Doc type / Publish Date
Cisco Public – 10/06/21

UMBRELLA SEAMLESS IDENTITY SHARING

CISCO SECURE WEB APPLIANCE – ASYNCOS 14.1

SECURITY BUSINESS GROUP
NETWORK SECURITY TECHNICAL MARKETING ENGINEERING

© 2021 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Contents

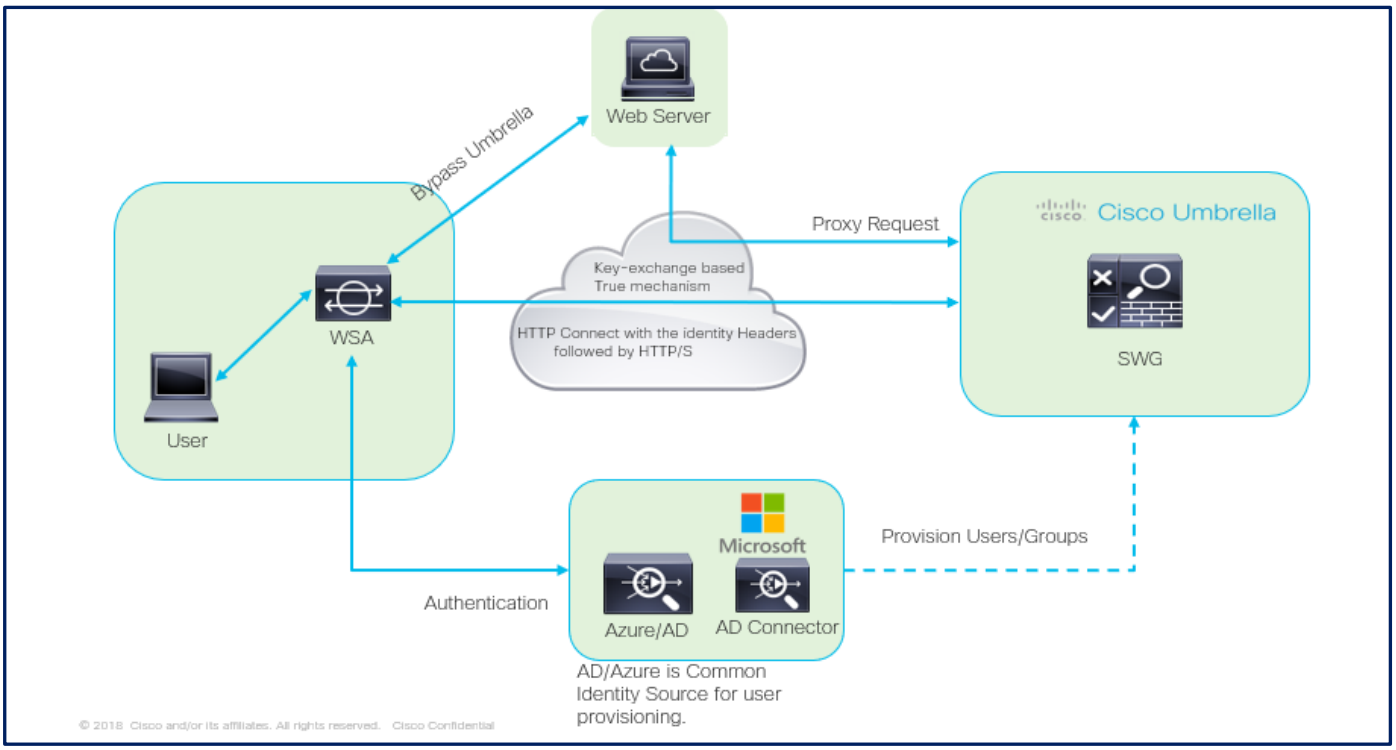
© 2021 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Introduction

Cisco WSA Async OS 14.1 introduces **Cisco Umbrella Seamless Identity Sharing** to enhance Cisco Umbrella's Secure Web Gateway (SWG) active directory-based authentication. Currently, Cisco Umbrella supports end-users SAML based authentication for on-premise and the AnyConnect Umbrella connector for roaming users. The Cisco Umbrella Seamless Identity Sharing feature improves the user experience by using transparent authentication, which compared to SAML's requirement IP surrogates, removes the need for the WSA to decrypt the traffic locally.

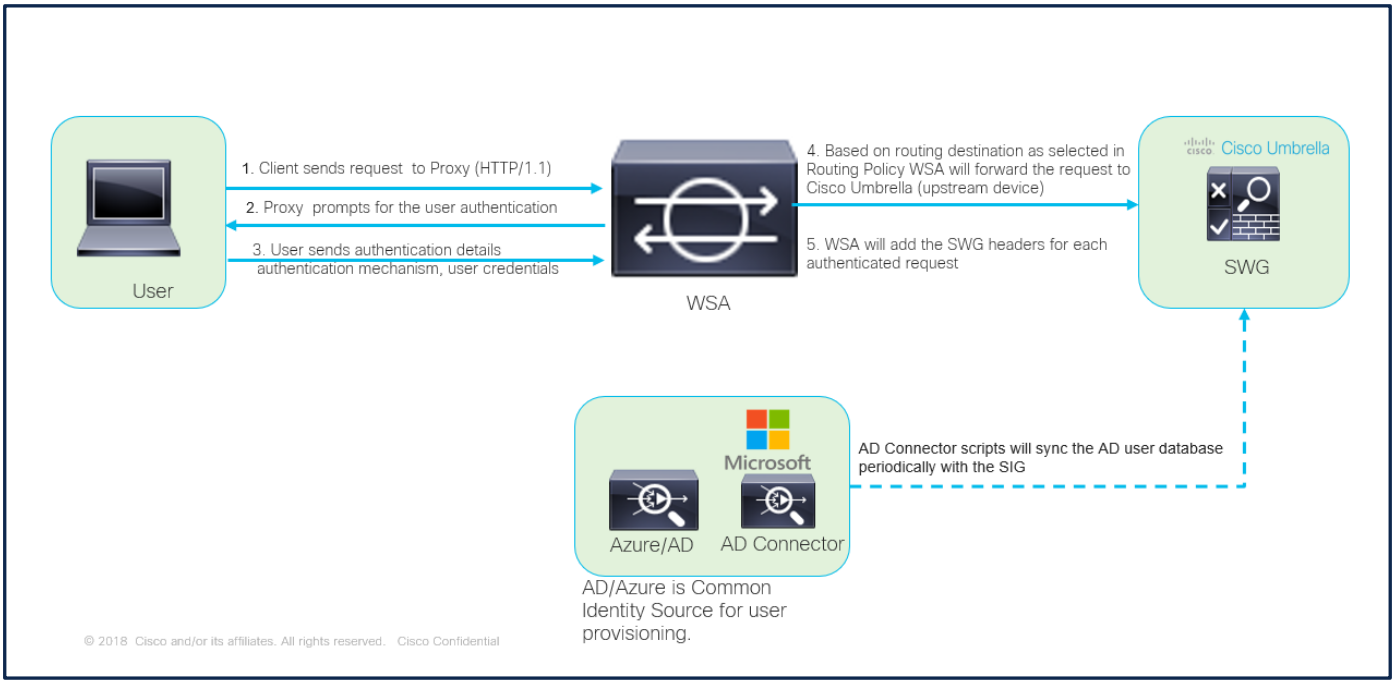
Cisco Umbrella Seamless Identity Sharing can authenticate on-premise active directory end-users and forward traffic to Cisco Umbrella to apply web policies based on user privileges. The WSA provides Identity information to Cisco Umbrella so that network administrators can apply different controls on the information received from the downstream WSA. This feature utilizes the best of both WSA and Umbrella, which have evolved over time to fulfill enterprise environments increasing demands. The WSA supports active directory-based proxy authentication, e.g., BASIC, NTLMSSP, KERBEROS authentication mechanisms. Cisco Umbrella acts as an upstream proxy to the WSA using a newly added interface that uses header-based authentication for trusting the downstream proxy. Cisco Umbrella recognizes the authentication headers to make decisions on the incoming user traffic.

High-Level Architecture



© 2021 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Packet Flow



Configuration

Prerequisites

1. To use the Cisco Umbrella Seamless Identity Sharing feature, please reach out to your Cisco Umbrella Account Manager to enable it for your account.
2. Once enabled, import the Root Certificate from Umbrella before configuring the Seamless ID on the WSA under **Network > Certificate Management > Manage Trusted Root Certificates** as shown below:

© 2021 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

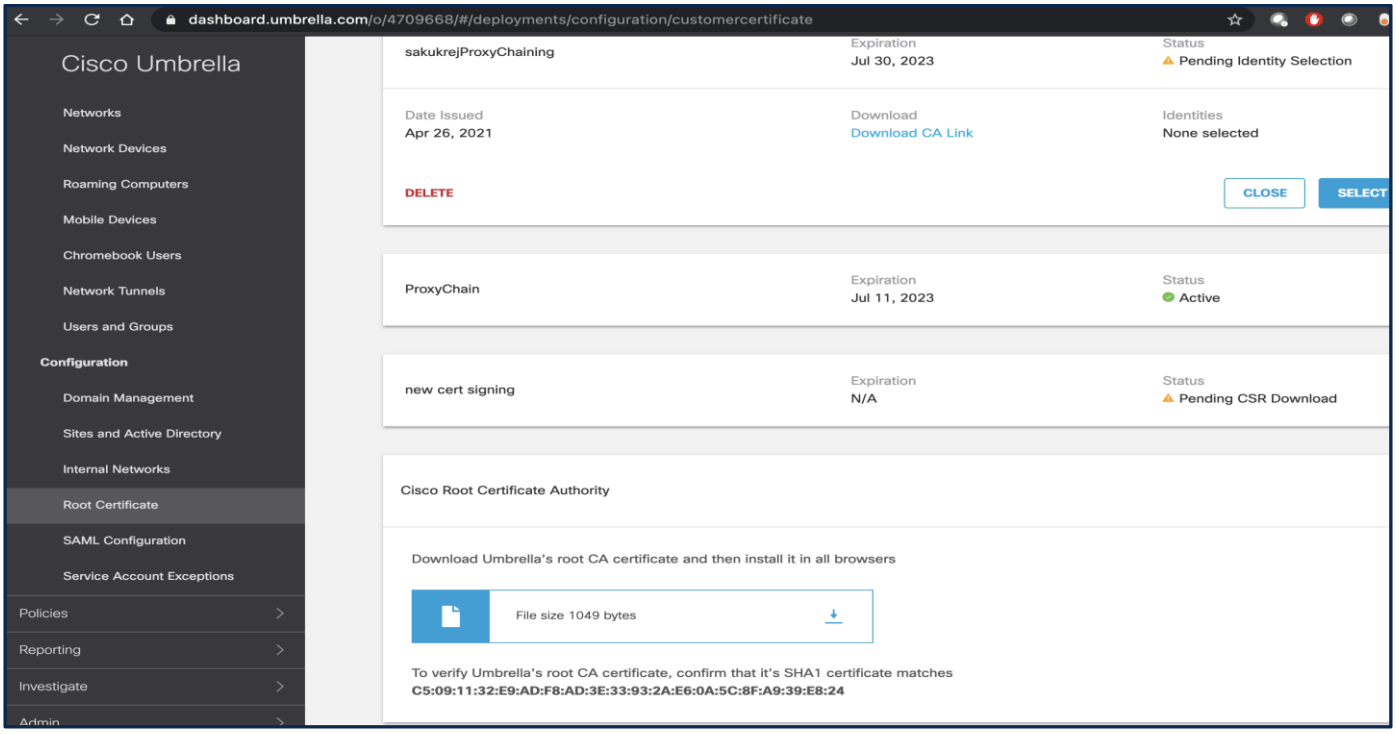


Figure 1 – Self-signed Certificate

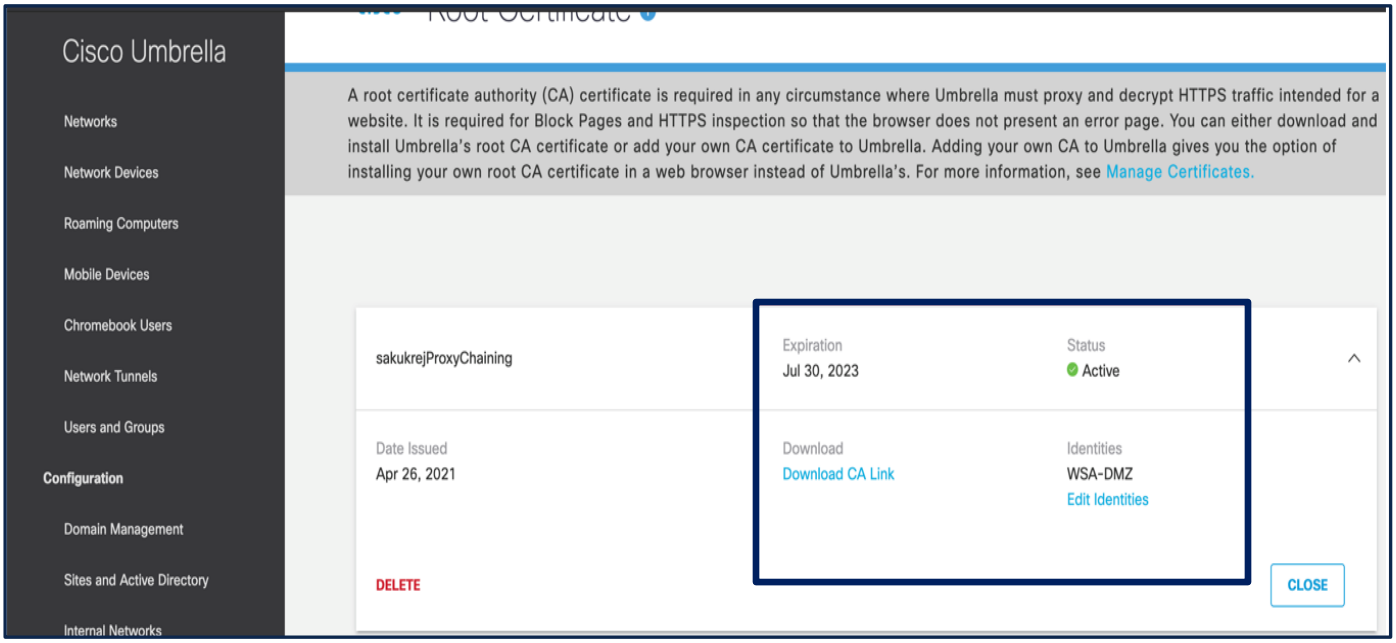


Figure 2 – CA Signed Certificate

© 2021 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

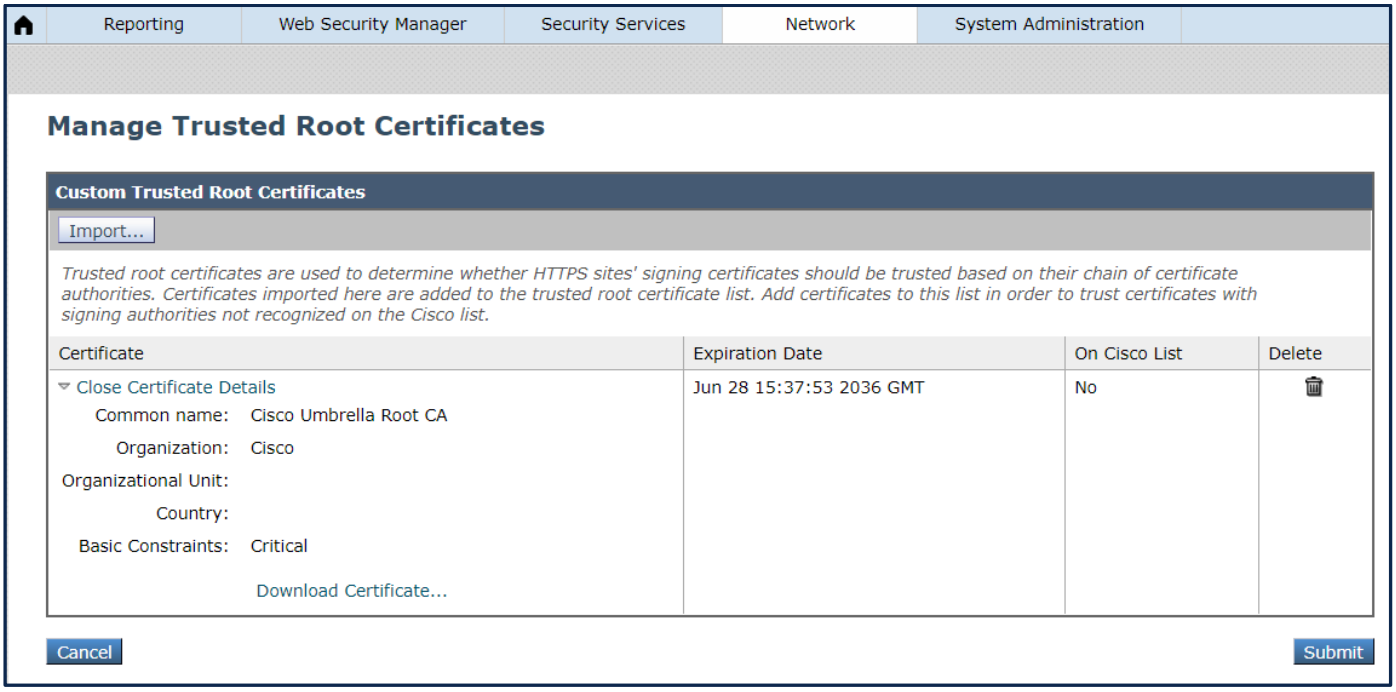
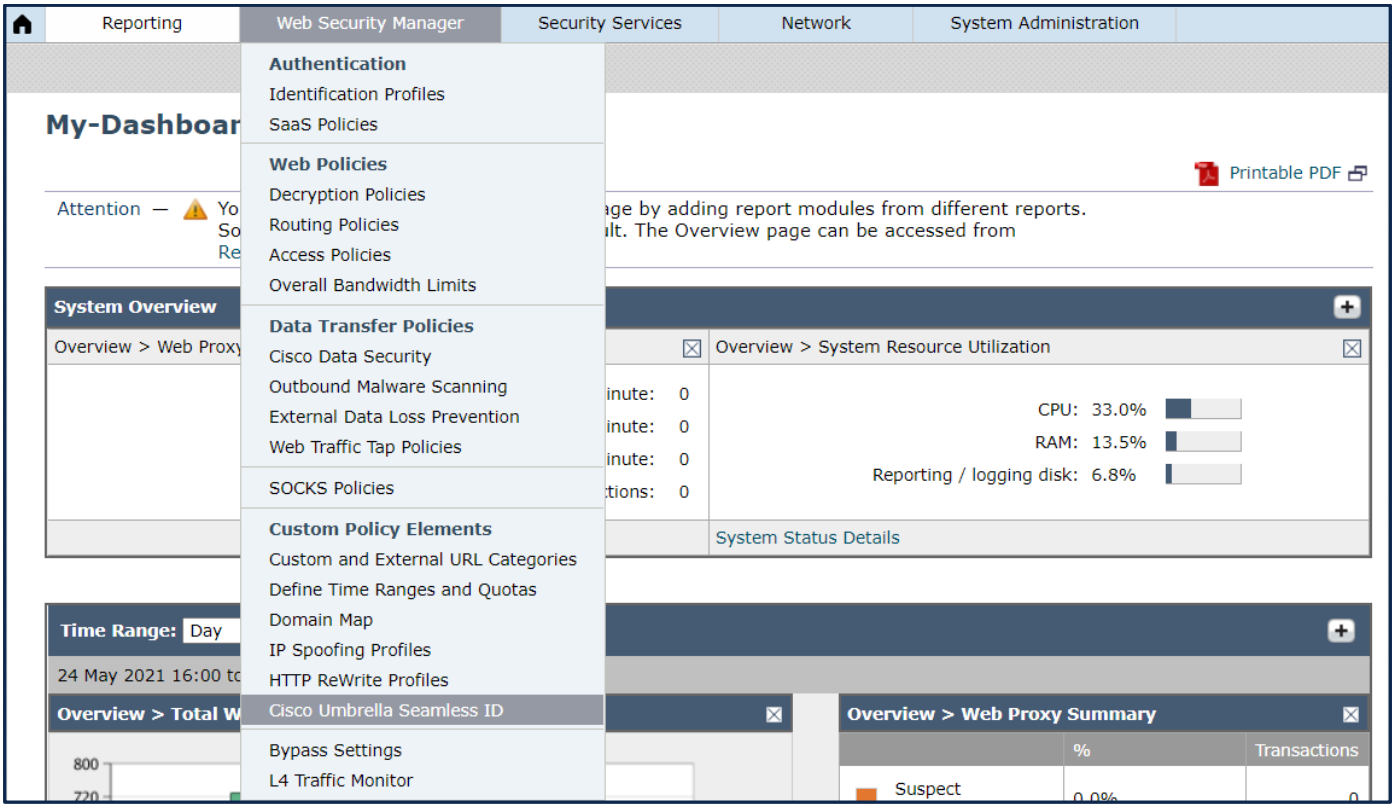


Figure 3 - Trusted Root Certificate

3. To configure the Seamless ID feature on the WSA, navigate to **Web Security Manager > Cisco Umbrella Seamless ID**



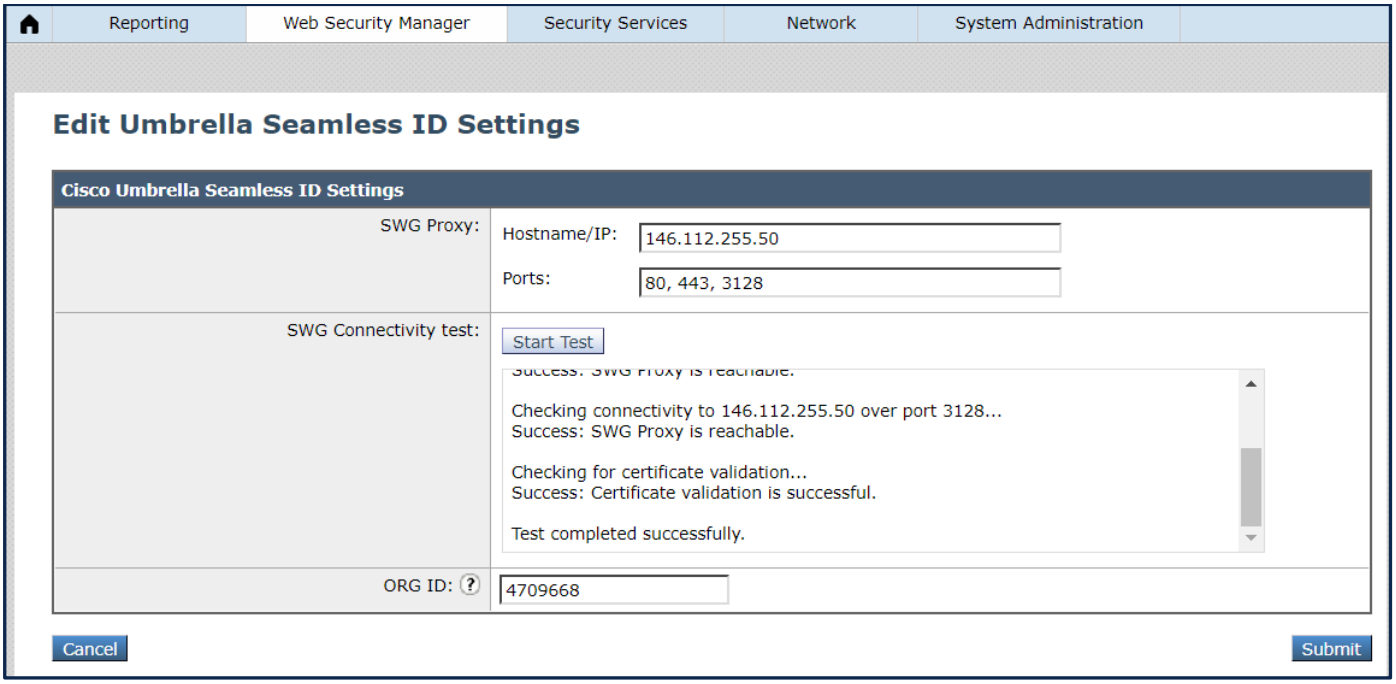
© 2021 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

4. Configure the details as shown below. You'll find the required information once you have logged into your organization's Umbrella portal.

The org id is unique to your organization and is used by Umbrella to recognize traffic coming from users in your organization to apply policies accordingly. Log into http://dashboard.umbrella.com, which redirects to "`dashboard.umbrella.com/o/xxxxxxx/#/overview`" *once logged in.* Please note that **"xxxxxxx"** indicates the org-id, a 7-digit number. Use org-id to configure your WSA to communicate with Umbrella.

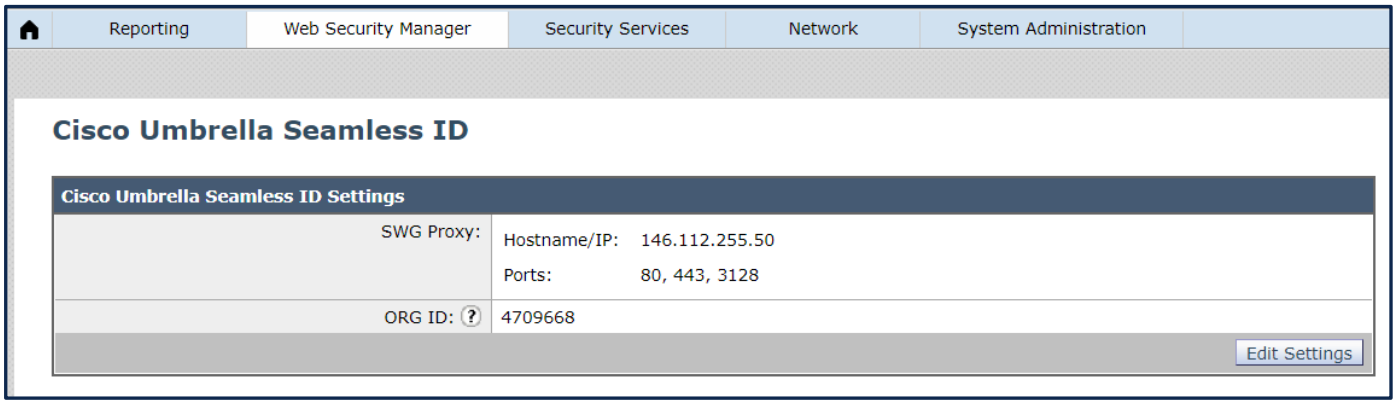
Please refer to https://docs.umbrella.com/umbrella-user-guide/docs/manage-proxy-chaining for additional details. The WSA allows configuring 6 unique ports to communicate with Umbrella for redundancy and segregating traffic on Umbrella.

Note: Currently, Umbrella supports only 3 ports, as shown below.

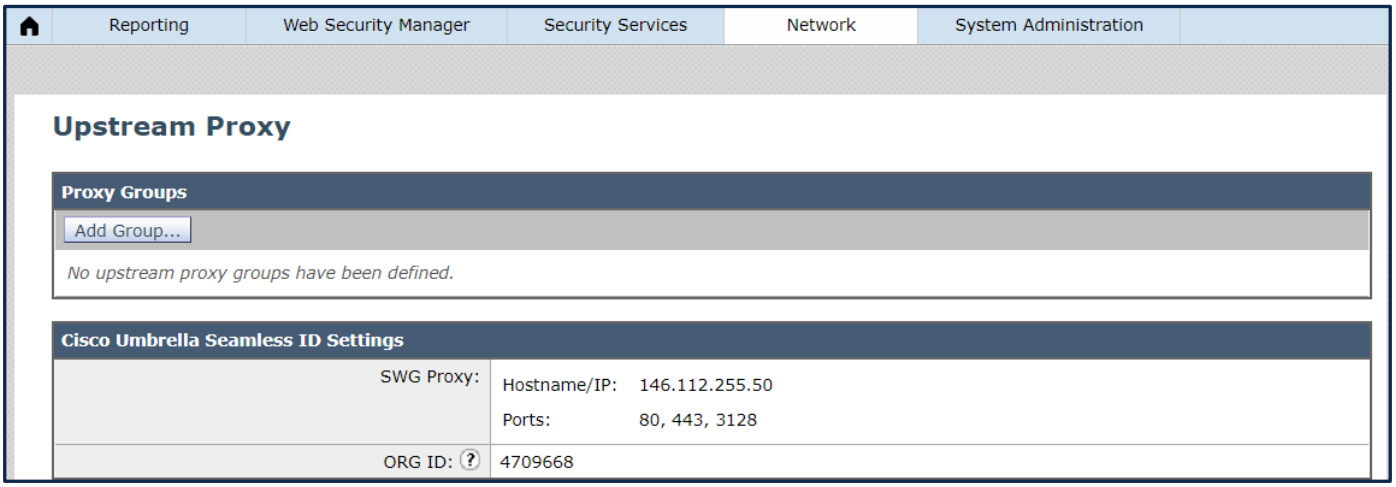


© 2021 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Clicking on the Start Test button tests the connectivity between the WSA and Umbrella by trying to reach the IP address/Hostname configured for each port number provided and validate the certificate to ensure connectivity, and that all the services are up and running. Please submit and commit the changes.

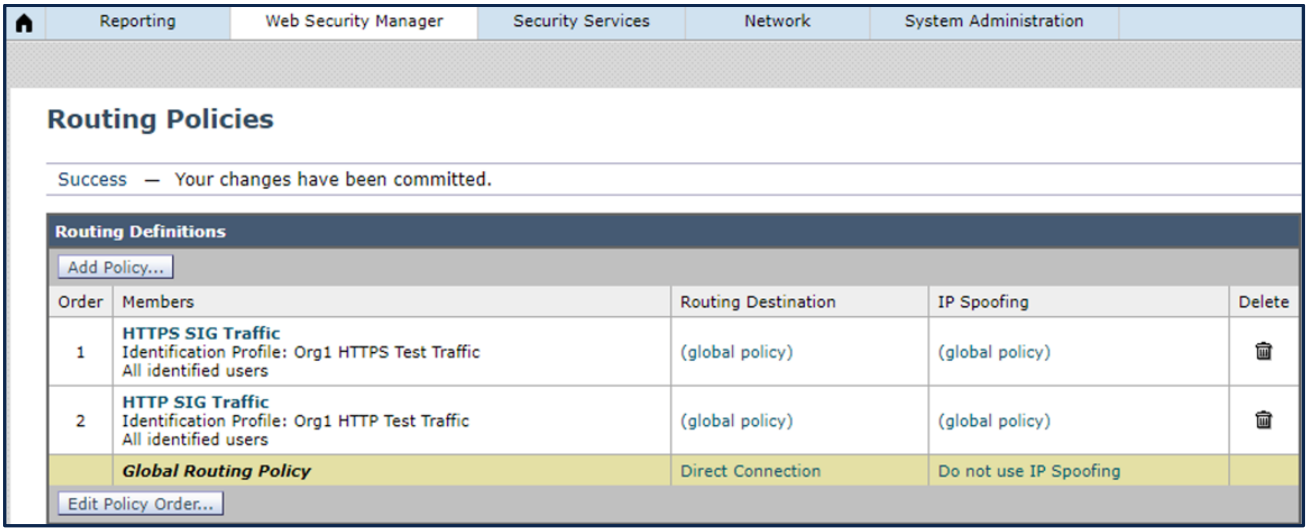


5. Once the Umbrella settings are configured as shown above, the WSA populates Umbrella as an upstream proxy **Network > Upstream Proxy**.

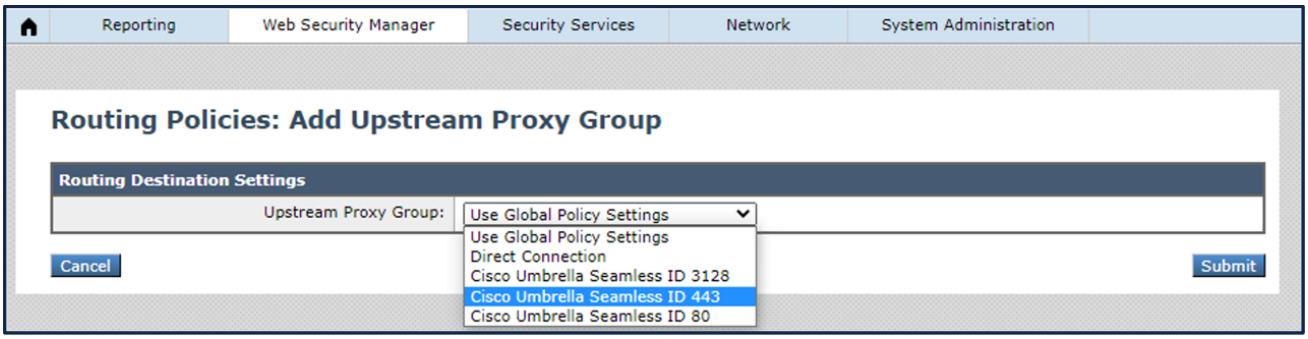


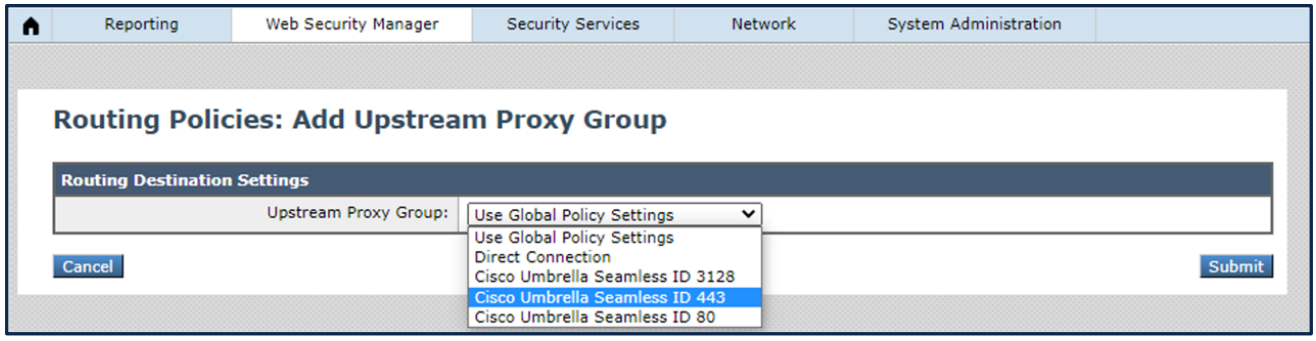
6. To route traffic from the WSA to Umbrella, choose Umbrella as the upstream proxy under **Web Security Manager > Routing Policies**. Change the Routing Destination to one of the populated Umbrella Policies.

© 2021 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

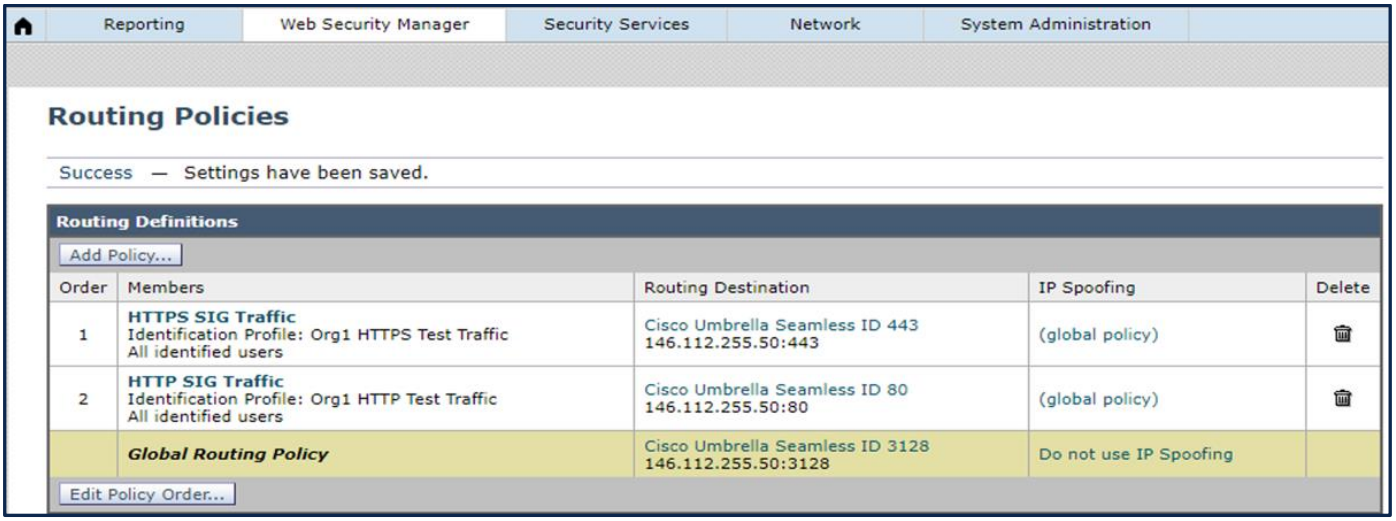


As shown below, the Umbrella policies are populated corresponding to the port numbers configured in Step 4.





© 2021 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

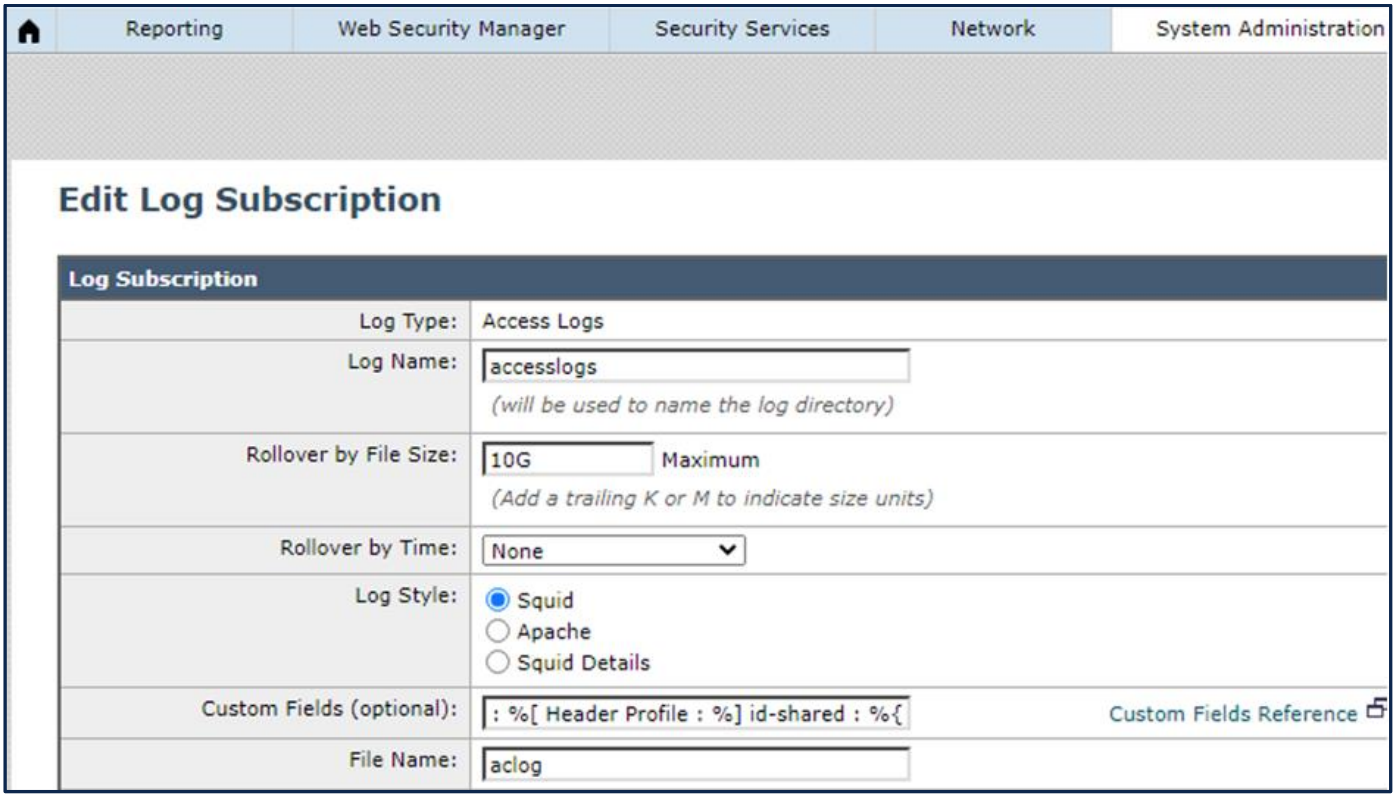


Logging:

Special Format specifiers have been introduced to represent information being shared with Umbrella, as shown below:

Logs name	Description
Access Logs	To check if the id-sharing headers are added for a given request optional formatter “%{“ in accesslogs is introduced.
Auth Logs	Auth logs will log the event when the OrgID is configured on WSA and as identified by SIG for the network traffic doesn’t match.

© 2021 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.



The access log below indicates that the request was processed by Umbrella, and the Identity information for this user that was shared with Umbrella is represented by **"ID_SHARED."**

```
1621509856.915 387 192.168.104.103 TCP_MISS_SSL/200 132 CONNECT
tunnel://edition.cnn.com:443/ "DC1\testuser123@AD" DEFAULT_PARENT/146.112.255.50 -
DECRYPT_WEBCAT_7-Org1_Decryption_Policy-Org1_HTTPS_Test_Traffic-NONE-NONE-NONE-
HTTPS_SIG_Traffic-NONE <"IW_news",2.0,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","-",-,-
,"IW_news",-,"-","News","-","Unknown","Unknown","-","-",2.73,0,-,"-","-",-,"-",-,-,"-","-
",-,-,"-",-,-> - - - NTLMSSP User-Agent : "curl/7.68.0" IP Spoofing Profile : - Header
Profile : None id-shared : ID_SHARED
```

The access log below indicates that the request below was processed by Umbrella however, no Identity information for this user was shared with Umbrella as is represented by **"-"** in the place holder for the format specifier for id sharing.

```
1621509859.222 2305 192.168.104.103 TCP_MISS_SSL/200 1122223 GET
https://edition.cnn.com:443/ "DC1\testuser123@AD" DEFAULT_PARENT/146.112.255.50
text/html DEFAULT_CASE_12-Org1_Access_Policy-Org1_HTTPS_Test_Traffic-NONE-NONE-
NONE-HTTPS_SIG_Traffic-NONE <"IW_news",2.0,1,"-",0,0,0,1,"-",-,-,-,"-",1,-,"-","-
",-,-,"IW_news",-,"Unknown","News","-","Unknown","Unknown","-","-",3894.92,0,-
,"Unknown","-",1,"-",-,-,"-","-",-,-,"-",-,-> - - - NTLMSSP User-Agent :
"curl/7.68.0" IP Spoofing Profile : - Header Profile : None id-shared : -
```

© 2021 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

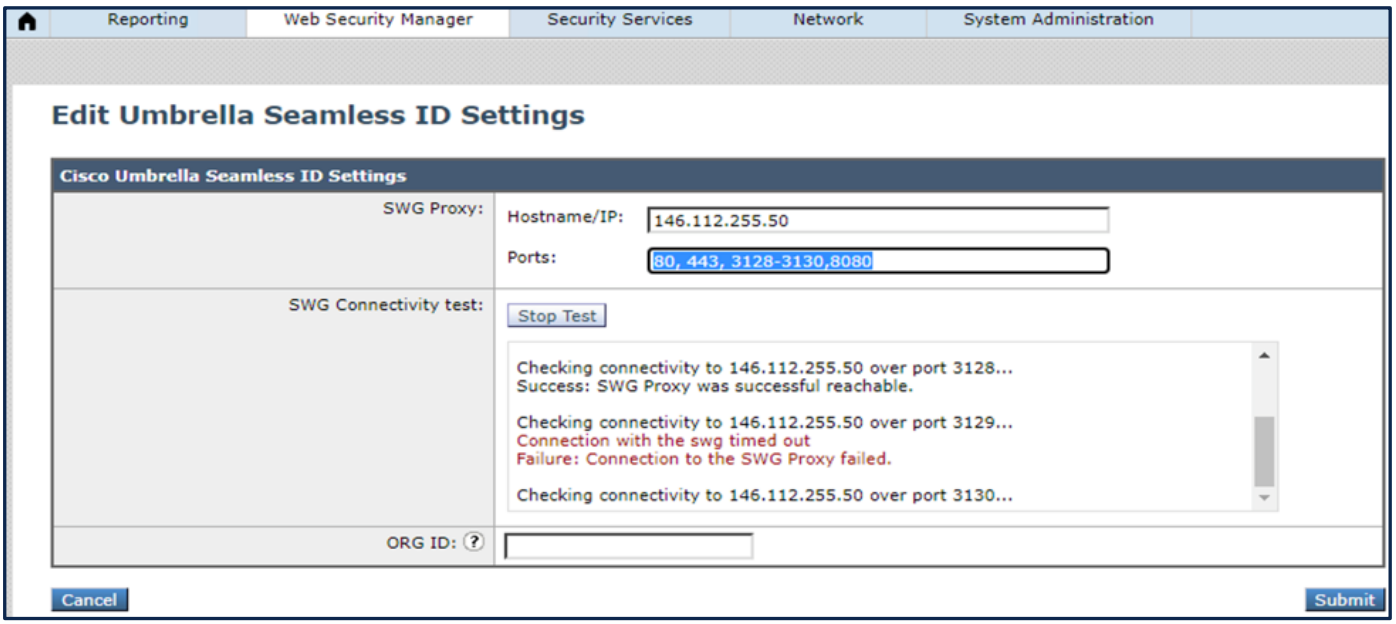
Troubleshooting:

To verify the ID Sharing with Cisco Umbrella is functioning:

1. Check the access logs for the DEFAULT_PARENT, and the routing policy should match the URL Web category the user is trying to access.

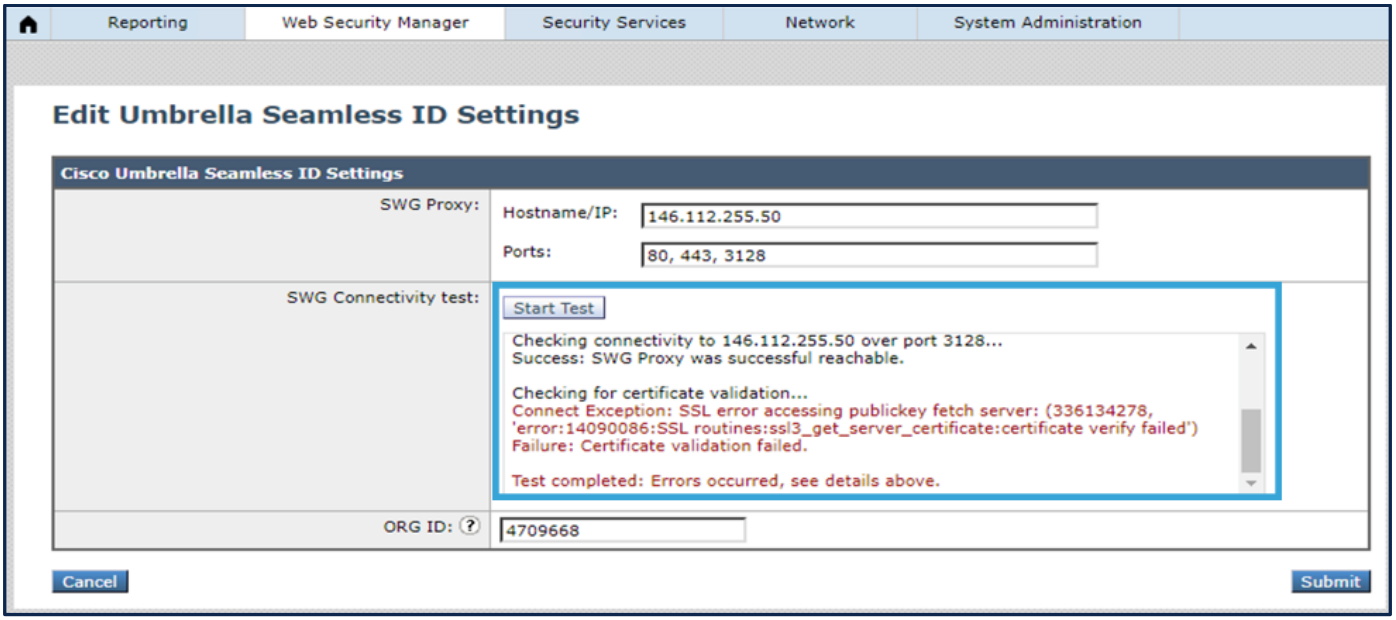
2. Currently, Umbrella only listens on ports 80, 443, and 3128 for HTTP and HTTPS traffic. Port 3128 needs to be manually enabled by Umbrella support at umbrella-support@cisco.com.

3. Currently, SIG listens on port 80 for HTTP traffic, port 443 for HTTPS traffic, and port 3128 for both HTTP and HTTPS traffic. When Umbrella is not listening on port 3129, the reachability test fails as shown below:

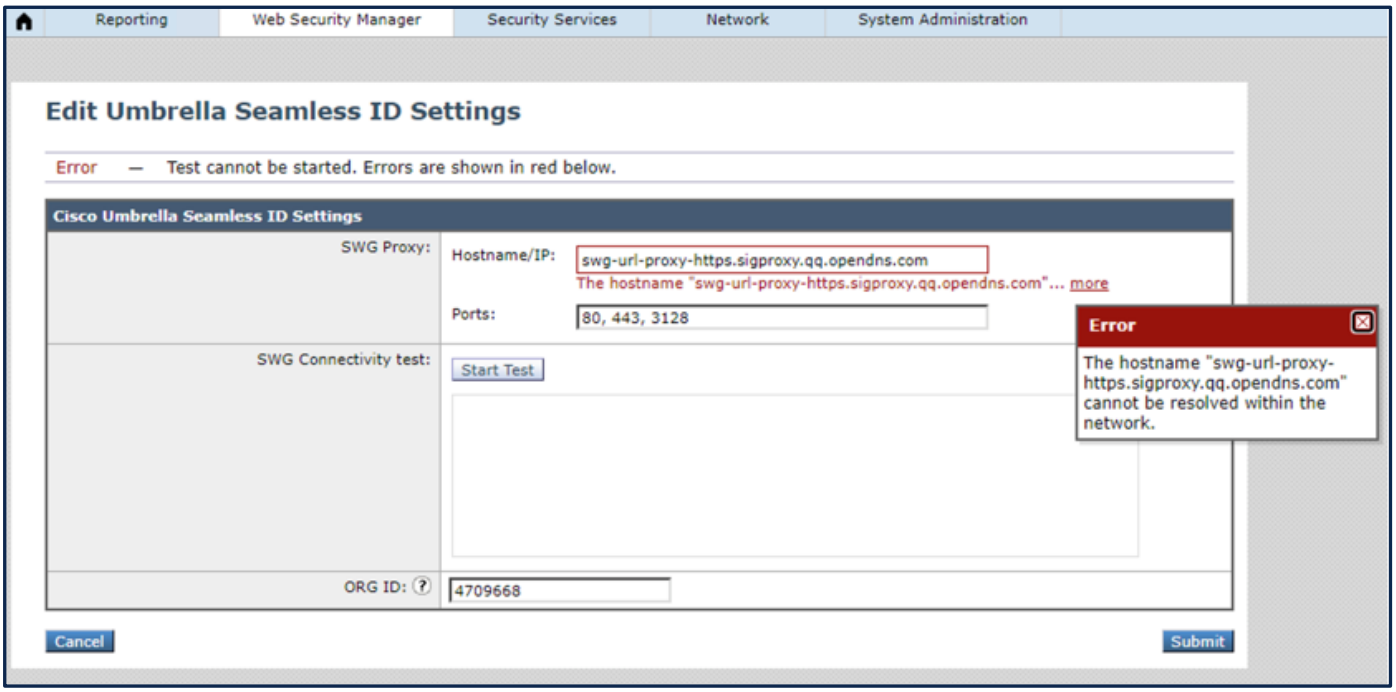


4. The Root / Custom signed certificate of the Umbrella SWG should be imported first on the WSA, or the certificate validation will fail as shown below:

© 2021 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

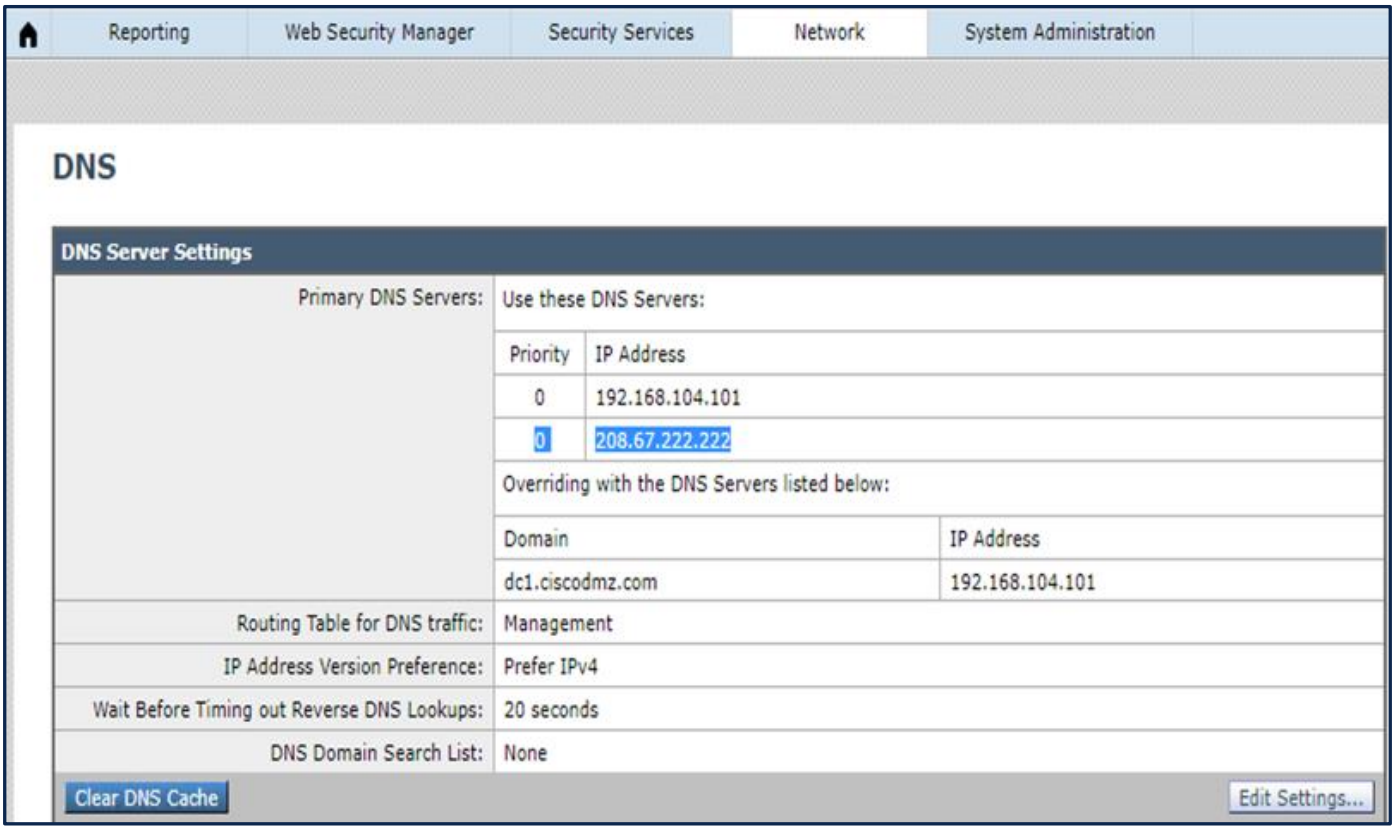


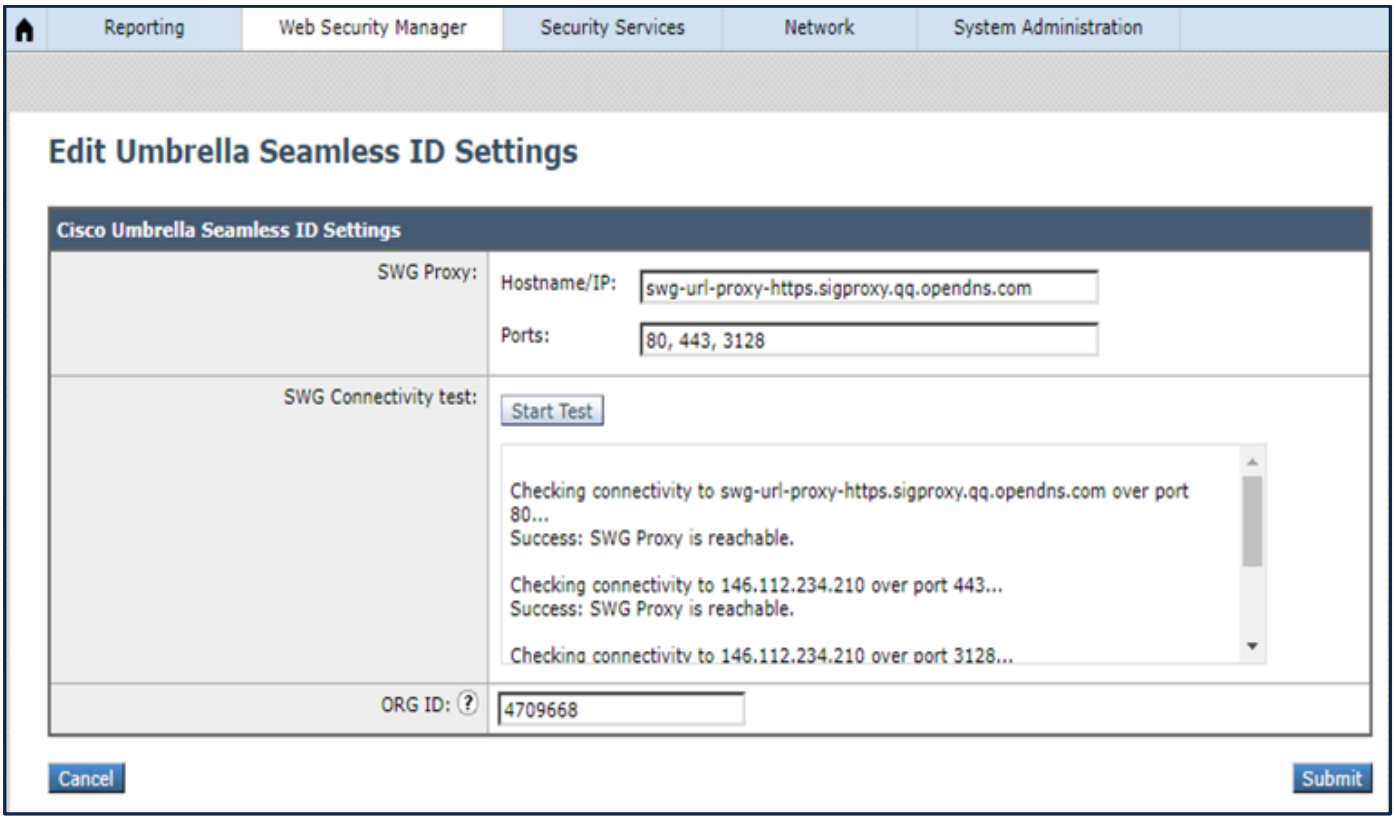
5. The FQDN configured for SWG proxy must be resolvable by the WSA, or an error occurs as shown below:



© 2021 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

To clear this error, configure OpenDNS as the DNS server on the WSA under **Network > DNS**.

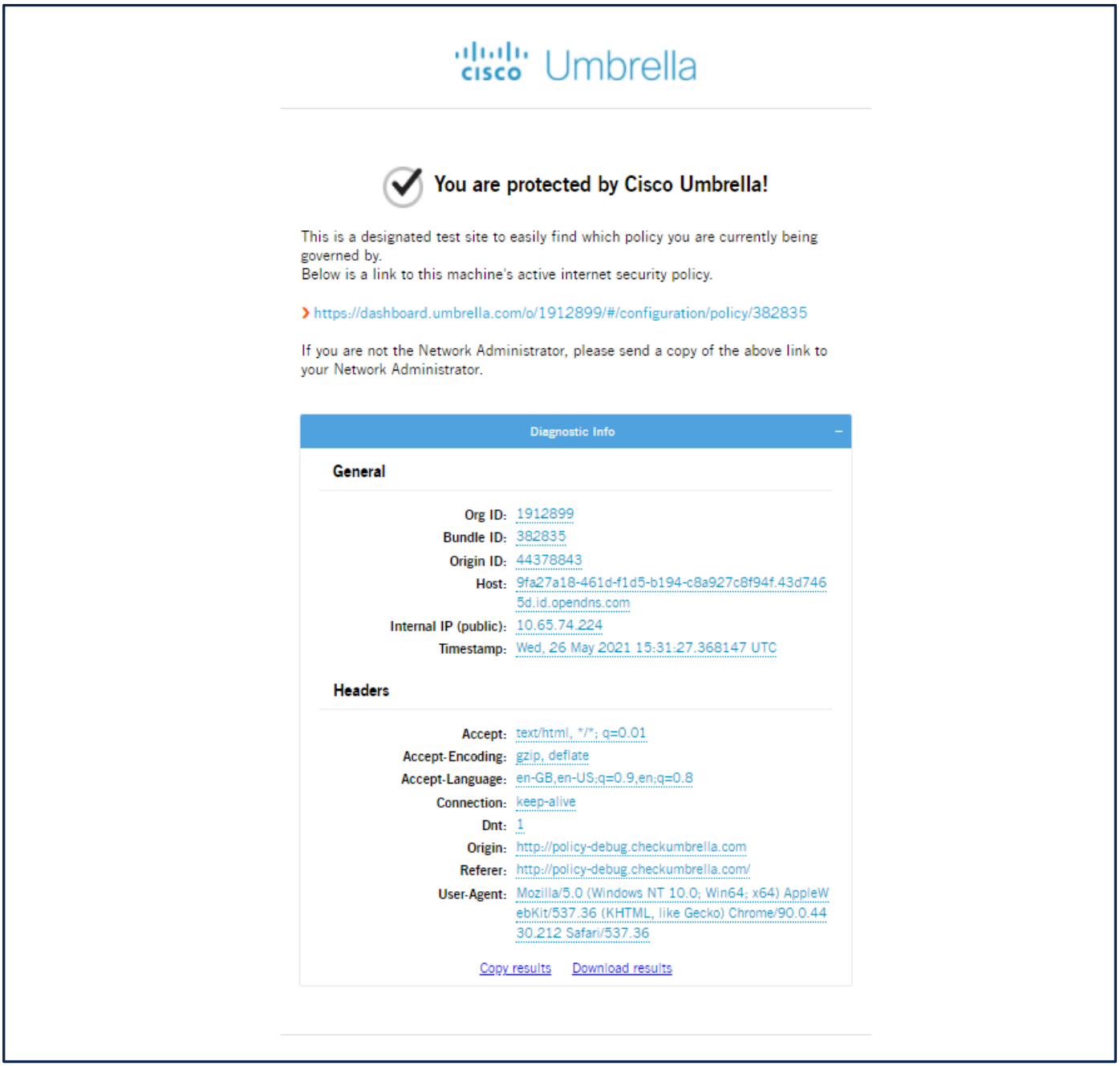




© 2021 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

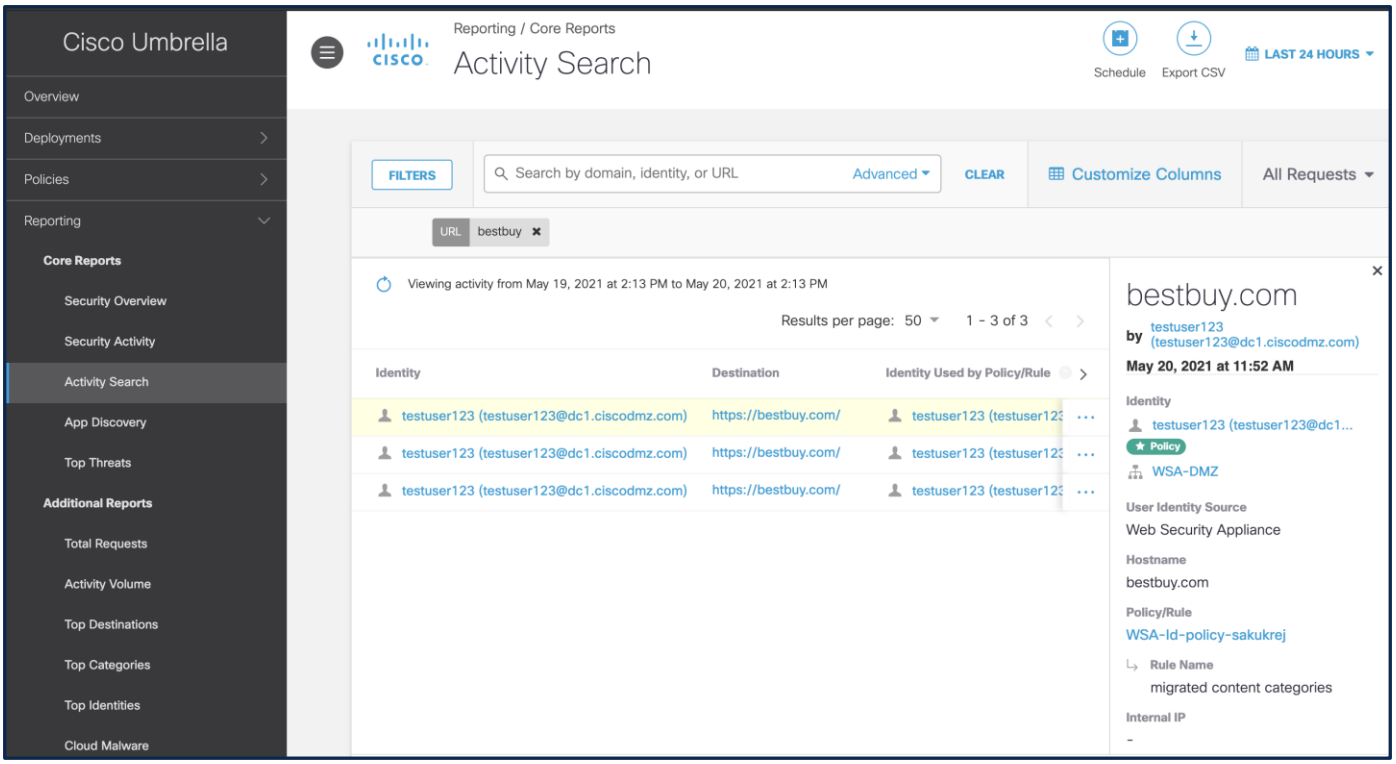
Umbrella:

1. Use the http://policy-debug.checkumbrella.com URI to check the applied end-user web policy, which returns the Web-Policy, OrgID, and User-Info / Type.



© 2021 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

2. From the Umbrella Dashboard, check the Umbrella Reporting > Activity Search to determine if the user-type is Remote, a tunnel user (i.e., AnyConnect users) or a WSA authenticated user.



For more information on Umbrella, please refer to https://docs.umbrella.com/umbrella-user-guide/docs/getting-started.

© 2021 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.