The bridge to possible

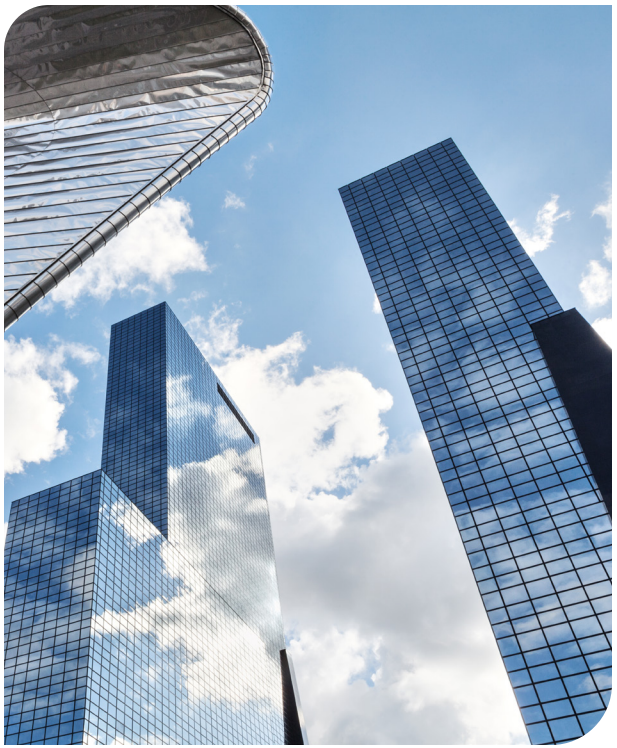
Cisco SWA-Umbrella Integration: Unified Policies and Common Reporting

The bridge to possible

Overview

The cyber-attack vectors can be present anywhere in an enterprise or individual's network making it really difficult for network security administrators to enforce the policies for their organisational users. In this modern era, the hybrid work has taken over the conventional campus working models. The users can now join the network physically or virtually from a remote location. Also the organisations are relying more and more on cloud-delivered applications allowing users to access them from any device of their choice, making it really difficult for administrators to manage the web policies or grant access to web applications in the same way they would do it for their campus networks.

The need for hybrid deployment is prevalent for the organisations that have global presence. The data sovereignty laws and in general, the law of land varies and sometimes changes significantly. These laws governing the user-confidential data such as their browsing patterns, any Personally Identifiable Information (PII), or exporting the web-browsing logs outside the state or region where the users are based in.



Introduction to Secure Web Appliance Integration with Cisco Umbrella: A Hybrid Approach

Hybrid deployment mode is essentially deploying Secure Web Appliance (SWA), alongside Cisco Umbrella – Secure Internet Gateway (SIG) for those specific scenarios where the administrators want to enforce the same web policies and application access to the users as they have defined it for their user-base in cloud delivered web gateway solution. SWA can now deeply integrate with the Umbrella SIG Web Policies and adapt the same granular policies that are defined in Rulesets and Rules for various for the Identity types. These SIG policies can now be translated and push down to On-Premise appliances. This allows network administrators to keep the web-policies synchronised between the Cloud proxy and On-Premise proxy solutions, simplifying the process to manage the policies from one-singe dashboard.

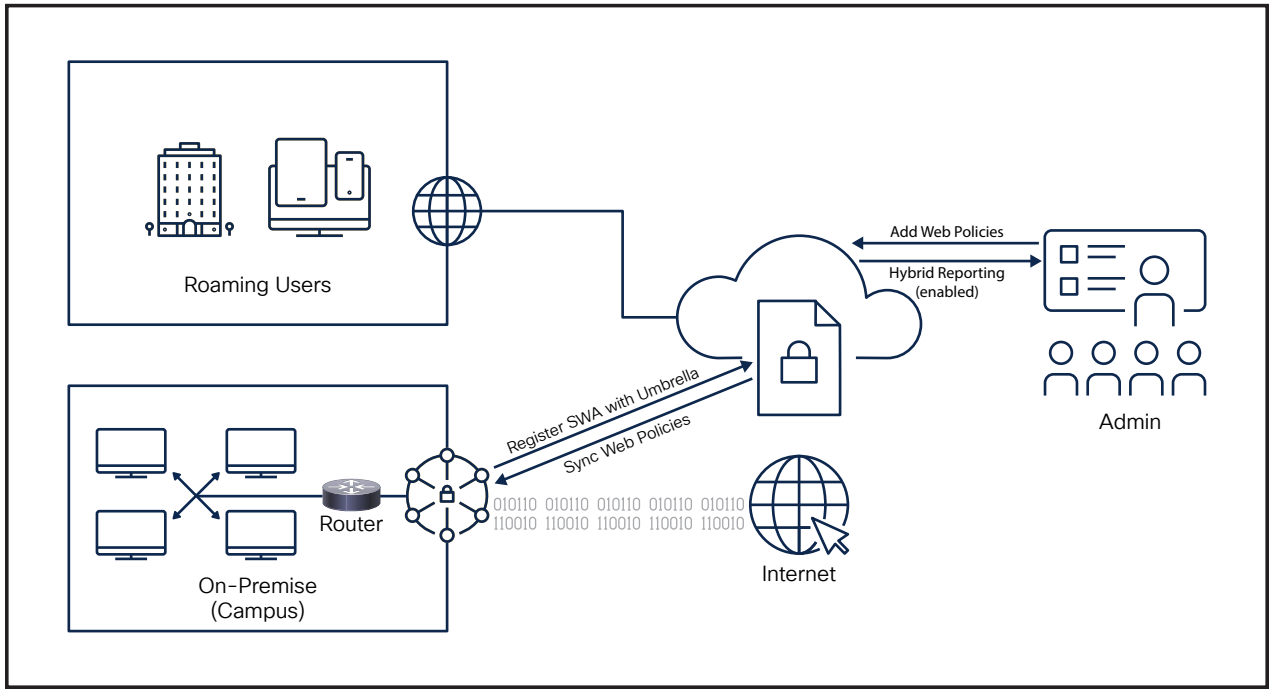
The bridge to possible

"Hybrid deployments lack feature parity and seamless integration between the two products. For example, the policies share common categories, but must be managed separately."

Gartner, Magic Quadrant for Secure Web Gateways, 2019

Product requirements

- Secure Web Appliance (support for all hardware and virtual platforms)
- Cisco Umbrella SIG Bundle (Essentials or Advantage)

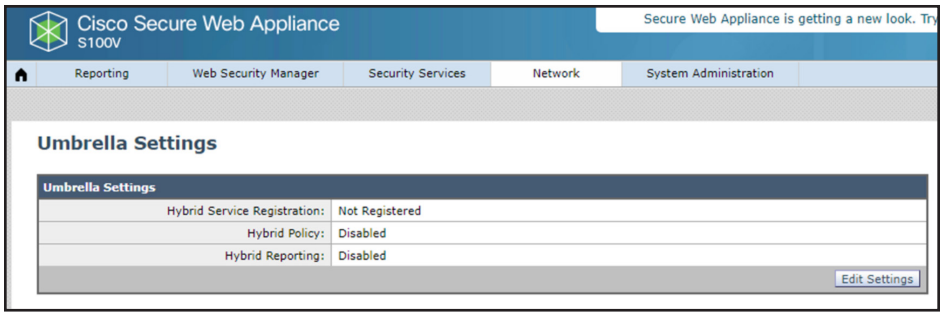


The bridge to possible

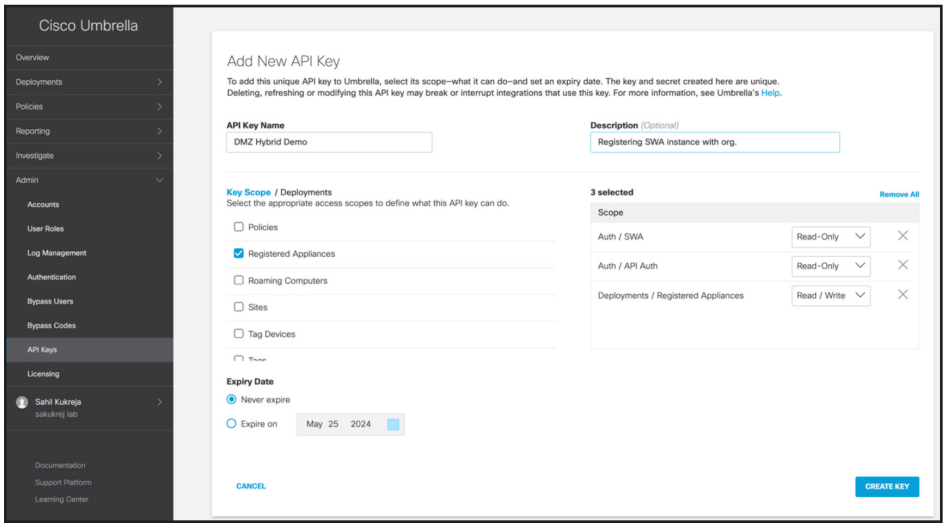
Configuration

Step 1 – Log in to the Secure Web Appliance UI using the admin credential: https://wsa_hostname:8443.

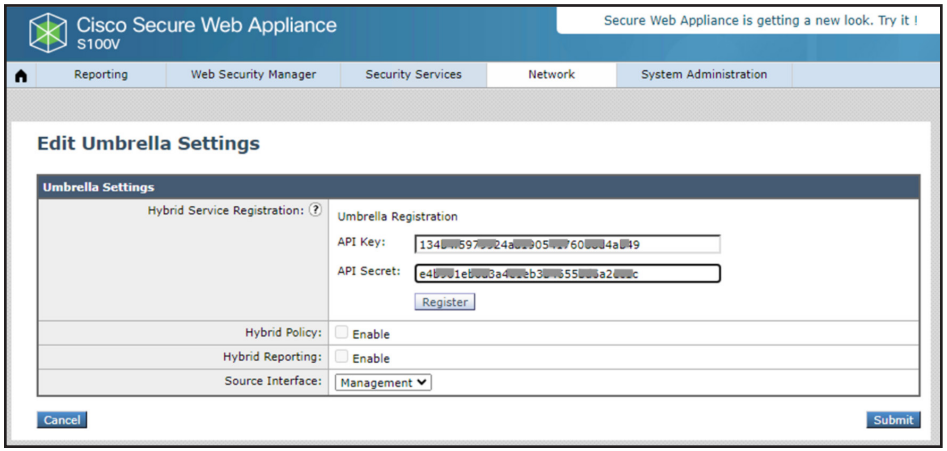
Step 2 – Navigate to Network > Umbrella Settings , and click on the Edit Settings button:



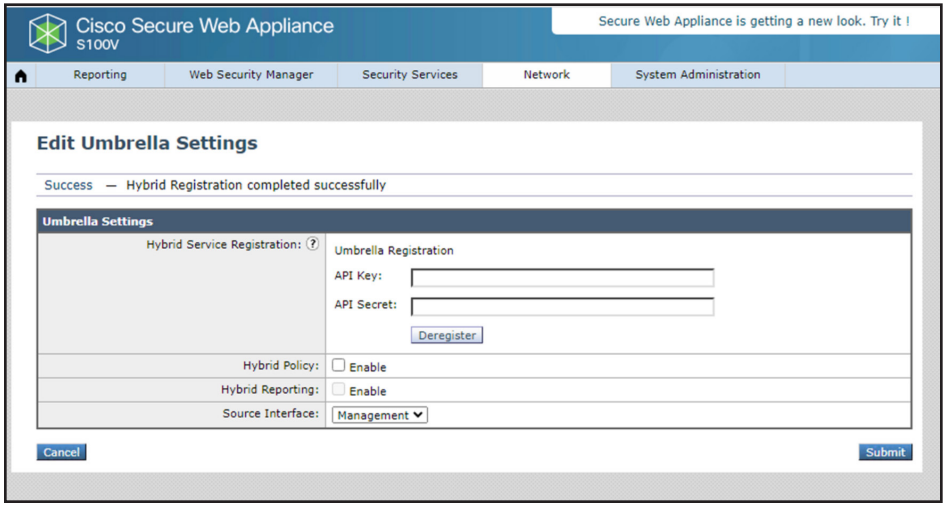
Step 3 – To register an appliance with Umbrella SIG, create an API key and secret pair on your Umbrella dashboard (and store it in file for future reference – optional).



Step 4 – Register the appliance using the created Umbrella API Key and Secret pair, save and commit the change on SWA to successfully complete the process.

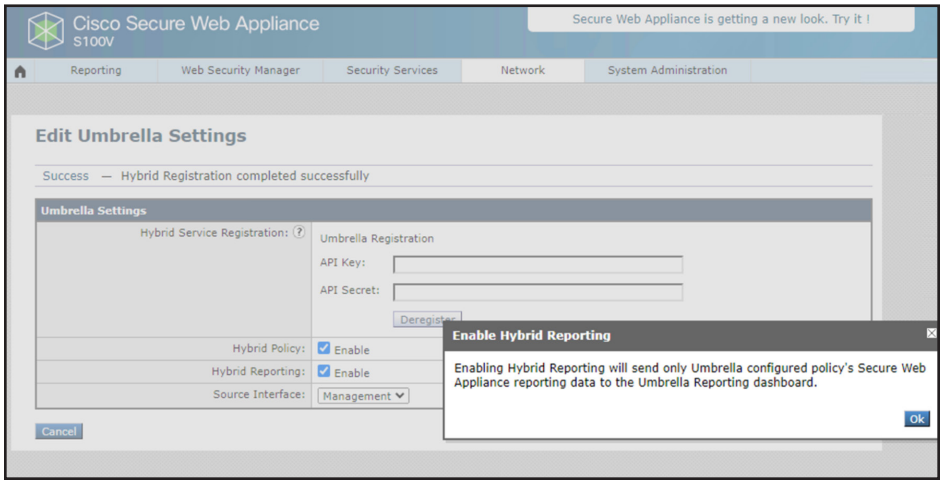


Step 5 – Click on the Submit button complete the process.

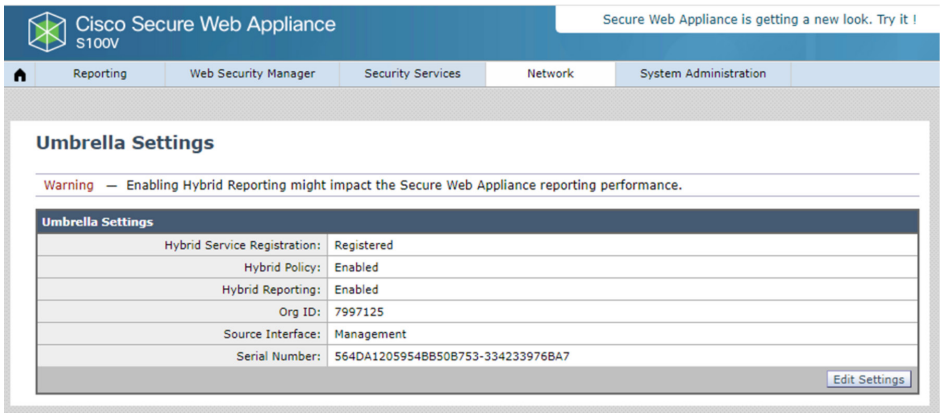


The bridge to possible

Step 6 – Hybrid configuration allows admins to selectively enable the Hybrid Policies sync and Reporting on SWA UI.

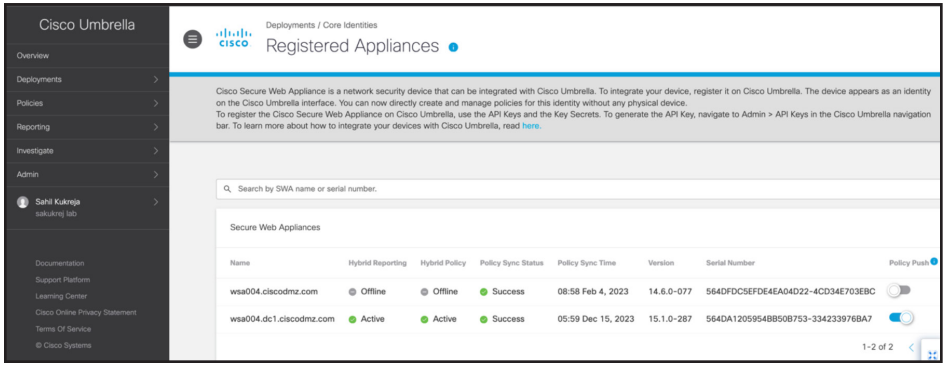


Step 7 – Once the appliance is successfully registered with the Umbrella Org., the status will be displayed under Network > Umbrella Settings main page on SWA UI with hybrid services status, registered OrgID, Source Interface used to sync policies and exporting reporting data with Umbrella, and Serial number of SWA to uniquely identify the registered appliance.

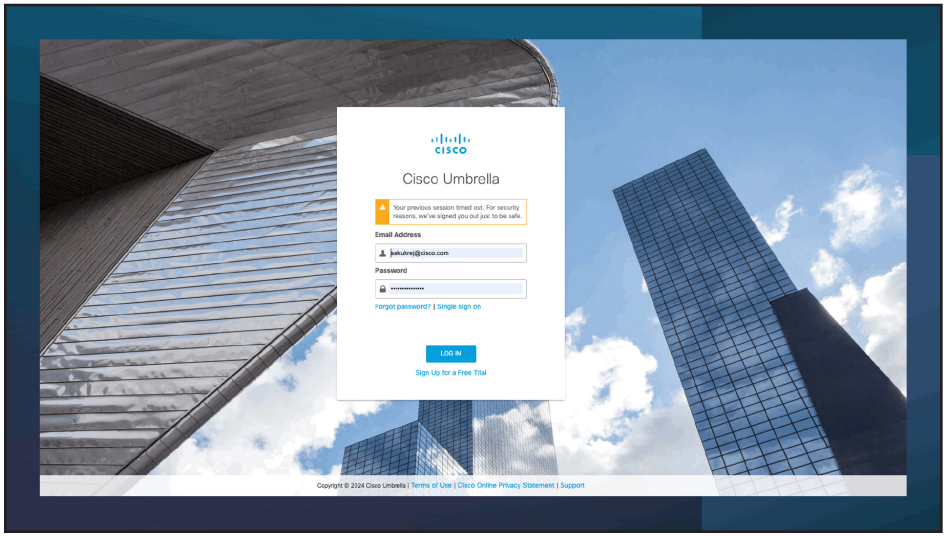


(Note : Source Interface needs to access to Internet or exception to reach out to Umbrella SIG FQDN or Umbrella anycast IPs)

Step 8 – Login to Umbrella dashboard, navigate to Deployments > Registered Appliance to check the status. It shows the hostname individual hybrid services status, last Policy sync with the registered appliance, installed AsyncOS version and Serial Number of appliance to uniquely identify the SWA. The Policy Push can be selectively enabled or disabled for each appliance using the toggle switch.



Step 9 – Confirm the Web Policies once pushed down to SWA from Umbrella. A default Identification Profile should be added to SWA. Also, each rule should be translated to Access Policies with either a subnet or User-group.



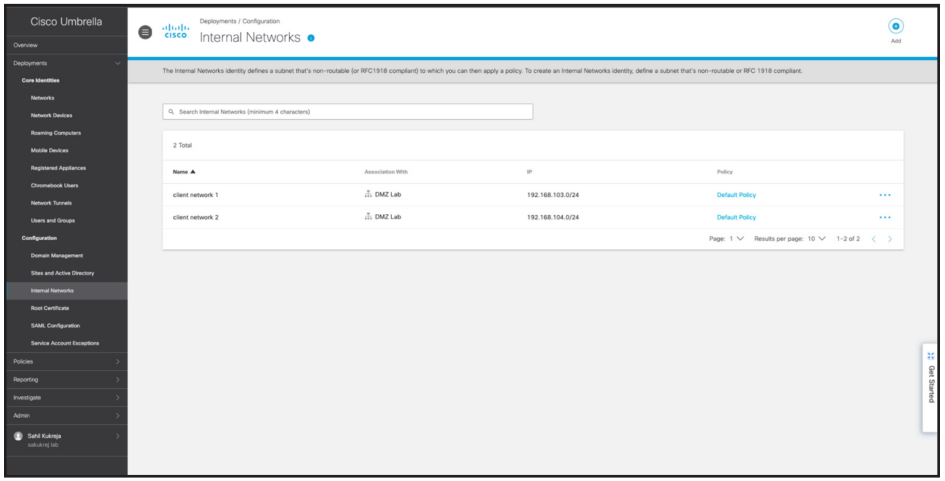
Use cases for hybrid configuration

The following section walks through a few common use cases adopted by organizations.

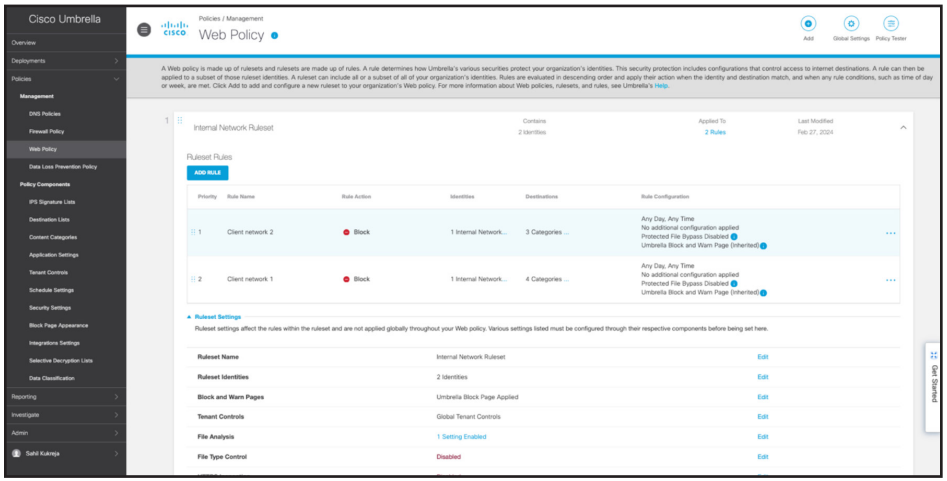
Rules based on Internal Networks or Subnets

The above configuration will translate all web policies on Umbrella and push them down to SWA. This section will walk administrators through the testing step by step and show the translated policies on SWA to ensure the same access privileges for On-Premise users.

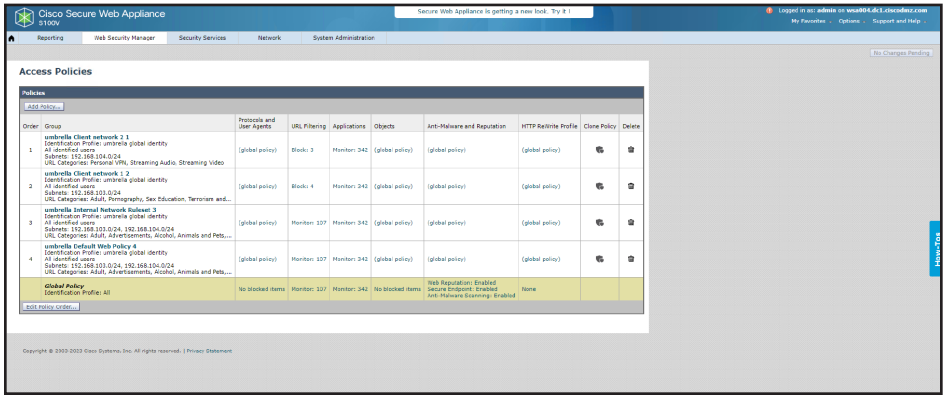
Step 1 – Login to Umbrella dashboard and add Deployment > Network and subnets under Deployment > Internal Network.



Step 2 – Register the appliance with Umbrella, navigate to Policies > Web Policy on Umbrella to create ruleset selecting the added Internal Networks as Ruleset Identities. And add Rules to either Block, Warn or Allow URL Categories.



Step 3 – Ensure that the Web Policies are being translated to Access Policies: Login to SWA UI and navigate to Web Security Manager > Access Policies.



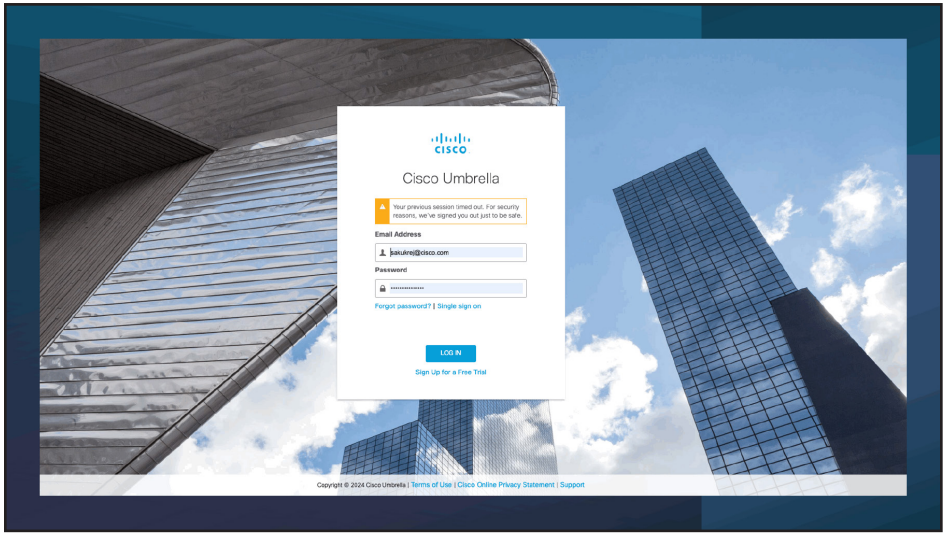
The bridge to possible

Configure Destination Lists, Microsoft 365 feeds for Proxy Bypass and Selective HTTPS Inspection for AD Users or Internal Networks

Step 1 – Go to Policies > Web Policy on Umbrella to create ruleset selecting the added Internal Networks as Identity.

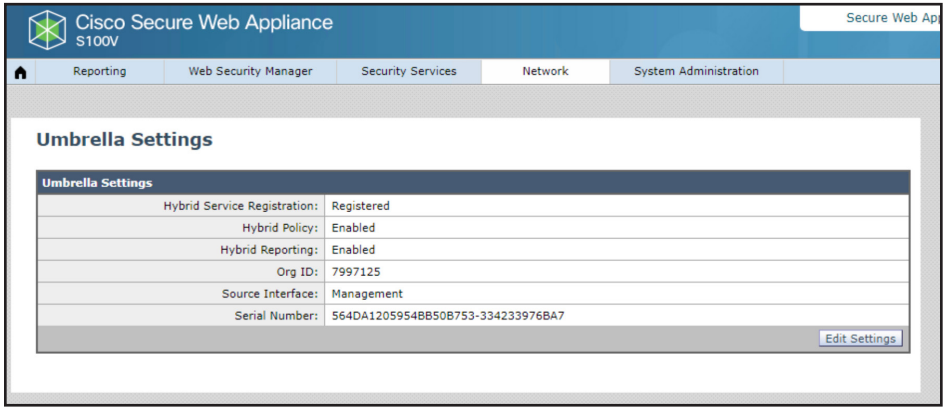
Step 2 – Create Selective Decryption Lists and add that to HTTPS Inspection.

Step 3 – Add a Rule with policy action set to WARN for a URL Category.

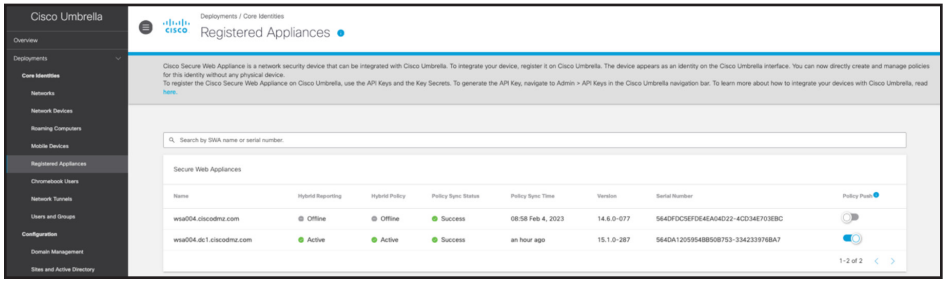


Common Reporting dashboard for Secure Web Gateway – Exporting SWA Logs to Umbrella and Filtering in Activity Search

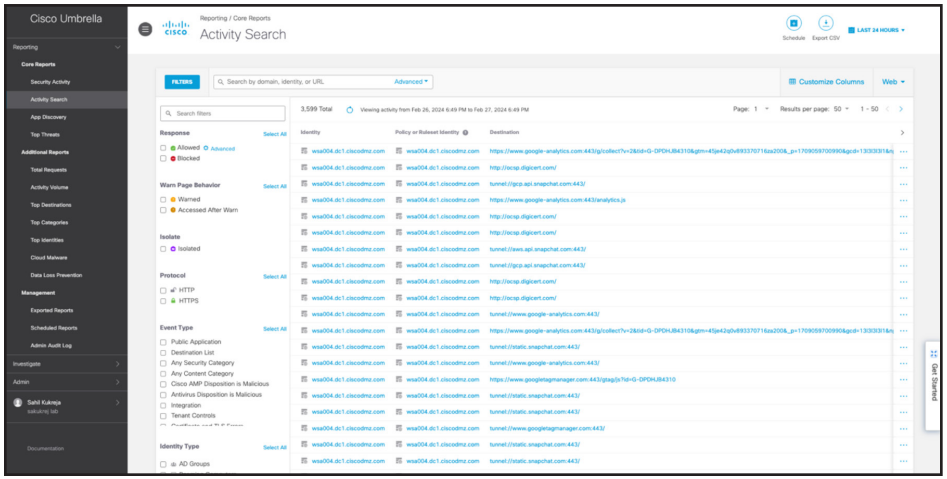
Step 1 – Login to SWA and navigate to Network > Umbrella Settings to enable Hybrid Reporting for the registered appliance.



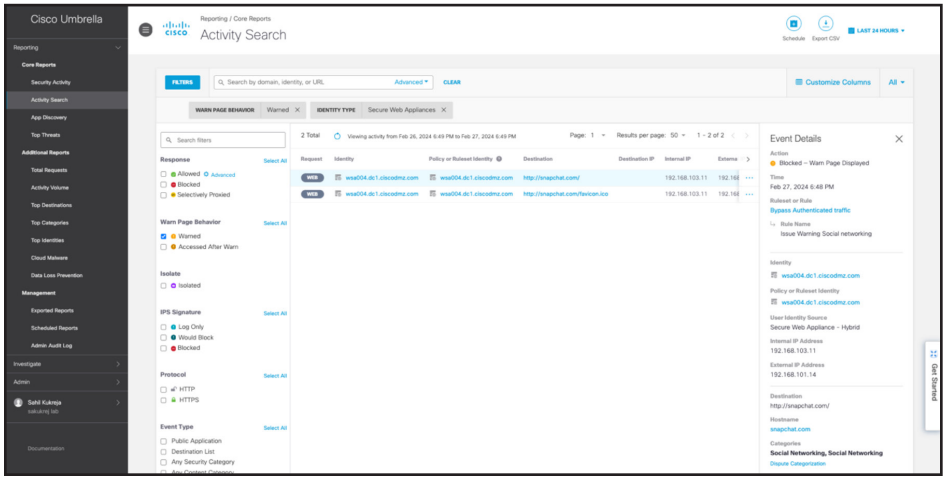
Step 2 – Check the status of Hybrid Reporting service on Umbrella Dashboard > Deployments > Registered Appliances.



Step 3 – Navigate to Reporting > Activity Search to see all the transactions that match the policies created on Umbrella web policies and synchronised with registered SWAs.



Step 4 – Apply filter Identity type as Secure Web Appliance. Click on View full details to see the search results.



Conclusion

SWA hybrid mode will offer a deeper integration with Cisco Umbrella, allowing network administrators to manage the secure web gateway (both the cloud and on-premise appliance) and observe user activity from one single place. This enhances the overall experience while ensuring the security posture for all type of users irrespective of their location, devices or authentication mechanism.

- Gives an opportunity to Secure Web Appliance customers to start planning the migration to Cisco Umbrella.
- Common Reporting Dashboard to see all activity on Umbrella dashboard makes the whole experience seamless and smooth.
- Head-end approach to achieve hybrid web gateway solution for existing Umbrella customers.
- Selective Policy push and Hybrid Reporting functionality on-demand give finer control over the appliance allowing administrators to manage the policies for On-Premise users.
- Organisations can choose the logs storage location from Umbrella dashboard, even for Secure Web Appliance.

The bridge to possible

Package information

Hybrid mode will be supported for all the Umbrella Orgs that either have the SIG Essentials or Advantage packages. There's no separate Hybrid SKUs for SWA to synchronising on-premise appliance with Umbrella Web Policies or allow reporting logs to be exported and viewed on Umbrella Activity Search for the policies created on Umbrella dashboard and pushed down to registered appliances.

For more information

For detailed information on Cisco Secure Web Appliance, go to www.cisco.com/go/wsa.

A Cisco sales representative, consulting system engineer, or channel partner can help to evaluate how Cisco Secure Web Appliance will enhance your security.

C22-4328099-00 04/24