

Configure the Remember Me API for PST on Webex Sites Managed via Control Hub

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Verify](#)

[Troubleshoot](#)

Introduction

This document describes how to configure the Remember Me API for integrations with Persistent Session Tokens (PST) when Single Sign On (SSO) is enabled for CI Webex Sites (managed via Webex Control Hub). When SSO is enabled, you can set up PST from your Identity Provider (IdP) so that sessions take longer to expire. For CI Sites, the Webex idbroker does not honor PST by default.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Know your Org ID and get a Bearer Token
- Have Postman installed. You can download the desktop version or the Add-on for Chrome

Note: Navigate to Background Information in order to know how to get a Bearer Token.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

You can find the Org ID in the Webex Control Hub. Access to Control Hub and click on **My Company**.

In order to get a Bearer Token, follow these steps:

Step 1. From Google Chrome, navigate to **admin.webex.com**.

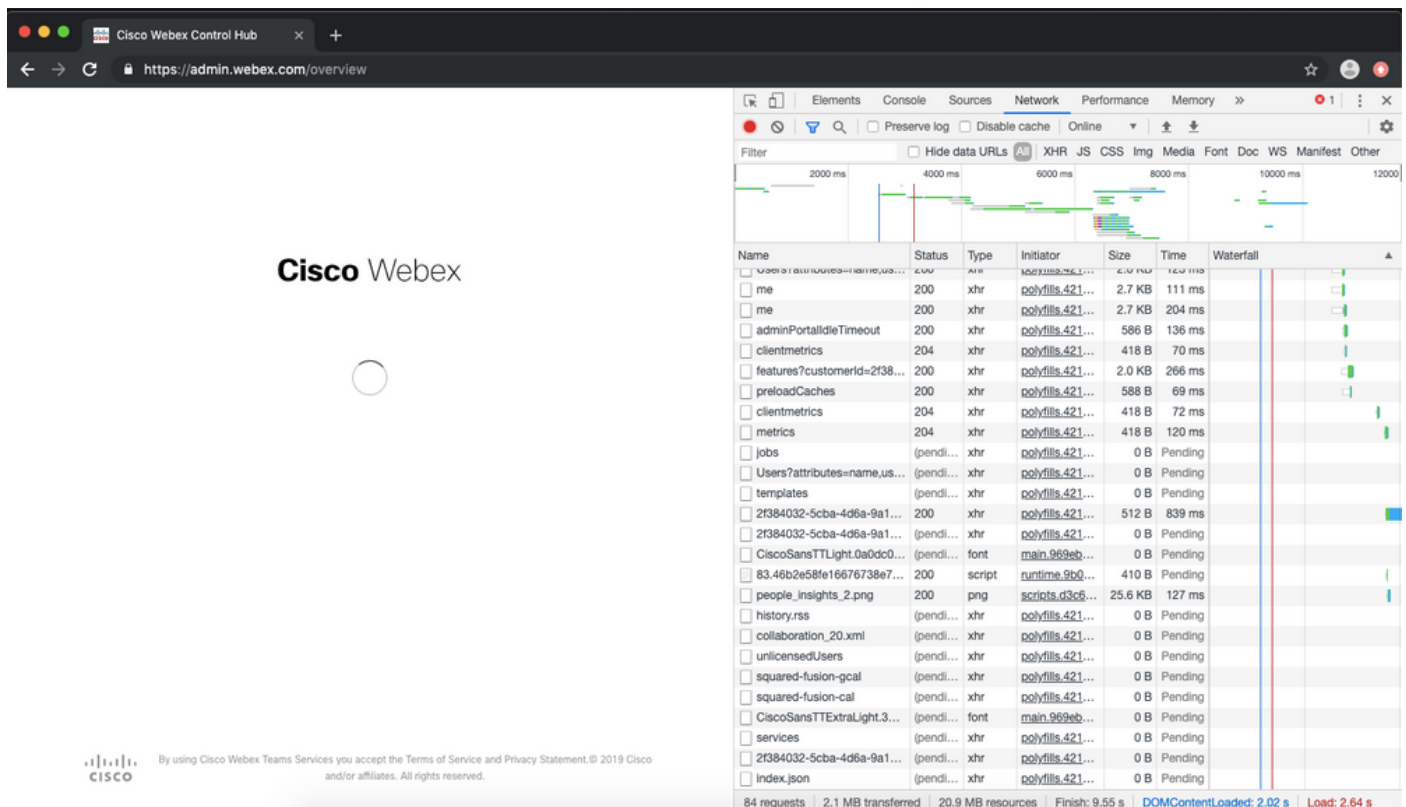
Step 2. At the top-right of your browser window, click the Chrome menu (**⋮**).

Step 3. Select **Tools > Developer Tools**. The Developer Tools window opens as a docked panel at the side or bottom of Chrome.

Step 4. Select the **Network** tab.

Step 5. Log in with your Full Admin account.

This image illustrates Steps 1. to 5.:



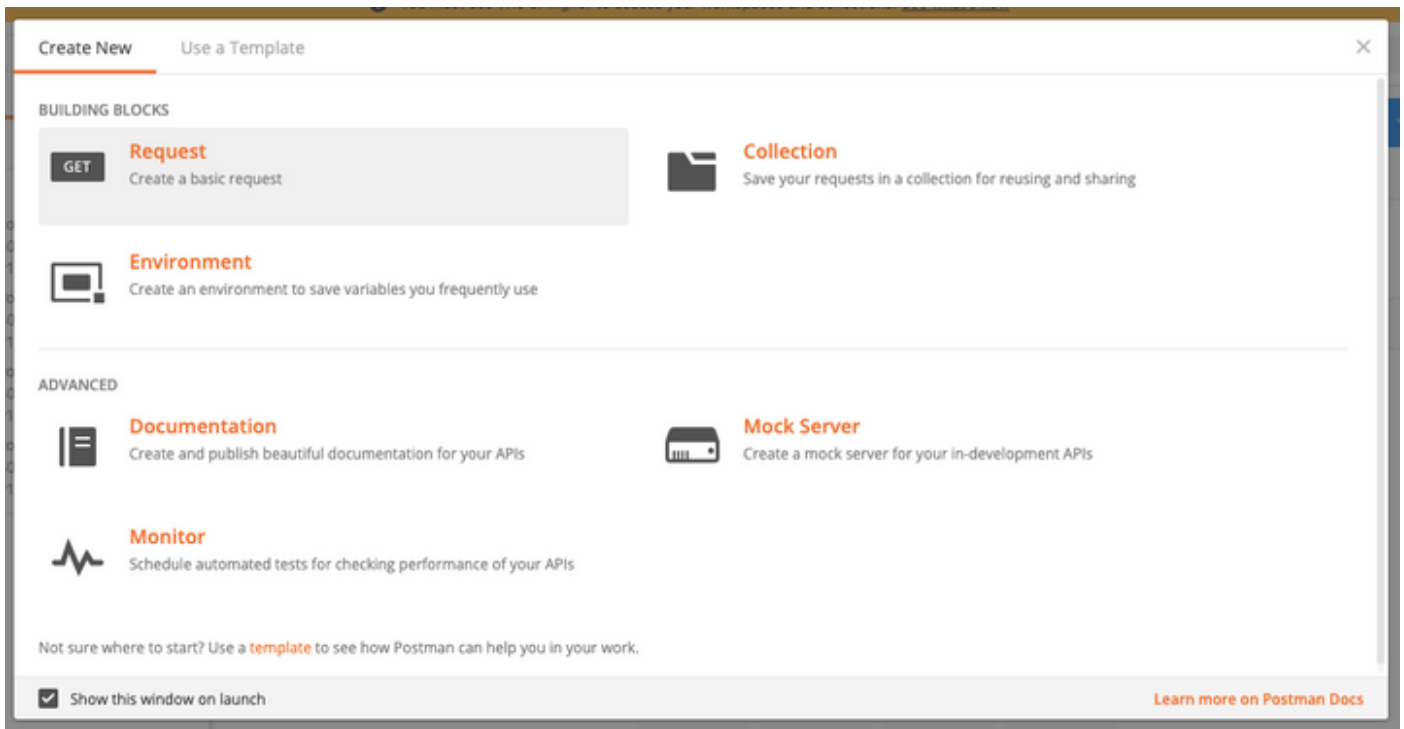
Step 6. After you pass the SSO login window, look for an entry called **Me**.

Step 7. Click on the **Me** entry. Navigate to the Headers tab and then scroll down until **Request Headers**. Next to **Authorization** is the Bearer token.

Name	Headers	Preview	Response	Timing
<input type="checkbox"/> usage	Transfer-Encoding: chunked			
<input type="checkbox"/> services	X-Content-Type-Options: nosniff			
<input type="checkbox"/> 2f384032-5cba-4d6a-9a18-1...	X-Frame-Options: DENY			
<input type="checkbox"/> flags?name=fms.services.squ...	▼ Request Headers			
<input type="checkbox"/> 2f384032-5cba-4d6a-9a18-1...	⚠ Provisional headers are shown			
<input type="checkbox"/> 2f384032-5cba-4d6a-9a18-1...	Accept: application/json, text/plain, */*			
<input type="checkbox"/> keys	Access-Control-Expose-Headers: TrackingID			
<input type="checkbox"/> atlas.notification.dismissed-n...	Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJjbHVzdGvYIjoiUEY4NCIsInBya			
<input type="checkbox"/> 2f384032-5cba-4d6a-9a18-1...	XZhdGU0iJleUpqZEhraU9pSktWMVFPtENKbGJtTWlPaUpCTVRJNFEwSkRMVWhUTWpVMkL			
<input type="checkbox"/> atlas.notification.dismissed-n...	pd2lZV3huSwpvaVpHbHlJbjAuLmV4MW5fcjNrUFdZVXA0TDJDS0w4M0EuNjh0d0I3T0hiV			
<input type="checkbox"/> domains	lN4UmFn0DBEUKLS0Us2bDJuRFVpc2Q5cjJsVE5pQ0lUaFBvbERQM1RzUEQ5aG5nQ0lsaDl			
<input type="checkbox"/> 2f384032-5cba-4d6a-9a18-1...	HMFdJdDZPamIxY1dPc05UUXBGQTLlNC1PaU12NThct0hF0G4zbgmyaF9jUzVwUG4ybzVnT			
<input type="checkbox"/> 2f384032-5cba-4d6a-9a18-1...	zZlM28wS2pSbGtBNVJmaGxEeDI3YmVq0W1DM0VqMkJiTTYxc0VMN2FhaEdWmM54UVNUUdh			
<input type="checkbox"/> CiscoSansTTEExtraLight.38be...	EcWnpc2N40G1icmg1dV9YTTVlcWo3S1hmTDcwRwPnbzVwQzQyS1MyVwobw45dmtsYVZJb			
<input checked="" type="checkbox"/> me	VpJcHZ1V0xFOHvVxZNLNUpFQXNXUW45VWpmdU5tNmpkTVhaeGtTbGkUXd0S1lLc0JHd2d			
<input type="checkbox"/> data:image/svg+xml;...	CeVNDNTRiLvhSQUxjN1dQUWV40WpWa2x5VXQyWTRwbGlvXzlaTERqSjhIYTFlbW9Xb1ZjT			
<input type="checkbox"/> control-hub-white.svg	k43RXBzwl83M1hndk5QT0tMUKNzbHZRdL0ZjRvRVRaTU0cGZXM2pi0WNSN0tCWxvtcnR			
<input type="checkbox"/> squared-fusion-gcal	uWVBqb1EzLTFoeTEwCHFjeVlsUTdoMURkMjhJUFhzSXNmM2FIS3Q2ZudpX0JUMza5N0d2U			
<input type="checkbox"/> squared-fusion-cal	ExNdUdLTFNsS3NtV1NvNnbv1gweGYzUENWUnFx0Xl1Y2szYmg5UU5tY2ExbwPStkp4NFV			
<input type="checkbox"/> services	YNGVfdHE3MTE1eLJKMl8yV2tnN3FiQU8zclBiRmxsTUtPeLNPyY1aMHkwVF81c2RWYVp0Z			
<input type="checkbox"/> services	WVLUUVyWXZmS181Q1JfdEJEQkFsZmcwVlVSWGdGNnZ4U1hwaTFXblBaUEFnMlF0U0pEZDR			
<input type="checkbox"/> domains	iUl5d5RDZ6S1ptMGJ0QzMyb21HcFQyWEV0UHJZQ3pxaDE1aVhHdkczZjhi0EFjbnBBMXVXR			
<input type="checkbox"/> trials	TB0WmtmbE56eUNjdWZ20EVfWxhtRzI4UjZpQU03WjAweTRwQWZmckZSVTltdXctRDZV0VF			
<input type="checkbox"/> CiscoSansTTThin.f51c3a281...	oQ0d3M2ZWUudQMWNkX0E5T2F4R19rUnlfsGpFRDM2SwtdXpVbDgzTU1fvjhRaG1lSU1VN			
<input type="checkbox"/> jobs	01ieLVPQLA1TjFwazNGSnBfTGYxUDhid0xnTGMtcGNJNF9VQ3Rkc2N2RDNjb0RPTEUtUFh			
	tVEhLUWU30E1lUEthWTKyeC1fr3hTcGRGYktLbGlnb0FOX0VmZmlpbDYyWGJsNHFLcHZTZ			
109 requests	2.4 MB transferred			

Configure

Step 1. Open Postman and create a new Request.



Enter a name and click **Save to Webex**.

SAVE REQUEST



Requests in Postman are saved in collections (a group of requests).

[Learn more about creating collections](#)

Request name

Remeber Me API

Request description (Optional)

Adding a description makes your docs better

Descriptions support Markdown

Select a collection or folder to save to:

Search for a collection or folder

< Webex Teams

+ Create Folder

Cancel

Save to Webex Teams

Step 2. Navigate to the Headers tab and enter the Keys and Values below:

Authorization
Content-Type
Accept

Bearer Token
application/json
application/json

Step 3. Replace {OrgID} in the URL with the orgid that you found in Control Hub.

<https://idbroker.webex.com/idb/idbconfig/{orgid}/v1/authentication>

Step 4. Do a GET from Postman in order to see the contents of the authentication policy:

```
{
  "EmailAsUid": true,
  "JITCreation": false,
  "JITUpdate": false,
  "KeepMeSignedIn": false,
  "KeepMeSignedInDuration": 14,
  "LockoutDuration": 1,
  "LockoutDurationMultiplier": 1,
  "LockoutFailureCount": 5,
  "LockoutFailureDuration": 300,
  "RememberMyLoginId": false,
  "RememberMyLoginIdDuration": 30,
  "mfaEnabled": false,
  "schemas": [
    "urn:cisco:codev:identity:idbroker:authnconfig:schemas:1.0"
  ]
}
```

This image illustrates Step 1. and Step 2.

The screenshot shows a REST client interface with a GET request to `https://idbroker.webex.com/idb/idbconfig/2f384032-5cba-4d6a-9a18-17c9e709a8ec/v1/authentication`. The Headers tab is active, showing three headers: Authorization (Bearer eyJhbGciOiJSUzI1NiJ9.eyJjbHVzdGVyJoiUEY4NCIs...), Content-Type (application/json), and Accept (application/json). The Body tab is also active, showing a JSON response with the following content:

```

1 {
2   "EmailAsUid": true,
3   "JITCreation": false,
4   "JITUpdate": false,
5   "KeepMeSignedIn": false,
6   "KeepMeSignedInDuration": 14,
7   "LockoutDuration": 1,
8   "LockoutDurationMultiplier": 1,
9   "LockoutFailureCount": 5,
10  "LockoutFailureDuration": 300,
11  "RememberMyLoginId": false,
12  "RememberMyLoginIdDuration": 30,
13  "mfaEnabled": false,
14  "schemas": [
15    "urn:cisco:codev:identity:idbroker:authnconfig:schemas:1.0"
16  ]
17 }

```

Step 5. Copy the above from your GET response and paste it in the **Body** tab with the use of the **Raw** format as shown in the image:

The screenshot shows the REST client interface with the Body tab selected. The format is set to 'raw'. The JSON response content is pasted into the body field:

```

1 {
2   "EmailAsUid": true,
3   "JITCreation": false,
4   "JITUpdate": false,
5   "KeepMeSignedIn": false,
6   "KeepMeSignedInDuration": 14,
7   "LockoutDuration": 1,
8   "LockoutDurationMultiplier": 1,
9   "LockoutFailureCount": 5,
10  "LockoutFailureDuration": 300,
11  "RememberMyLoginId": true,
12  "RememberMyLoginIdDuration": 30,
13  "mfaEnabled": false,
14  "schemas": [
15    "urn:cisco:codev:identity:idbroker:authnconfig:schemas:1.0"
16  ]
17 }

```

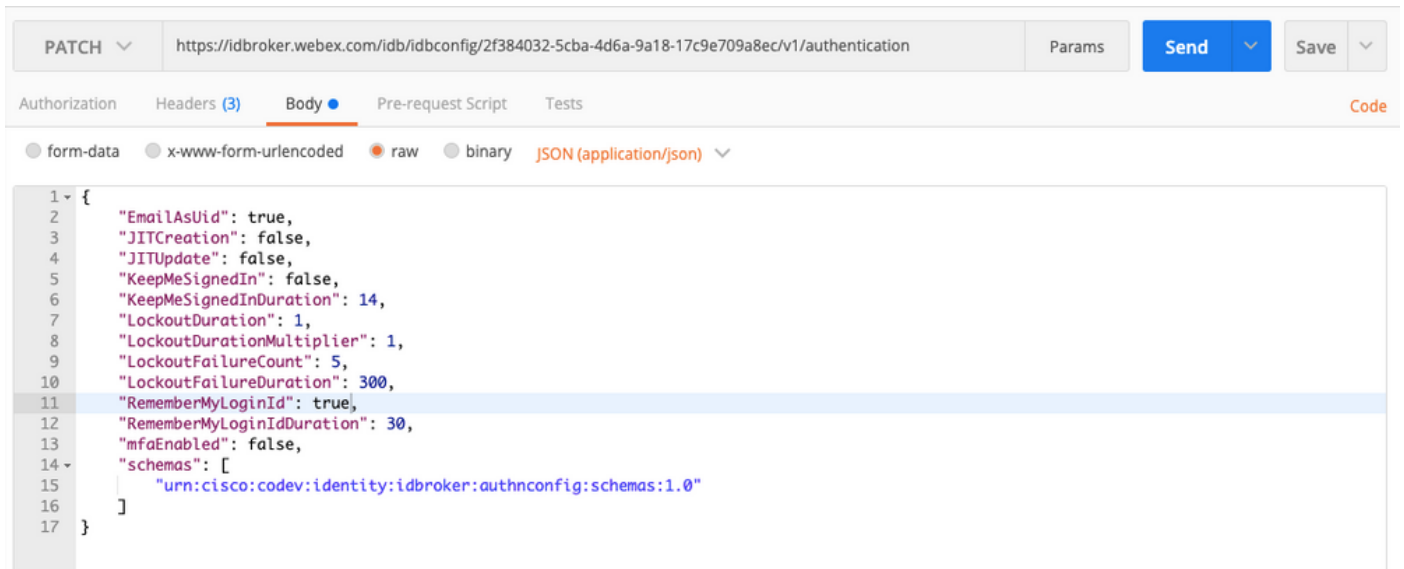
Change **RememberMyLoginId: false** to **RememberMyLoginId: true**.

Choose a value for the **RememberMyLoginIdDuration** appropriate for your users. This value determines how long (days) the Remember Me token is valid in the browser. If a user tries to log in

to a Webex site in that browser and on that machine with a different email address for testing purposes or as a different employee identity for any reason, they will not be recognized with that identity.

Note: The Remember Me token is an encrypted hash of the email address only for the purpose of identification in the **Discovery Screen**.

Step 6. Do a PATCH from Postman in order to overwrite your changes.



The screenshot shows a Postman interface for a PATCH request. The URL is `https://idbroker.webex.com/idb/idbconfig/2f384032-5cba-4d6a-9a18-17c9e709a8ec/v1/authentication`. The request body is a JSON object with the following properties:

```
1 {
2   "EmailAsUid": true,
3   "JITCreation": false,
4   "JITUpdate": false,
5   "KeepMeSignedIn": false,
6   "KeepMeSignedInDuration": 14,
7   "LockoutDuration": 1,
8   "LockoutDurationMultiplier": 1,
9   "LockoutFailureCount": 5,
10  "LockoutFailureDuration": 300,
11  "RememberMyLoginId": true,
12  "RememberMyLoginIdDuration": 30,
13  "mfaEnabled": false,
14  "schemas": [
15    "urn:cisco:codev:identity:idbroker:authnconfig:schemas:1.0"
16  ]
17 }
```

Caution: Do not change any of the other values as they will affect the ability of your site for all users to handle authentication. If you change any of these values, you will not be able to receive support from Cisco TAC.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.