# WSA HTTP Header Rewrite

13-April-2021

# Contents

AsyncOS 14.0 is the latest release of Cisco's Web Security Appliance, an enterprise network proxy solution. One of the many features in this release, HTTP Header Rewrite, can be very useful for adding, removing, or even modifying HTTP request headers' content. Use multiple HTTP headers to enhance security, including some well-known or standard HTTP headers, like X-Forwarded-For (XFF) or Via (which displays the Proxy-in-the-network). HTTP headers allow network admins to send the authentication headers containing a username and groups for proxy authentication with Active Directory or Cisco Identity Service Engine (ISE) providing the user identity information.

## Header Rewrite Use Cases

The addition of this feature provides the WSA with the ability to modify HTTP headers as needed. A common use case allows an administrator to authenticate users against the WSA (client-side proxy) and have the WSA forward the authentication headers to the upstream proxy for user Identification using the header information to apply appropriate policies.

## Microsoft Office 365 Tenant Restriction

An administrator may want to allow users access to the organization’s Microsoft 365 applications while preventing access to other organizations’ instances of these applications. With tenant restrictions, organizations can choose the tenants' list that their users can access and specify it in HTTP headers. Azure AD then only grants access to these permitted tenants.

For each incoming request to login.microsoftonline.com, login.microsoft.com, and login.windows.net, the proxy inserts two HTTP headers: Restrict-Access-To-Tenants and Restrict-Access-Context.

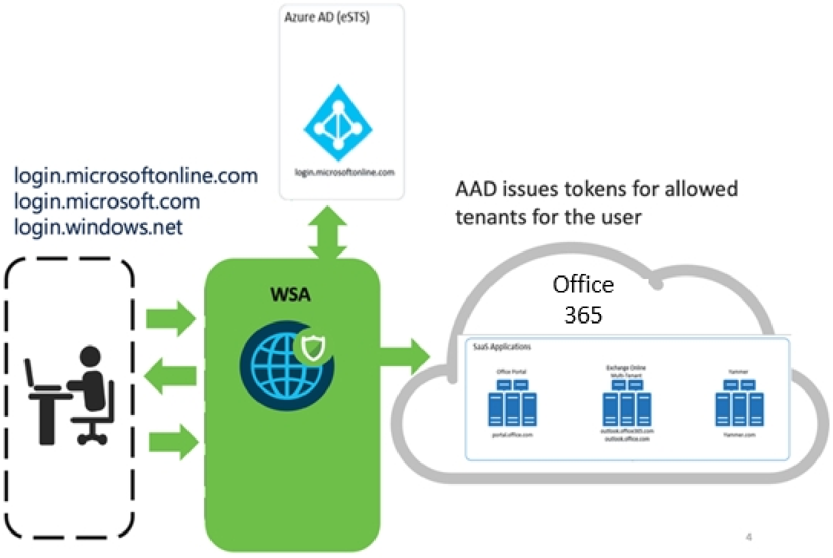


**Figure 1.**

Based on the HTTP packet headers, Azure AD issues security tokens to the allowed users for the permitted tenants only.

## Restrict YouTube Content

For this use case, an administrator may set policies in their network to restrict which YouTube videos are available to employees or students. For this purpose, the YouTube-Restrict header provides options to set strict or moderate rules for users.

To set strict restricted access, insert YouTube-Restrict: **Strict**.
To set moderate restricted access, insert YouTube-Restrict: **Moderate**.

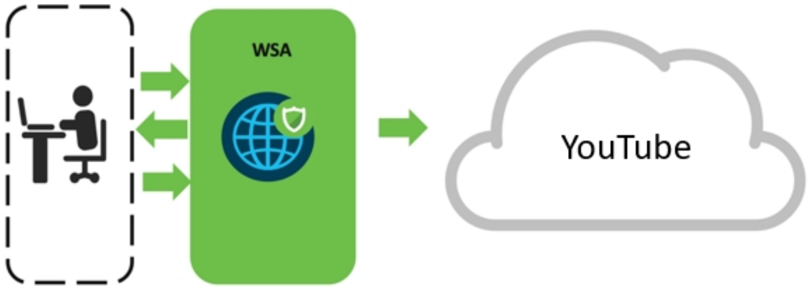


**Figure 2.**

## Restrict Users Access to Google Suite Applications

Like the previous use case, the WSA uses Header Rewrite to block user accounts from accessing specific google services. An administrator can prevent users from signing in to Google services using Google Accounts other than those explicitly specified.

To set restricted access, insert X-GoogApps-Allowed-Domains: mydomain1.com, mydomain2.com

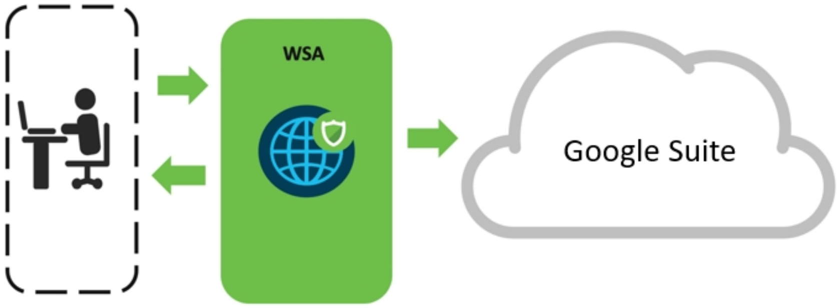


**Figure 3.**
Use the X-GoogApps-Allowed-Domains header to list registered Google Workspace domains.

## Managing SaaS Applications using Azure Tenant Restriction

WSA Header Rewrite works with Azure and other SaaS applications (like Office 365 or Dropbox) to provide user tenant restrictions. Many organizations moving to cloud-based applications, combined with traditional on-premise managed applications that worked with Windows Active Directory (AD), now want their Identity and Access Management (IAM) to work seamlessly for their network users. The increasing demand for secure Single Sign-On (SSO) while retaining traditional Active Directory as the primary IdP (Identity Provider) has many enterprises moving towards Microsoft Azure Active Directory as a cloud-based IAM.

Domain user permissions present a more significant challenge for organizations. As a result, Microsoft Azure restricts enterprise user access and user authentication using Azure Active Directory. The Restrict-Access-To-Tenants HTTP request header takes advantage of these restrictions by using a comma-separated list of tenants to allow user access. The Restrict-Access-Context header uses a single directory ID value to declare the tenant setting the tenant restrictions.

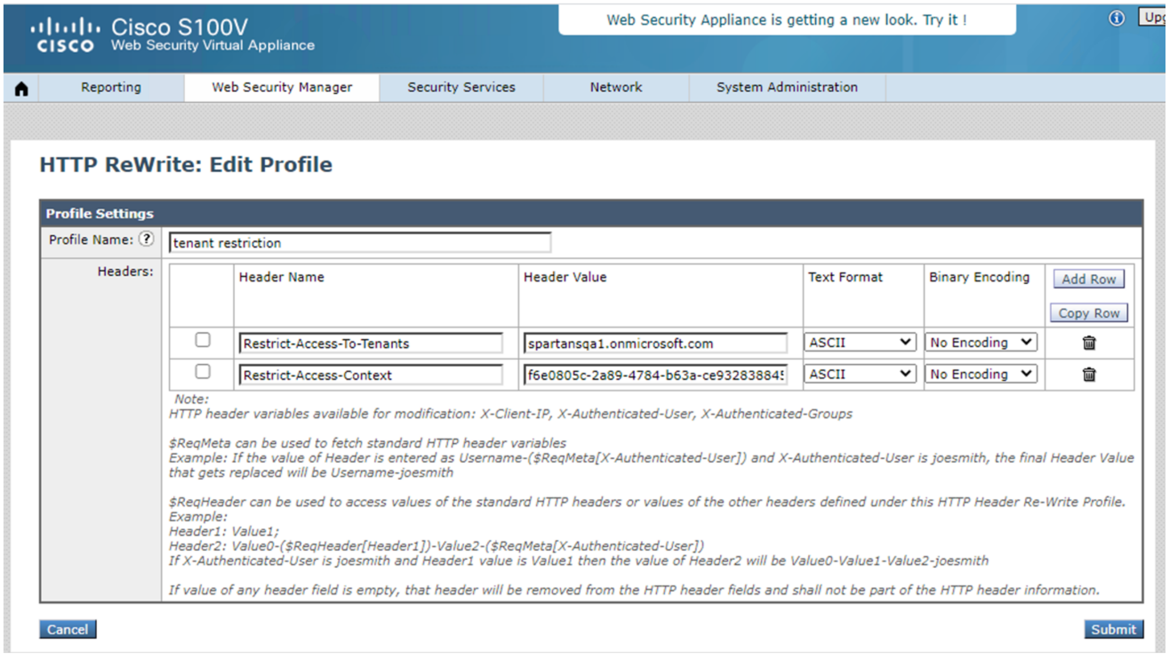
## Configuring HTTP Rewrite

Below provides step-by-step guidance on configuring the WSA to restrict enterprise domain users access to SaaS applications:

**Step 1.** In the WSA UI, navigate to Web Security Manager > HTTP Rewrite Profiles and click on Add HTTP Rewrite Profile HTTP Rewrite Profiles

Enter a Profile Name and add these two headers:

**Restrict-Access-To-Tenants and Restrict-Access-Context**



HTTP ReWrite: Edit Profile

| Profile Settings | |
|---|---|
| Profile Name: ? | tenant restriction |
| Headers: | |

| | Header Name | Header Value | Text Format | Binary Encoding | Add Row<br>Copy Row |
|---|---|---|---|---|---|
| □ | Restrict-Access-To-Tenants | spartansqa1.onmicrosoft.com | ASCII | No Encoding | 🗑 |
| □ | Restrict-Access-Context | f6e0805c-2a89-4784-b63a-ce93283884! | ASCII | No Encoding | 🗑 |

*Note:*
*HTTP header variables available for modification: X-Client-IP, X-Authenticated-User, X-Authenticated-Groups*

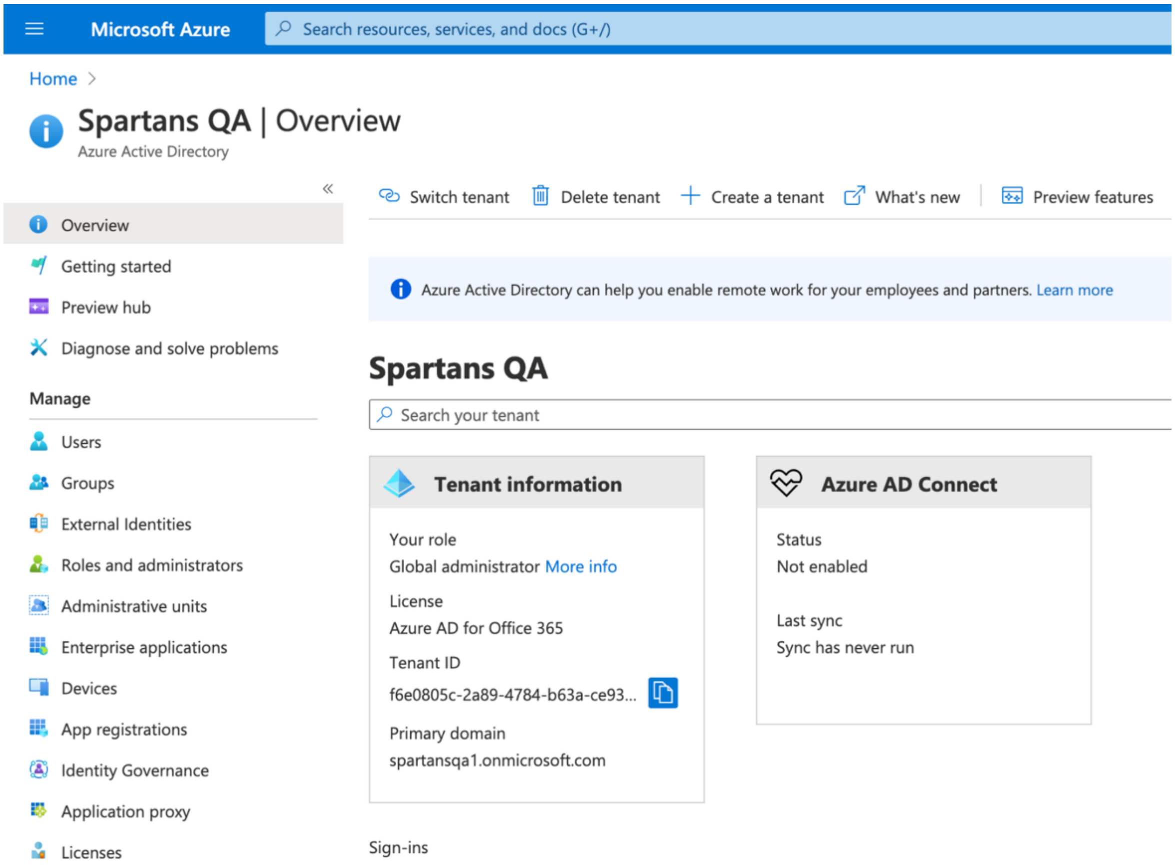
*$ReqMeta can be used to fetch standard HTTP header variables*
*Example: If the value of Header is entered as Username-($ReqMeta[X-Authenticated-User]) and X-Authenticated-User is joesmith, the final Header Value that gets replaced will be Username-joesmith*

*$ReqHeader can be used to access values of the standard HTTP headers or values of the other headers defined under this HTTP Header Re-Write Profile.*
*Example:*
*Header1: Value1;*
*Header2: Value0-($ReqHeader[Header1])-Value2-($ReqMeta[X-Authenticated-User])*
*If X-Authenticated-User is joesmith and Header1 value is Value1 then the value of Header2 will be Value0-Value1-Value2-joesmith*

*If value of any header field is empty, that header will be removed from the HTTP header fields and shall not be part of the HTTP header information.*

**Figure 4.**

**Step 2.** Refer to the Azure Tenant's dashboard for the Restrict-Access-To-Tenants and Restrict-Access-Context.



Spartans QA | Overview

Azure Active Directory

Azure Active Directory can help you enable remote work for your employees and partners. Learn more

Spartans QA

Tenant information

Your role
Global administrator More info

License
Azure AD for Office 365

Tenant ID
f6e0805c-2a89-4784-b63a-ce93...

Primary domain
spartansqa1.onmicrosoft.com

Azure AD Connect

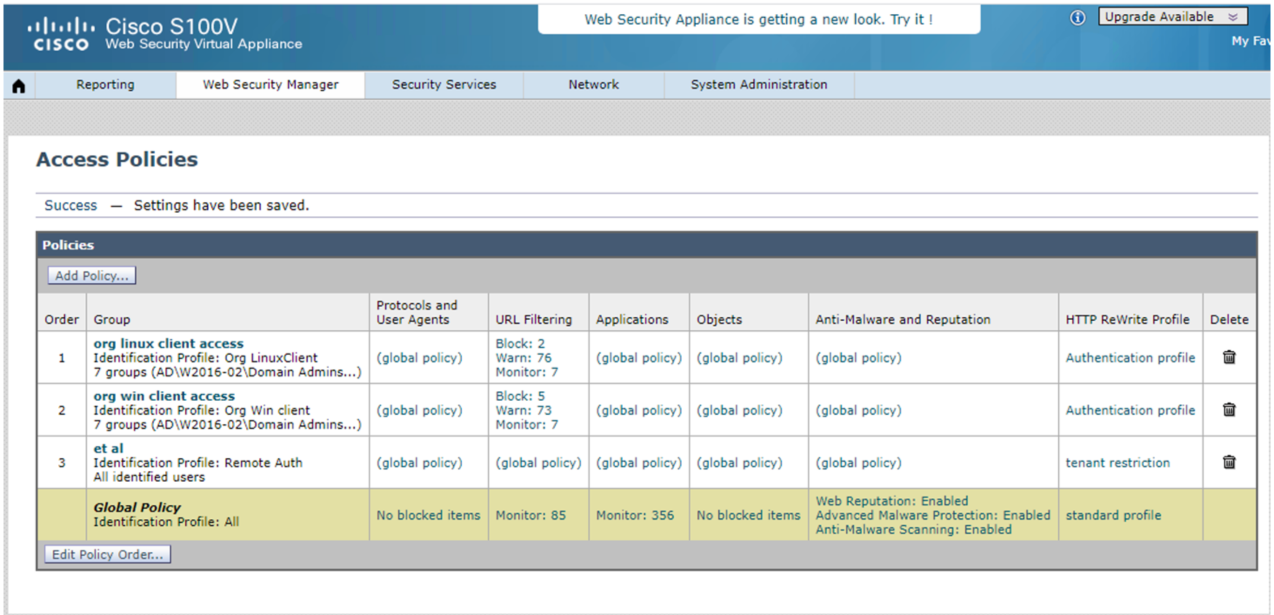
Status
Not enabled

Last sync
Sync has never run

**Figure 5.**

**Step 3.** Next, ensure the Security Services > HTTPS Proxy is enabled. Verify Web Security Manager > Decryption Policies is set to either decrypt or monitor for Microsoft domains or your enterprise application gateways. You can use Microsoft Office 365 feeds and custom categories on the WSA for Microsoft-specific URIs.

**Step 4.** Navigate to Web Security Manager > Access Policies. Add a new access policy for the SaaS, Computers and Security, Office 365 based feeds, or Custom categories and assign the HTTP Rewrite profile to this access policy.



Access Policies

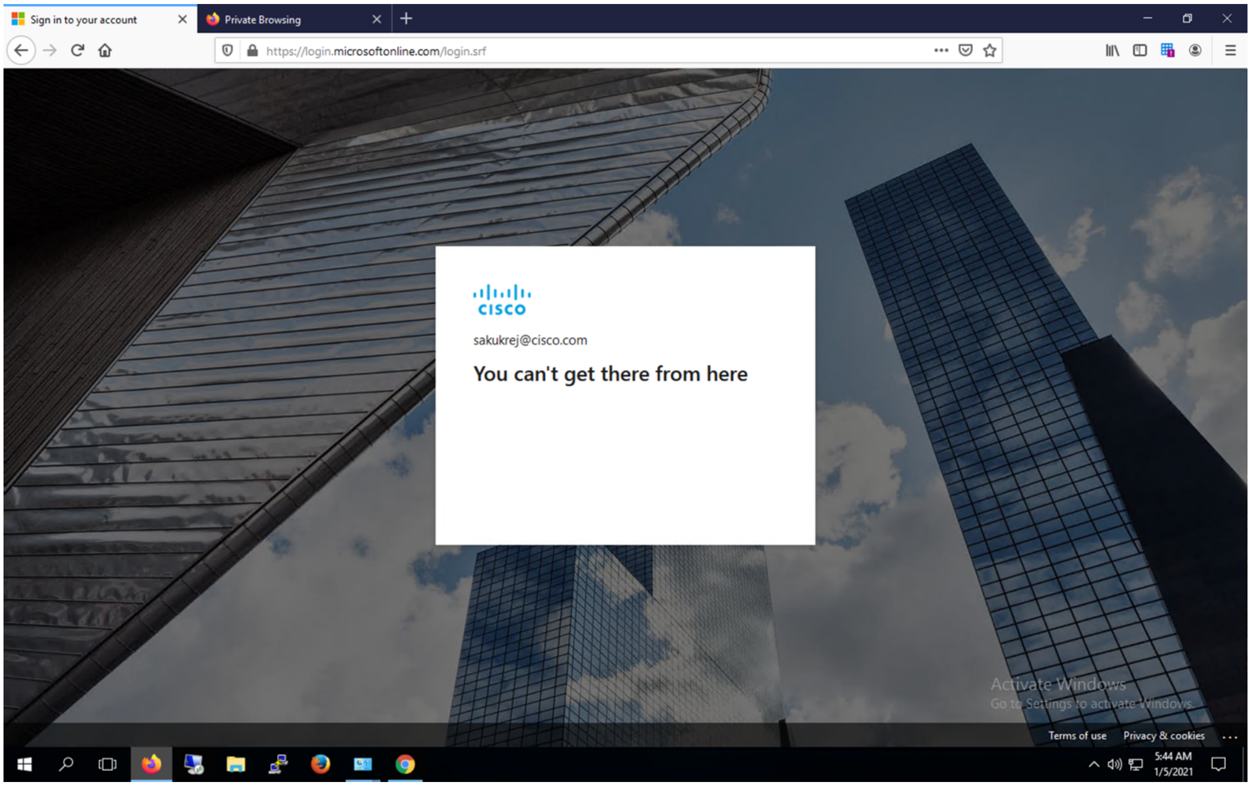
Success — Settings have been saved.

Policies

| Order | Group | Protocols and User Agents | URL Filtering | Applications | Objects | Anti-Malware and Reputation | HTTP ReWrite Profile | Delete |
|---|---|---|---|---|---|---|---|---|
| 1 | **org linux client access**<br>Identification Profile: Org LinuxClient<br>7 groups (AD\W2016-02\Domain Admins...) | (global policy) | Block: 2<br>Warn: 76<br>Monitor: 7 | (global policy) | (global policy) | (global policy) | Authentication profile | 🗑 |
| 2 | **org win client access**<br>Identification Profile: Org Win client<br>7 groups (AD\W2016-02\Domain Admins...) | (global policy) | Block: 5<br>Warn: 73<br>Monitor: 7 | (global policy) | (global policy) | (global policy) | Authentication profile | 🗑 |
| 3 | **et al**<br>Identification Profile: Remote Auth<br>All identified users | (global policy) | (global policy) | (global policy) | (global policy) | (global policy) | tenant restriction | 🗑 |
|  | ***Global Policy***<br>Identification Profile: All | No blocked items | Monitor: 85 | Monitor: 356 | No blocked items | Web Reputation: Enabled<br>Advanced Malware Protection: Enabled<br>Anti-Malware Scanning: Enabled | standard profile |  |

**Figure 6.**

To test if the defined Azure AD users can only access your enterprise applications, try logging in with any other account that is not part of Azure AD. Access should be blocked as shown below:

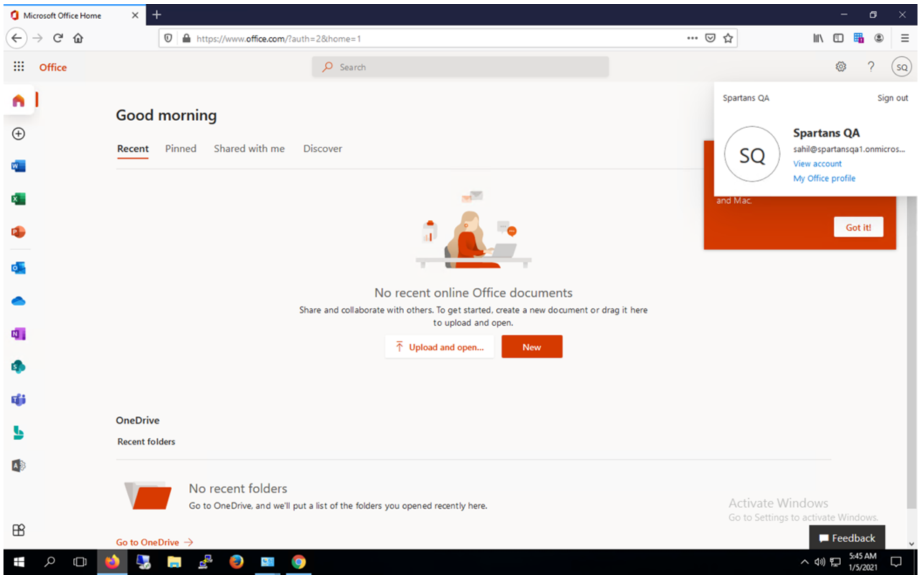


sakukrej@cisco.com

You can't get there from here

**Figure 7.**

Use an enterprise domain user account to verify you can successfully login to your organization’s Office 365 tenant.



No recent online Office documents

Share and collaborate with others. To get started, create a new document or drag it here to upload and open.

No recent folders

Go to OneDrive, and we'll put a list of the folders you opened recently here.

**Figure 8.**

In conclusion, the WSA Header Rewrite feature enables the ability to insert or remove standard or custom headers into HTTP packets as they pass through the WSA to help with various use cases beneficial to most organizations.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA 05/21