Browser-Based Authentication Bypass

The Browser-Based Authentication Bypass feature enables web browsers to bypass authentication methods such as HTTP Basic, Web Authorization Proxy, and Windows NT LAN Manager (NTLM) (passive or explicit). Specific web browsers can be configured for authentication, and other browsers can be configured to bypass authentication.

This module provides information about the feature and how to configure it.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Browser-Based Authentication Bypass

- You must configure at least one of these authentication methods—HTTP Basic, Web Authorization Proxy, or Windows NTLM—with browser-based authentication bypass.
- Use browser-based authentication bypass with the Default User-Group Policy feature.

Information About Browser-Based Authentication Bypass

Browser-Based Authentication Bypass Overview

While using web browsers, as part of the user authentication, a pop-up or dialog box appears in some web browsers. The Browser-Based Authentication Bypass feature helps to bypass this user authentication and thus avoid the authentication pop-ups.

With the Browser-Based Authentication Bypass feature, you can configure web browsers that must be authenticated and browsers that can bypass user authentication. Bypassing is supported for authentication methods such as HTTP Basic, Web Authorization Proxy, and Windows NT LAN Manager (NTLM) (passive or explicit).

The Browser-Based Authentication Bypass feature supports the following web browsers:

- Chrome
- Firefox
- Internet Explorer 8 (IE8)
- IE9
- Safari

A network administrator configures a list of regular expression (regex) patterns in the IP admission module. When the IP admission module receives the HTTP Get request, the module compares the user-agent string in the HTTP header to the regex pattern that the administrator has configured for the bypass method.

The following rules apply to the Browser-Based Authentication Bypass feature:

- If a configured regex pattern does not match the user-agent field, a web browser is authenticated on the basis of the configured web authentication method.
- If a configured regex pattern matches the user-agent field, authentication is bypassed for the web browser and the HTTP traffic goes through to the Cisco Web Security cloud.

How to Configure Browser-Based Authentication Bypass

Configuring Browser-Based Authentication Bypass

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type regex** *regex-map*
4. **pattern** *expression*
5. **exit**
6. **ip admission name** *admission-name* **bypass regex** *regex-map* [**absolute-timer** *minutes*]
7. Perform one of the following tasks:
   - **ip admission name** *admission-name* **ntlm**
   - **ip admission name** *admission-name* **http-basic**
   - **ip admission name** *admission-name* **proxy http**
8. **interface** *type number*
9. **ip admission** *admission-name*
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**parameter-map type regex** *regex-map* **Example:** `Device(config)# parameter-map type regex regex-map1`	Configures a parameter-map type with a regular expression (regex) to match a specific traffic pattern and enters parameter-map type inspect configuration mode.

	Command or Action	Purpose
Step 4	**pattern** *expression* **Example:** `Device(config-profile)# pattern Chrome`	Configures a matching pattern that compares the user-agent field in the HTTP Get request and the regex pattern.
Step 5	**exit** **Example:** `Device(config-profile)# exit`	Exits parameter-map type inspect configuration mode and enters global configuration mode.
Step 6	**ip admission name** *admission-name* **bypass regex** *regex-map* [**absolute-timer** *minutes*] **Example:** `Device(config)# ip admission name rule1 bypass regex regex-map1 absolute-timer 10`	Creates an IP Network Admission Control (NAC) rule to enable browser-based authentication bypass.

Step 7	Perform one of the following tasks:
	• **ip admission name** *admission-name* **ntlm**
	• **ip admission name** *admission-name* **http-basic**
	• **ip admission name** *admission-name* **proxy http**
	
	Example:
	
	`Device(config)# ip admission name rule1 ntlm`
	
	`Device(config)# ip admission name rule1 http-basic`
	
	`Device(config)# ip admission name rule1 proxy http`
		Configures one of the following authentication methods:
		• Windows NT LAN Manager (NTLM)
		• HTTP Basic
		• Web Authorization Proxy

Step 8	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet0/1/0`	Configures an interface and enters interface configuration mode.
Step 9	**ip admission** *admission-name* **Example:** `Device(config-if)# ip admission rule1`	Creates a Layer 3 Network Admission Control (NAC) rule to be applied to the interface.

	Command or Action	Purpose
Step 10	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and enters privileged EXEC mode.

What to Do Next

For any parameter-map change to be reflected, remove and configure the **ip admission name** *admission-name* **bypass regex** *regex-map* [**absolute-timer** *minutes*] command in global configuration mode.

Verifying Browser-Based Authentication Bypass

SUMMARY STEPS

1. **enable**
2. **show ip admission cache**
3. **show ip admission configuration**

DETAILED STEPS

Step 1 **enable**
Enables privileged EXEC mode.

- Enter your password if prompted.

Example:

```
Device> enable
```

Step 2 **show ip admission cache**
Displays the current list of network admission entries and verifies the browser authentication bypass.

Example:

```
Device# show ip admission cache

Client Name N/A, Client IP 172.31.108.123, Port 63142, timeout 60, Time Remaining 60, state ESTAB
(Browser Auth Bypass)
```

Step 3 **show ip admission configuration**
Displays the Network Admission Control (NAC) configuration.

Example:

```
Device# show ip admission configuration

Auth-proxy name webauth-profile
!
browser bypass, regex parameter-map name: reg-map inactivity-time 12 minutes absolute-timer 10 minutes
```

Configuration Examples for Browser-Based Authentication Bypass

Example: Configuring Browser-Based Authentication Bypass

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type regex regex-map1
Device(config-profile)# pattern Chrome
Device(config-profile)# exit
Device(config)# ip admission name rule1 bypass regex regex-map1 absolute-timer 10
Device(config)# ip admission name rule1 ntlm
Device(config)# interface gigabitethernet0/1/0
Device(config-if)# ip admission rule1
Device(config-if)# end
```

Additional References for Browser-Based Authentication Bypass

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases

Related Topic	Document Title
Security commands	• Cisco IOS Security Command Reference: Commands A to C • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • Cisco IOS Security Command Reference: Commands S to Z
Cisco Web Security	"Cisco Web Security" module in the *Security Configuration Guide: Zone-Based Policy Firewall*
Authenticating and authorizing connections	"Configuring Authentication Proxy" module in the *Authentication Proxy Configuration Guide*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for Browser-Based Authentication Bypass

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Browser-Based Authentication Bypass

Feature Name	Releases	Feature Information
Browser-Based Authentication Bypass	15.3(3)M	The Browser-Based Authentication Bypass feature enables web browsers to bypass authentication methods such as HTTP Basic, Web Authorization Proxy, and Windows NTLM (passive or explicit). The following command was introduced: **ip admission name bypass regex**.