Allowed List of Specific URLs

- Allowed lists of specific URLs, on page 1
- Add URL to allowed list, on page 1
- Portal resolving to multiple IP addresses, on page 3
- Verify URLs on the allowed list, on page 4

Allowed lists of specific URLs

An allowed list of specific URLs is a wireless controller feature that

- lets you add URLs to a list on the controller or access point so designated sites remain accessible
- enables web authentication use cases such as captive portals and walled gardens, and
- allows users to reach permitted sites before authenticating, even without full internet access.

Additional reference information

You do not need to authenticate to access URLs in the allowed list. If you try to reach a site not in the allowed list, you are redirected to the login page.

Accessing a support site

If "support.example.com" is added to the allowed list, users can access this site for help or information prior to logging into the network.

Add URL to allowed list

To configure a URL filter that allows specific URLs while blocking others.

This procedure is used in network environments where URL filtering is necessary to control access to web resources.

Before you begin

Ensure you have administrative access to the device and that URL filtering is supported.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the URL filter profile.

Example:

```
Device(config)# urlfilter list url-allowedlist-nbn
```

Step 3 Set the action for the URL filter list.

Example:

```
Device(config-urlfilter-params)# action permit
```

Configures the list as an allowed list, and the **deny** command configures the list as a blocked list.

Step 4 Configure the IP address of the redirect servers to which user requests will be redirected in case of denied requests.

Example:

```
Device(config-urlfilter-params)# redirect-server-ipv4 X.X.X.X
```

Step 5 Configure the URL to be allowed.

Example:

```
Device(config-urlfilter-params)# url www.cisco.com
```

Note **redirect-server-ipv4** and **redirect-server-ipv6** is applicable only in the local mode, specifically in post-authentication. For any further tracking or displaying any warning messages, the denied user request is redirected to the configured server.

But the **redirect-server-ipv4** and **redirect-server-ipv6** configurations do not apply to pre-authentication scenario as you will be redirected to the controller for the redirect login URL for any denied access.

You can associate the allowed URL with the ACL policy in flex profile.

Associating the allowed URL with the ACL policy in flex profile:

```
Device(config)# wireless profile flex default-flex-profile
            Device(config-wireless-flex-profile)# acl-policy user_v4_acl
            Device(config-wireless-flex-profile-acl)# urlfilter list url_allowedlist_nbn
            Device(config-wireless-flex-profile-acl)# exit
            Device(config-wireless-flex-profile)# description "default flex profile"

Device(config)# urlfilter enhanced-list urllist_pre_cwa
                Device(config-urlfilter-enhanced-params)# url url1.dns.com preference 1
action permit
                Device(config-urlfilter-enhanced-params)# url url2.dns.com preference 2
action deny
```

```
                Device(config-urlfilter-enhanced-params)# url url3.dns.com preference 3
action permit

Device(config)# wlan wlan5 5 wlan5
                    Device(config-wlan)#ip access-group web user_v4_acl
                    Device(config-wlan)#no security wpa
                    Device(config-wlan)#no security wpa
                    Device(config-wlan)#no security wpa wpa2 ciphers aes
                    Device(config-wlan)#no security wpa akm dot1x
                    Device(config-wlan)#security web-auth
                    Device(config-wlan)#security web-auth authentication-list default
                    Device(config-wlan)#security web-auth parameter-map global
                    Device(config-wlan)#no shutdown
```

Portal resolving to multiple IP addresses

You can use two IP addresses with the controller. However, the Web Auth Parameter Map allows pre-authentication to only one IP address. If an external portal, such as Cisco Spaces, resolves to multiple IP addresses or other HTTP resources require pre-authentication, you need a URL filter. The URL filter dynamically permits traffic to the configured URLs by snooping DNS requests and adding each resolved IP address to the intercept (redirect) and security (pre-auth) ACLs. This process enables you to access clients when necessary.

Additional information

- For FlexConnect deployments with local switching, apply the URL filter to the client at the AP for DNS snooping to work properly.
- Configuring the Web Auth Parameter Map automatically creates the following ACLs:
  - Redirect or intercept ACL (WA-v4-int): handles URL redirection.
  - Security ACL (WA-sec-): permits pre-auth access for HTTP or HTTPS, DNS, DHCP, and other required services.

Configuration steps for URL filter in FlexConnect profile

If you miss this step, the AP cannot dynamically add IP addresses. Clients may fail to redirect to the portal page when they request a secondary portal IP address.

Note Tip: Use visuals, diagrams, or tables as needed to clarify configuration mapping, ACL lists, or traffic flow.

Associating the allowed URL with the ACL policy in a Flex profile

```
  Device(config)# wireless profile flex default-flex-profile
  Device(config-wireless-flex-profile)# acl-policy WA-v4-<ip> (security ACL)
Device(config-wireless-flex-profile-acl)# urlfilter list url_allowedlist_nbn

  Device(config-wireless-flex-profile-acl)# exit
  Device(config-wireless-flex-profile)# description "default flex profile"
```

Verify URLs on the allowed list

Verify URLs on the Allowed List.

```
Device# show wireless urlfilter summary
Black-list    - DENY
White-list    - PERMIT
Filter-Type   - Specific to Local Mode

URL-List                          ID  Filter-Type  Action   Redirect-ipv4  Redirect-ipv6
-------------------------------------------------------------------------------------------------
url-whitelist                     1    PRE-AUTH     PERMIT   192.0.2.1

Device#

Device# show wireless urlfilter details url-whitelist
List Name..................... : url-whitelist
Filter ID..................... : : 1
Filter Type................... : PRE-AUTH
Action........................ : PERMIT
Redirect server ipv4...... : 192.0.2.1
Redirect server ipv6...... :
Configured List of URLs
   URL....................... : www.example.com
```