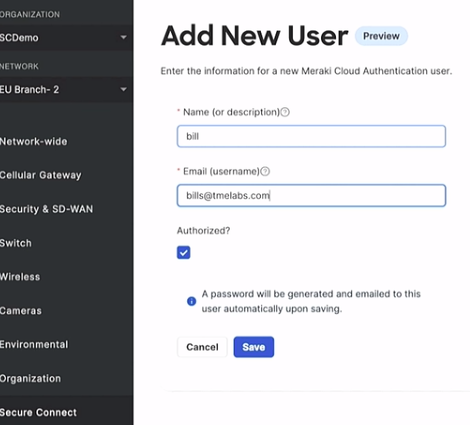
This will open a window as shown below.



When you click on ‘Connect to Meraki Cloud Auth’ button it will do all the jobs needed for user authentication in the background and a window as shown below will get popped up.



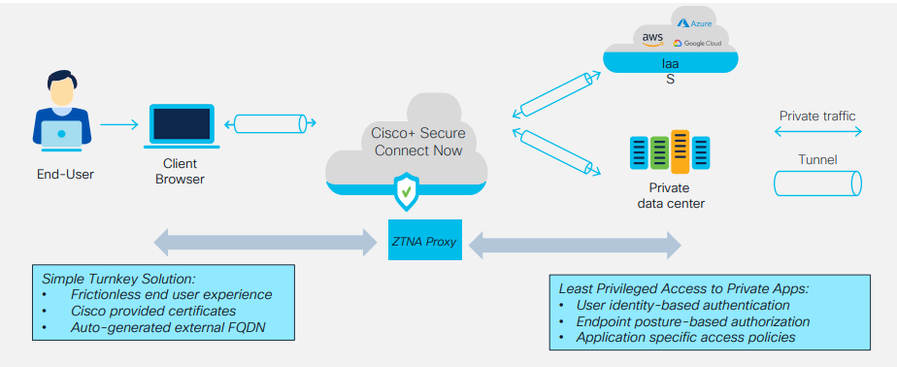
Just add the user details and check the option if the user is authorized to use the services and the click ‘Save’ button.



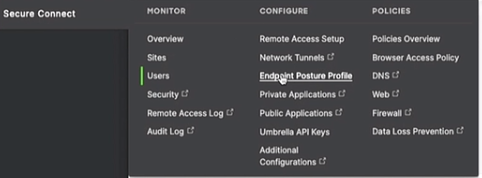
Within a few minutes, you can see that the user got added.



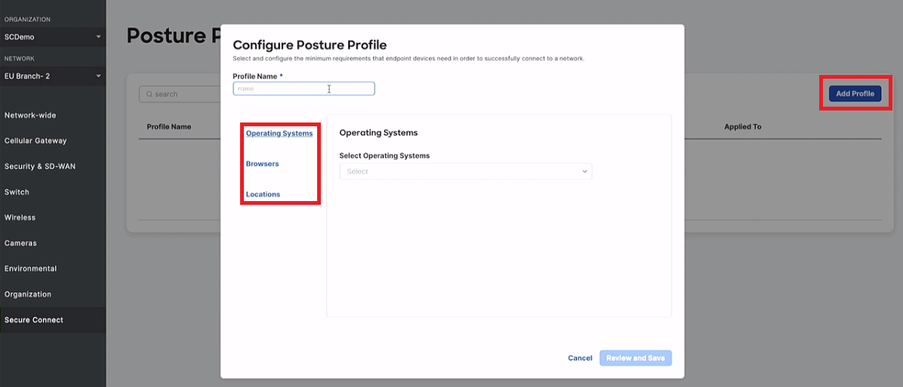
For the next use case, an end user comes to the client browser for accessing the private application on the cloud, the ZTNA (Zero Trust Network Access) Proxy solution comes into picture. It’s a simple turnkey solution were Cisco does all the heavy lifting of providing the certificates and making it user friendly.



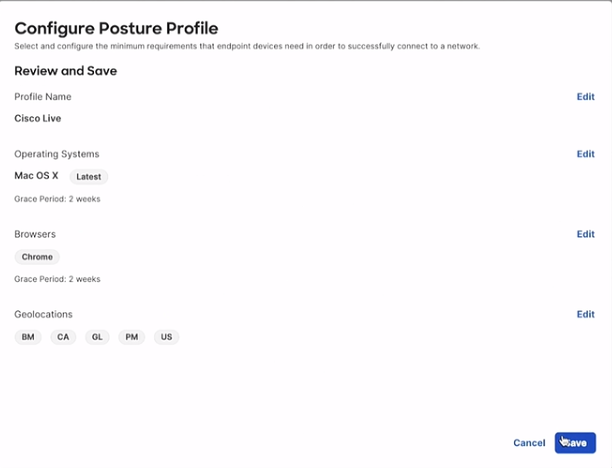
For setting it up, select ‘Endpoint Posture Profile’ from the Secure Connect Menu.



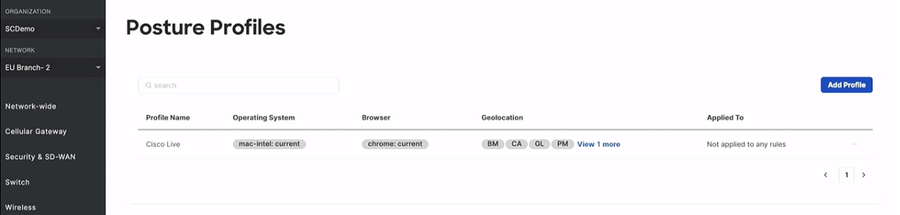
This will open up window where you will click on the button ‘Add Profile’, which will open up a pop-up window where you need to give the name of the profile, operating system and browser, along with the location.



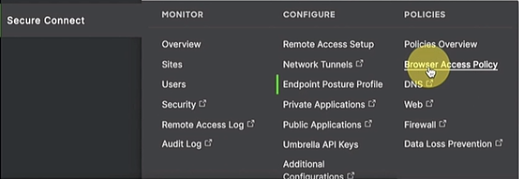
Once done,



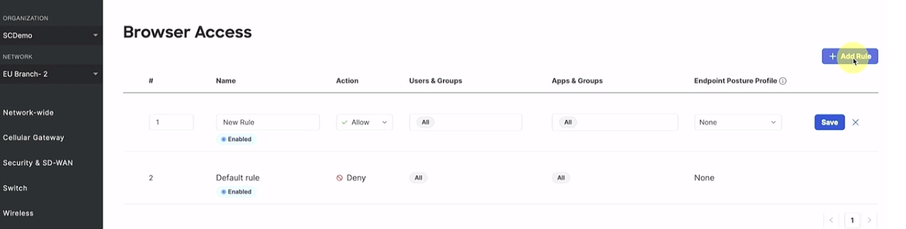
Click on ‘Save’ and you can see the Posture Profile as below.



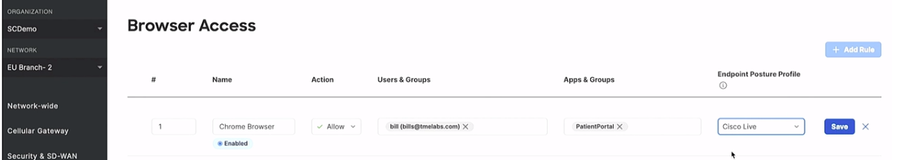
As you can see, this Posture profile is not applied to any of the rules. For that you need to go to ‘Browser Access Policy’ on Secure Connect



By this you are going to add a policy to the profile which you have created.



Give the details of the user and application name along with profile details as shown below. (It should be an application which is already running in the background)



Once saved on the browser, we can see…

Graphical user interface, text, application, Word

Description automatically generated

If you are using Multi Factor Authentication, once you click on the URL which Cisco had provided, it will take you to the login prompt and, once authenticated, you will be able to access the application.

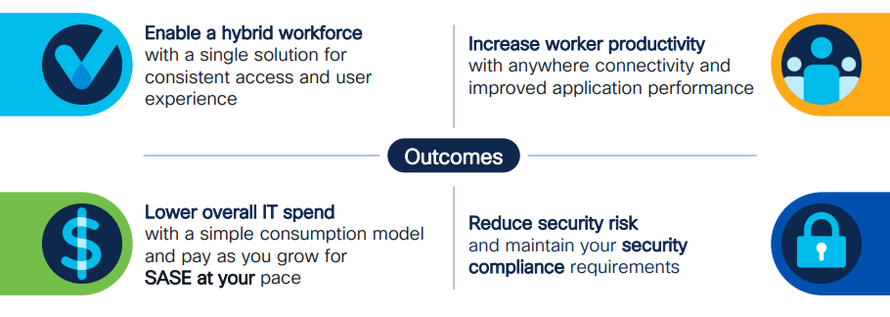


This is how the Dashboard looks and we can have single sign-on (SSO) using the Meraki Dashboard into Cisco Umbrella platform in just a few clicks.





The overall outcome on using **Cisco+ Secure Connect Now** are the following.



Reference

<https://blogs.cisco.com/ciscoit/the-sase-story-part-two-how-cisco-it-developed-our-internal-sase-product-amid-an-evolving-industry-landscape>

<https://www.youtube.com/watch?v=zcNaENtGRsg>

<https://www.youtube.com/watch?v=5_bSTGOfNI4>

Learning lab

<https://developer.cisco.com/learning/modules/security-sase-meraki/>

DevNet Page

<https://developer.cisco.com/SASE/>