

Configurazione dell'API Remember Me per PST sui siti Webex gestiti tramite Control Hub

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come configurare l'API Remember Me per le integrazioni con PST (Persistent Session Tokens) quando l'SSO (Single Sign On) è abilitato per CI Webex Sites (gestito tramite Webex Control Hub). Quando SSO è abilitato, è possibile configurare PST dal provider di identità (IdP) in modo che la scadenza delle sessioni sia più lunga. Per i siti CI, per impostazione predefinita Webex idbroker non rispetta PST.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conosci il tuo ID organizzazione e ottieni un token di connessione
- Postman installato. È possibile scaricare la versione desktop o il componente aggiuntivo per Chrome

Nota: Per informazioni su come ottenere un token di connessione, accedere a Background Information.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

L'ID organizzazione si trova in Webex Control Hub. Accedere a Control Hub e fare clic su **Società**.

Per ottenere un token Bearer, attenersi alla seguente procedura:

Passaggio 1. Da Google Chrome, passare ad **admin.webex.com**.

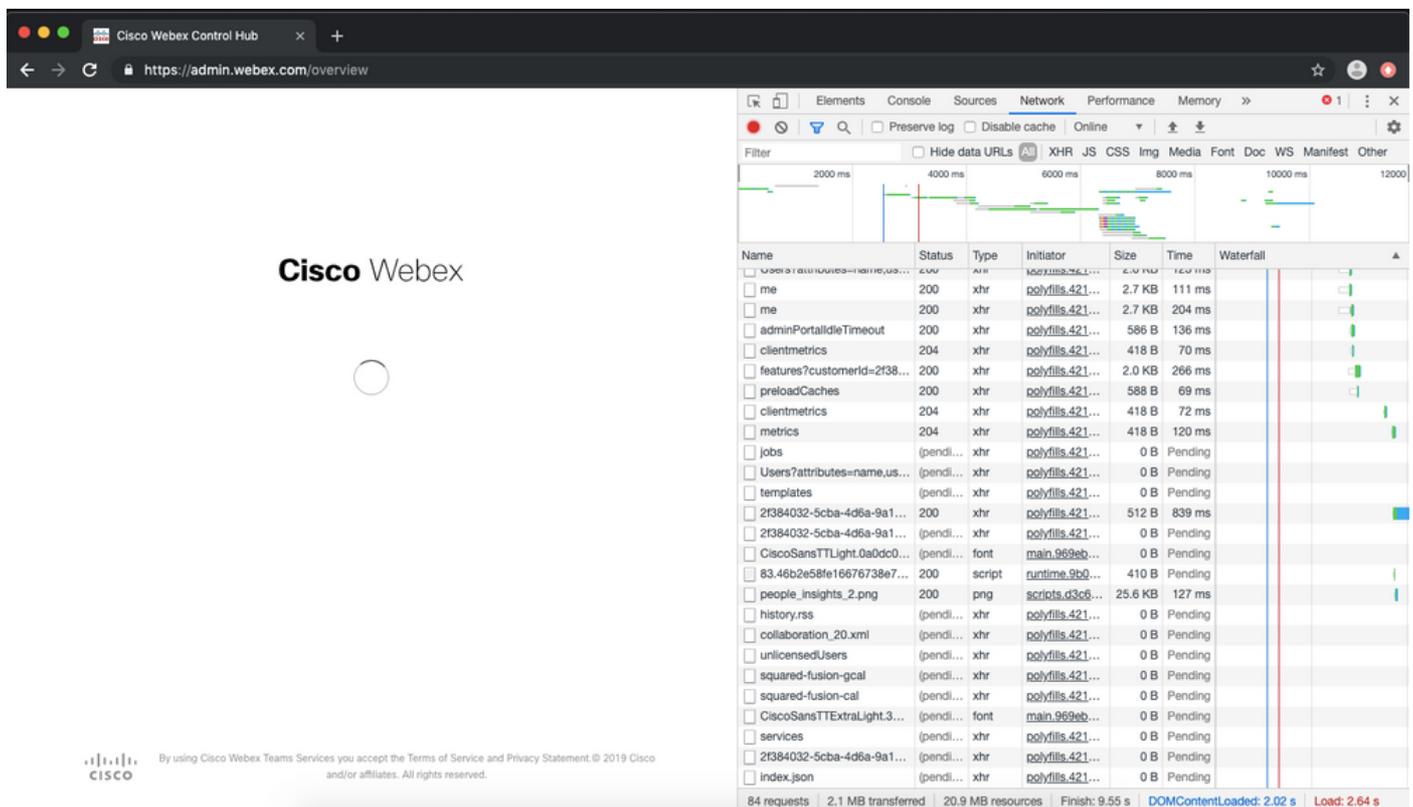
Passaggio 2. Nella parte superiore destra della finestra del browser, fare clic sul menu Chrome (:).

Passaggio 3. Selezionare **Strumenti > Strumenti di sviluppo**. La finestra Strumenti di sviluppo si apre come un pannello ancorato sul lato o sulla parte inferiore di Chrome.

Passaggio 4. Selezionare la scheda **Rete**.

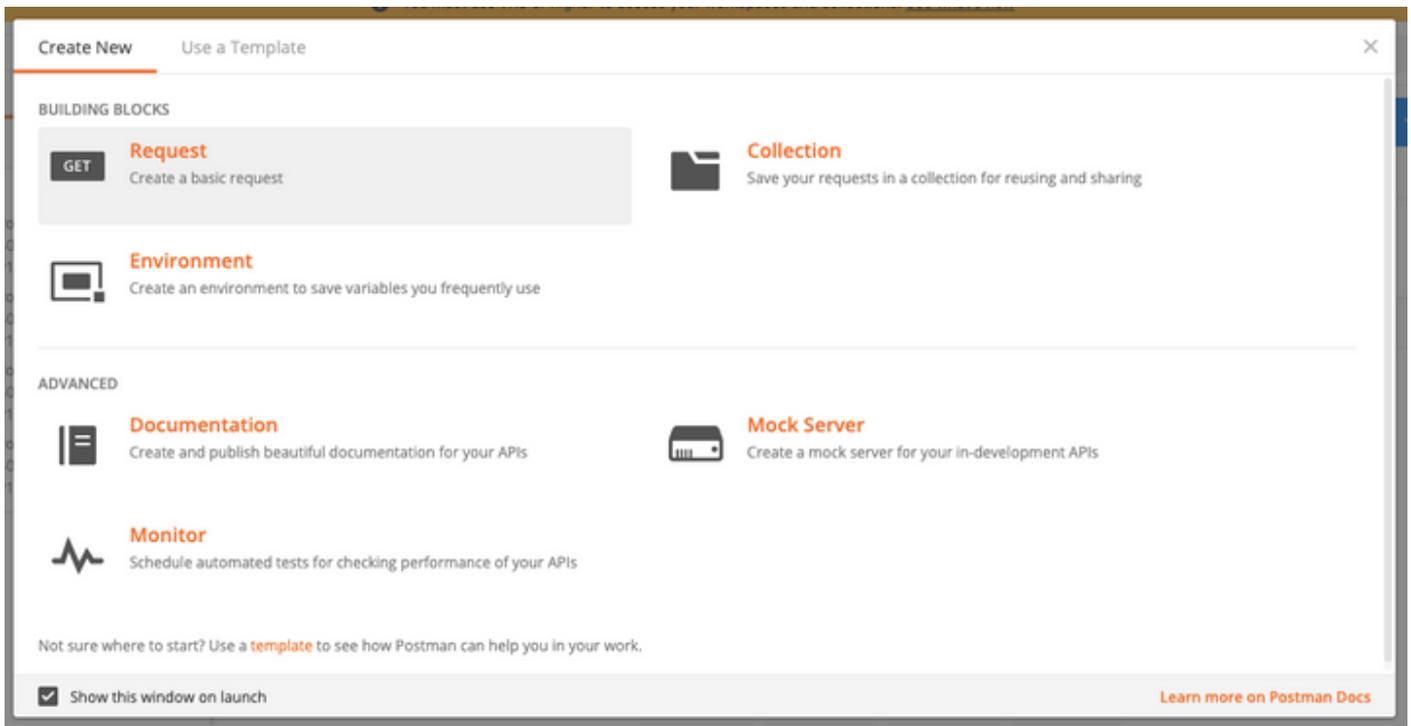
Passaggio 5. Accedere con l'account di amministratore completo.

Nell'immagine vengono illustrati i passaggi da 1 a 5.:



Passaggio 6. Dopo aver passato la finestra di accesso a SSO, cercare la voce **Me**.

Passaggio 7. Fare clic sulla voce **Me**. Passare alla scheda Intestazioni e scorrere verso il basso fino a **Intestazioni richieste**. Accanto a **Authorization** è disponibile il token Bearer.



Immettere un nome e fare clic su **Salva in 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

Passaggio 2. Passare alla scheda Intestazioni e inserire le chiavi e i valori seguenti:

Authorization
Content-Type
Accetta

Bearer Token
application/json
application/json

Passaggio 3. Sostituire {OrgID} nell'URL con l'orgid trovato in Control Hub.

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

Passaggio 4. Eseguire un'operazione GET da Postman per visualizzare il contenuto dei criteri di autenticazione:

```
{  
  "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"  
  ]  
}
```

In questa immagine vengono illustrati i passaggi 1 e 2.

GET Params

Authorization Headers (3) Body Pre-request Script Tests Code

Key	Value	Description	...	Bulk Edit	Presets
<input checked="" type="checkbox"/> Authorization	Bearer eyJhbGciOiJSUzI1NiJ9.eyjbHVzdGVyJoiUEY4NCIs...				
<input checked="" type="checkbox"/> Content-Type	application/json				
<input checked="" type="checkbox"/> Accept	application/json				
New key	Value	Description			

Body Cookies Headers (8) Test Results Status: 200 OK Time: 187 ms

Pretty Raw Preview JSON

```

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 }

```

Passaggio 5. Copiare quanto sopra dalla risposta GET e incollarlo nella scheda **Body** con il formato **Raw** come mostrato nell'immagine:

Authorization Headers (3) **Body** Pre-request Script Tests

form-data x-www-form-urlencoded raw binary **JSON (application/json)**

```

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 }

```

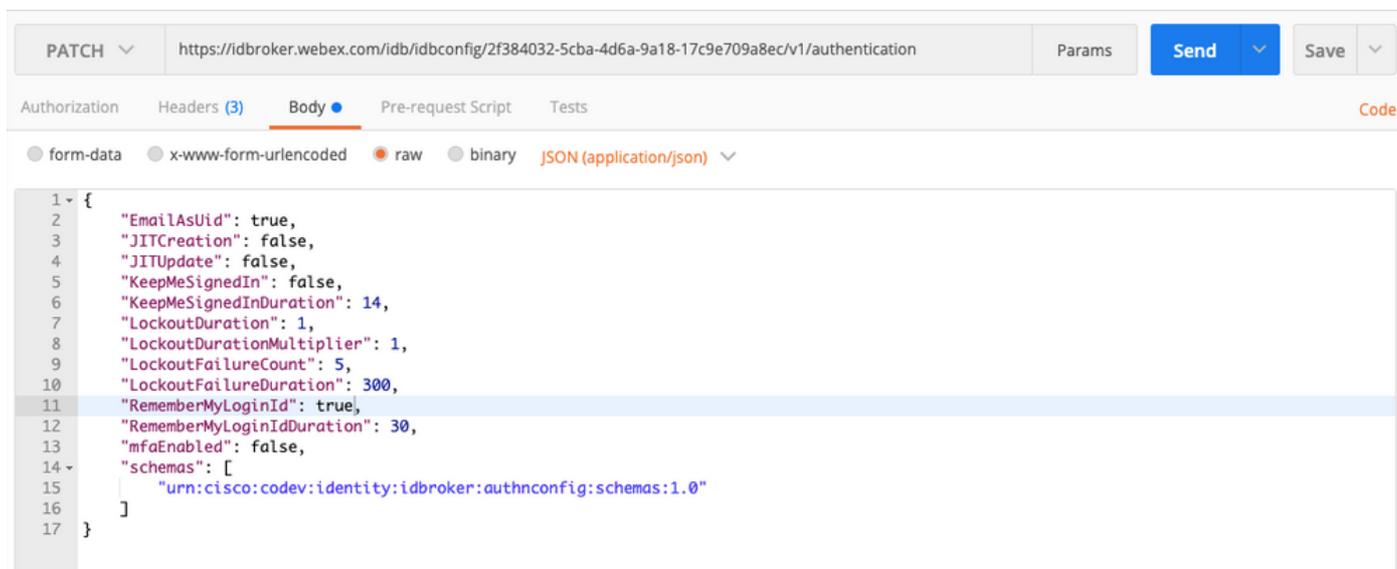
Cambia **RememberMyLoginId: false** to **RememberMyLoginId: vero**.

Scegliere un valore per **RememberMyLoginIdDuration** appropriato per gli utenti. Questo valore determina per quanto tempo (giorni) il token di memorizzazione è valido nel browser. Se un utente

tenta di accedere a un sito Webex in quel browser e su quel computer con un indirizzo e-mail diverso a scopo di test o come identità di un dipendente diverso per qualsiasi motivo, non verrà riconosciuto con quell'identità.

Nota: Il token di memorizzazione è un hash crittografato dell'indirizzo e-mail solo a scopo identificativo nella **schermata di individuazione**.

Passaggio 6. Eseguire una PATCH da Postman per sovrascrivere le modifiche.



Attenzione: Non modificare nessun altro valore in quanto influirà sulla capacità del sito di tutti gli utenti di gestire l'autenticazione. Se si modifica uno di questi valori, non sarà possibile ricevere supporto da Cisco TAC.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.