

# Errore Finesse IPPA "Phone URL Authentication" (Autenticazione URL telefono) generato dopo la terminazione della chiamata

## Sommario

[Introduzione](#)

[Risoluzione dei problemi di autenticazione URL FIPPA](#)

[Raccogli informazioni](#)

[Risoluzione dei problemi](#)

## Introduzione

In questo documento viene descritto un problema relativo a un agente IPPA (IP Phone Agent) Finesse che riceve un errore relativo a nome utente o password di autenticazione URL telefono non corretti nelle impostazioni dell'agente IP Phone. Contattare l'amministratore." dopo la normale terminazione della chiamata.

## Risoluzione dei problemi di autenticazione URL FIPPA

### Raccogli informazioni

Verificare le impostazioni IPPA dell'utente configurato nella pagina Web di Finesse Administration.

IP Phone Agent Settings

Note: Any changes made to the settings on this gadget require a restart of Cisco Finesse Tomcat to take effect.

Phone URL Authentication Settings

\*Username: pguser

\*Password: .....

\*Indicates required fields

Save Revert

Otteni informazioni di base sul telefono con il servizio FIPPA configurato. Per risolvere i problemi, è buono avere indirizzo MAC, indirizzo IP e interno del telefono.

Phone (1 - 1 of 1)								
Find Phone where Directory Number contains 1011								
Select item or enter search text								
	Device Name(Line) ^	Description	Device Pool	Extension	Partition	Device Protocol	Status	IPv4 Address
<input type="checkbox"/>	SEPC80084AA8721(1)	fippa 1011	Default: KRK_FL02	1011		SIP	Registered with 10.48.47.136	10.62.153.22

## Risoluzione dei problemi

La maggior parte delle operazioni di risoluzione dei problemi per questa funzionalità viene eseguita dalla prospettiva di Cisco Unified Communications Manager (CUCM).

Pertanto l'amministrazione dovrebbe avere una certa esperienza con CUCM.

Verificare che l'utente configurato nelle impostazioni IPPA di Finesse Administration disponga del telefono nell'elenco dei dispositivi controllati. A tale scopo, utilizzare questa query SQL. Sostituire il nome pguser nella query con quello configurato.

```
admin:run sql SELECT m.pkid,ap.name appuser,d.name device FROM ApplicationUserDeviceMap m INNER
JOIN device AS d ON d.pkid==m.fkdevice INNER JOIN applicationuser ap ON
ap.pkid==m.fkapplicationuser WHERE ap.name LIKE 'pguser'
pkid appuser device
=====
ea92949a-c8e4-4818-ad42-80ed5ba65135 pguser SEP0050569902C1
fb5af549-d1ae-423b-afa0-f28b32e4426d pguser SEP005056996F7E
1fe71268-328b-4810-9e55-5683647a82d1 pguser SEPC80084AA8721
```

Nell'esempio, **pguser** ha il telefono con l'indirizzo MAC C80084AA8721 nell'elenco delle periferiche controllate.

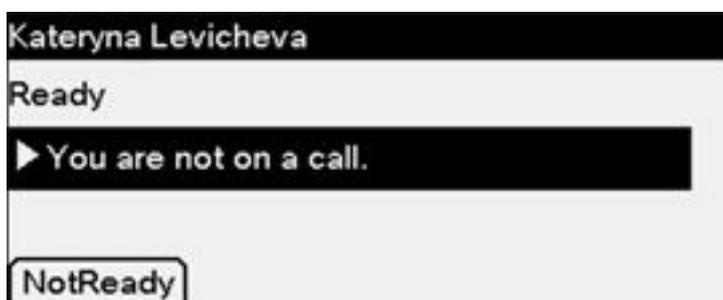
Se si utilizza il servizio Extended Mobility (EM), è necessario associare anche il profilo di dispositivo controllato CTI a pguser.

Utilizzare questo collegamento per assicurarsi che il telefono possa essere controllato in remoto. Sostituire l'indirizzo IP con quello del telefono FIPPA e fornire le credenziali pguser dopo il prompt.

<http://10.62.153.22/CGI/Screenshot>

**Nota:** Chiudere il browser se si desidera utilizzare il collegamento per eseguire nuovamente il test.

Se la configurazione è corretta, verrà visualizzata un'immagine simile.



In caso di problemi di configurazione, è possibile che venga visualizzato questo messaggio.

Il codice di errore "4" indica un problema di autenticazione.

Dal file di registro FIPPA verranno visualizzati messaggi simili.

```
0000001737: 10.48.47.140: Jun 08 2017 08:52:14.036 +0200: %CCBU_pool-148-thread-1-6-  
HTTP_RESPONSE: %[FIPPA_USER_ID=HttpClient-pushToPhone-24-15c86799425][HTTP_BODY=
```

```
] [HTTP_METHOD=POST] [HTTP_REQUESTID=null] [HTTP_RESPONSE_MESSAGE=OK] [HTTP_RESPONSE_STATUS=200] [HTT  
P_URL=http://10.62.153.22/CGI/Execute]: Received HTTP Response  
0000001738: 10.48.47.140: Jun 08 2017 08:52:14.039 +0200: %CCBU_pool-148-thread-1-3-FIPPA_ERROR:  
%[ERROR_DESCRIPTION=get invalid Response from phone:  
<CiscoIPPhoneError Number="4" />  
CiscoIPPhoneError: number=4][FIPPA_SOURCE=HttpPushClient-24-15c86799425]: An error was  
encountered
```

**Nota:** Per risolvere il problema, assicurarsi di abilitare il server Web nel layout di configurazione telefonica specifico del prodotto.

Verificare di aver specificato correttamente il collegamento relativo all'autenticazione URL risolvibile nei parametri Enterprise di CUCM.

Phone URL Parameters	
<a href="#">URL Authentication</a>	<input type="text" value="http://10.48.47.143:8080/ccmcp/authenticate.jsp"/>
<a href="#">URL Directories</a>	<input type="text" value="http://10.48.47.143:8080/ccmcp/xmldirectory.jsp"/>
<a href="#">URL Idle</a>	<input type="text"/>
<a href="#">URL Idle Time</a>	<input type="text"/>
<a href="#">URL Information</a>	<input type="text"/>
<a href="#">URL Messages</a>	<input type="text"/>
<a href="#">IP Phone Proxy Address</a>	<input type="text"/>
<a href="#">URL Services</a>	<input type="text" value="http://10.48.47.143:8080/ccmcp/getservicesmenu.jsp"/>

In alcuni casi, la rimozione dell'URL di autenticazione protetta consente di risolvere il problema.

Secure Phone URL Parameters	
<a href="#">Secure Authentication URL</a>	<input type="text"/>
<a href="#">Secure Directory URL (XML)</a>	<input type="text"/>

Se il problema persiste, provare a utilizzare una delle opzioni seguenti:

- rimuovi file ITL/CTL dal telefono
- rimuovi l'associazione del telefono con pguser e associa il telefono
- riavviare il processo CTIManager sul nodo su cui è registrato il telefono (nell'esempio, 10.48.47.136)