Cisco Jabber for Windows on CallManager Express Configuration Example

TAC   **Document ID: 118715**

Contributed by Jorge Armijo and Sreekanth Narayanan, Cisco TAC Engineers.

Jan 14, 2015

Contents

Introduction

This document describes new features introduced in Cisco CallManager Express (CME) Version 10.0, which include support for Cisco Jabber for Windows. The Jabber application works only in "Phone Only Mode" where it functions like a regular Session Initiation Protocol (SIP) Phone. Presence and Instant Messaging (IM) are not available with this mode of Jabber.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Integrated Services Router Generation 2 (ISR G2) router that runs Cisco IOS® version 15.3(3)M or later
- A PC with an operating system compatible with Jabber software. Check the requirements in the Cisco Jabber for Windows 9.2.x Installation and Configuration Guide.

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.

Configuration

Note: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

HTTPS Configuration

Cisco Jabber requires HTTPS in order to work. Therefore, you will first need to set up the HTTPS server on the CME so that the user can log into the Jabber endpoint.

```
CME(config)#ip http secure-server
CME(config)#ip http secure-port 8443
```

Voice Register Pool Configuration

This section configures the pool that the Jabber endpoint will register as.

```
CME(config)#voice register dn 1
CME(config-register-dn)#number 9999

CME(config)#voice register pool  1
CME(config-register-pool)#id device-id-name J4W
CME(config-register-pool)#type Jabber-Win
CME(config-register-pool)#number 1 dn 1
CME(config-register-pool)#dtmf-relay rtp-nte
CME(config-register-pool)#username 9999 password 9999
CME(config-register-pool)#codec g711ulaw
CME(config-register-pool)#no vad
```

Apply Configuration Changes on the SIP CME

The profiles need to be deleted and recreated for all SIP phones as this is not an automatic process.

```
CME(config)#voice register global
CME(config-register-global)#no create profile
CME(config-register-global)#create profile
```

Note: The voice register global must contain the *tftp−path flash:* command that ensures a configuration file is created on the flash for the Jabber SIP phone. Without this, Cisco Jabber will not be able to register with the CME.
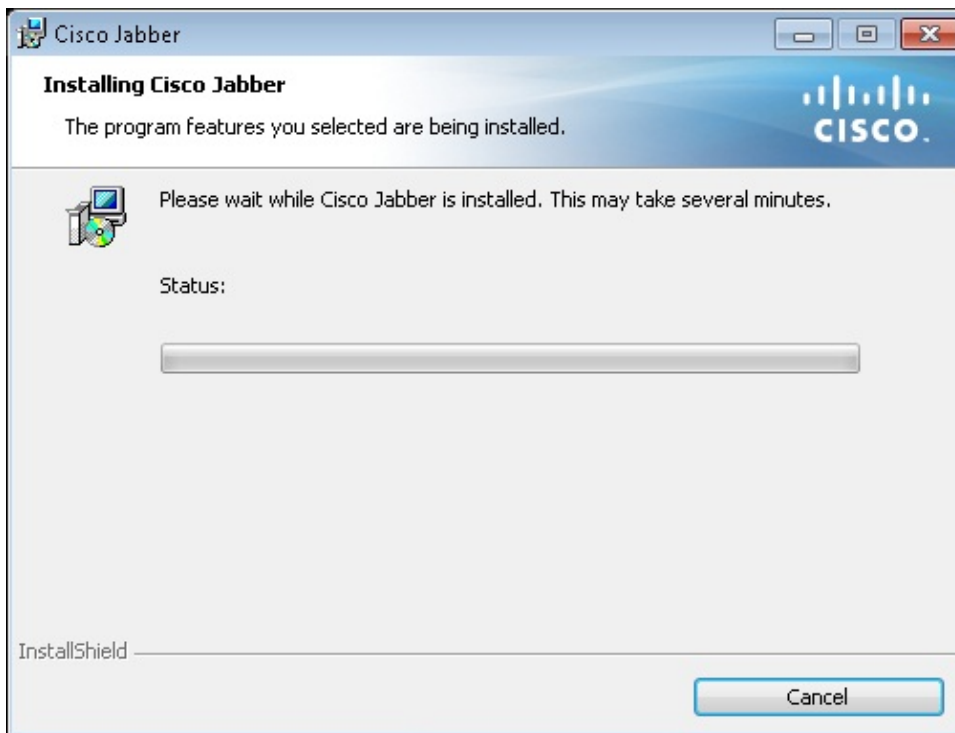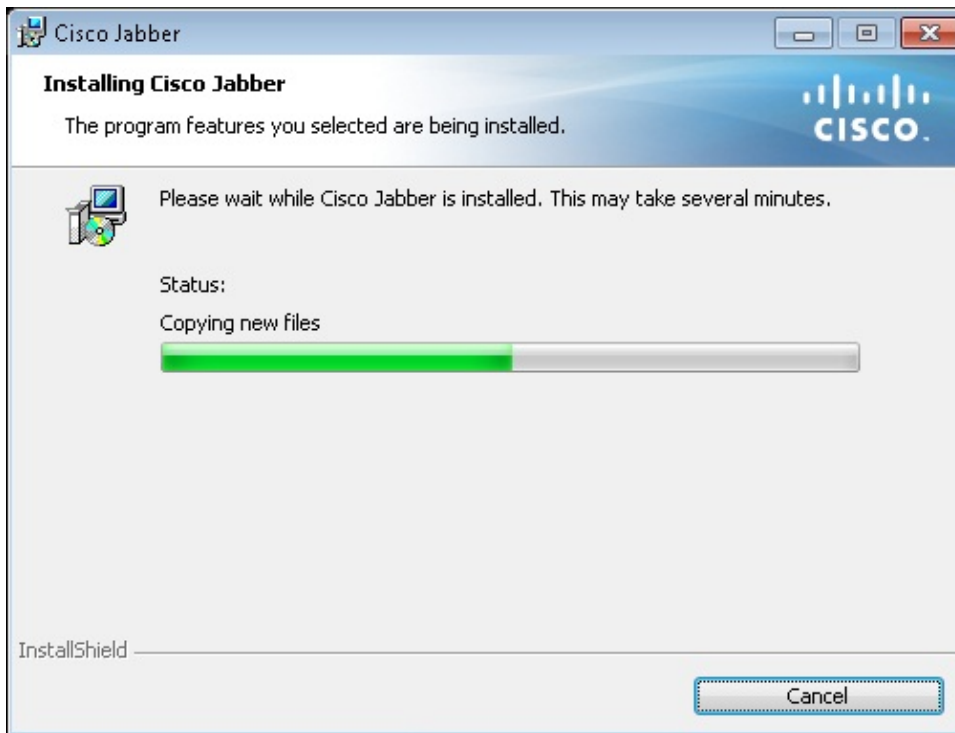
Install Jabber for Windows

Complete these instructions in order to install Jabber:

1. Download the installer from the Cisco web site and start the installation process with the installation wizard.
2. Click *Accept and Install*.
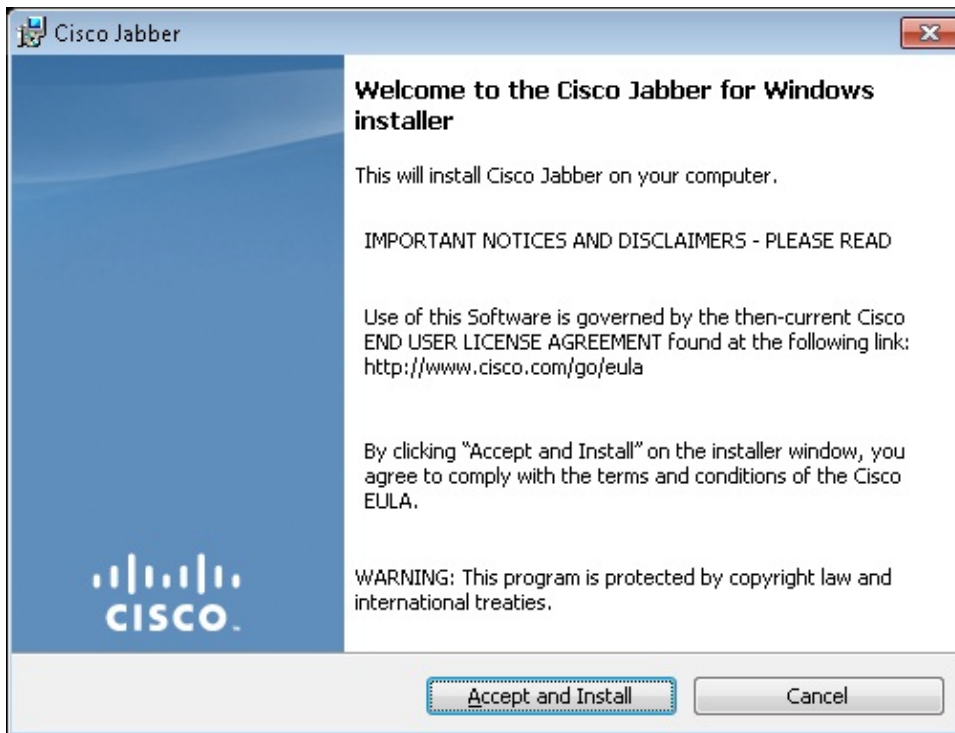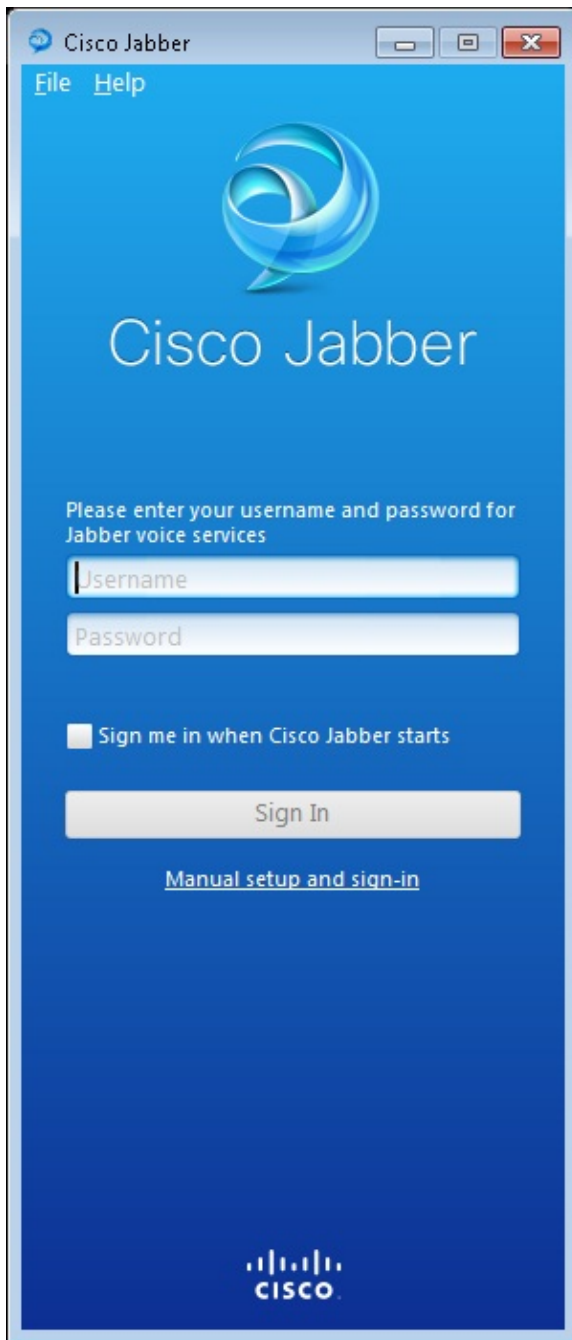
3. Wait for the installation to complete.

4. Click *Finish*.

Log Into Jabber

1. Once Jabber is installed and launched, enter your username and password in order to log in.

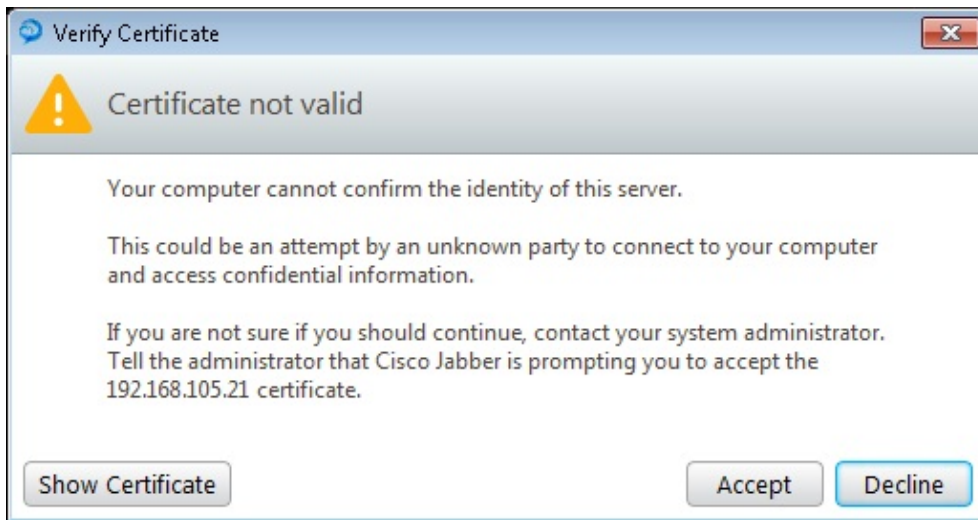2. Set up the TFTP and CME server.

3. Enter the username and password that were configured under the voice register pool and click *Sign In*.
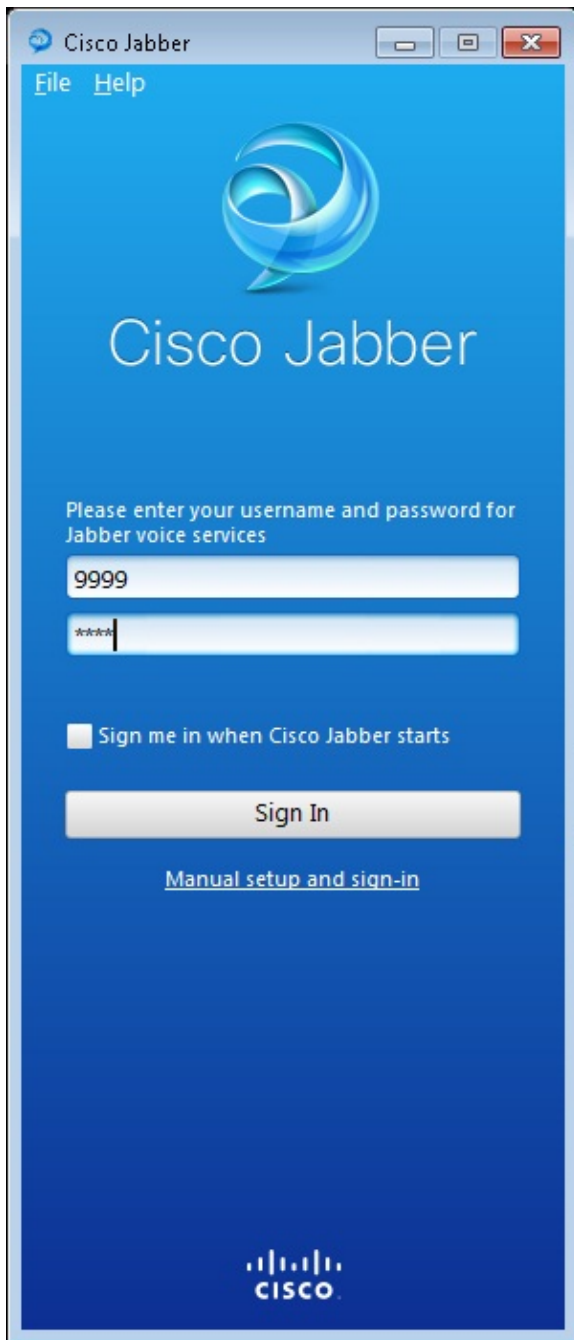
4. An alert pop ups up in regards to the self–signed certificate from the CME. Click *Accept* in order to accept the certificate and allow Jabber to authenticate and log in.

Jabber for Windows is now ready to make and receive calls.
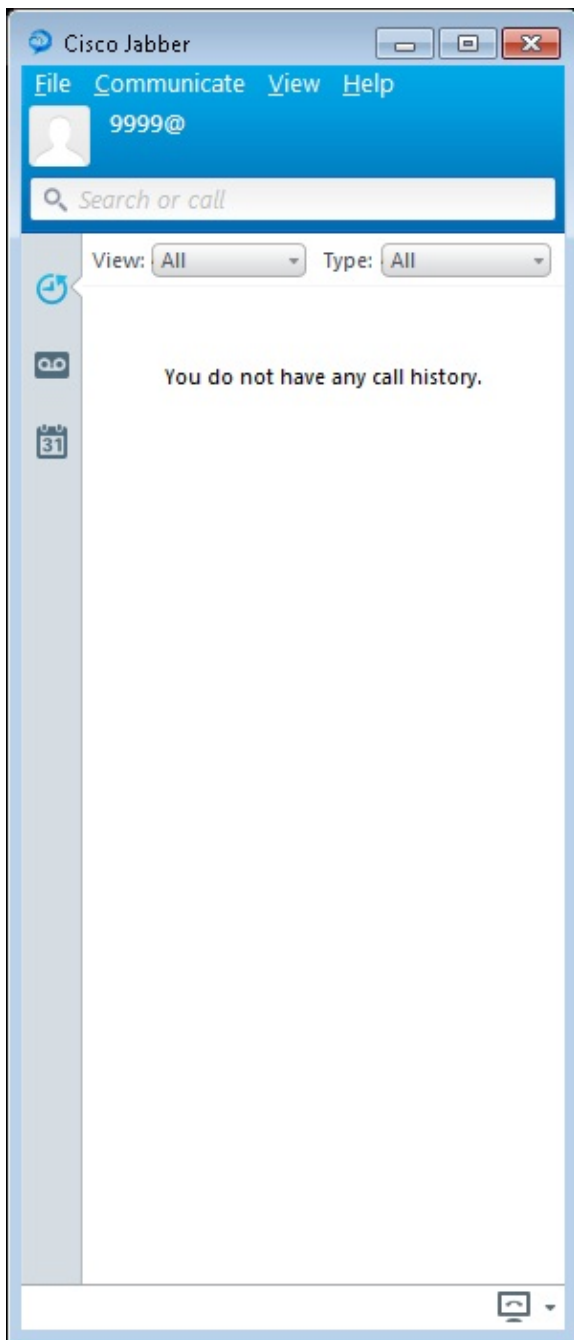
Known Issue: Certificate Error

When you try to log in to Jabber, there is a message in regards to a certificate error:

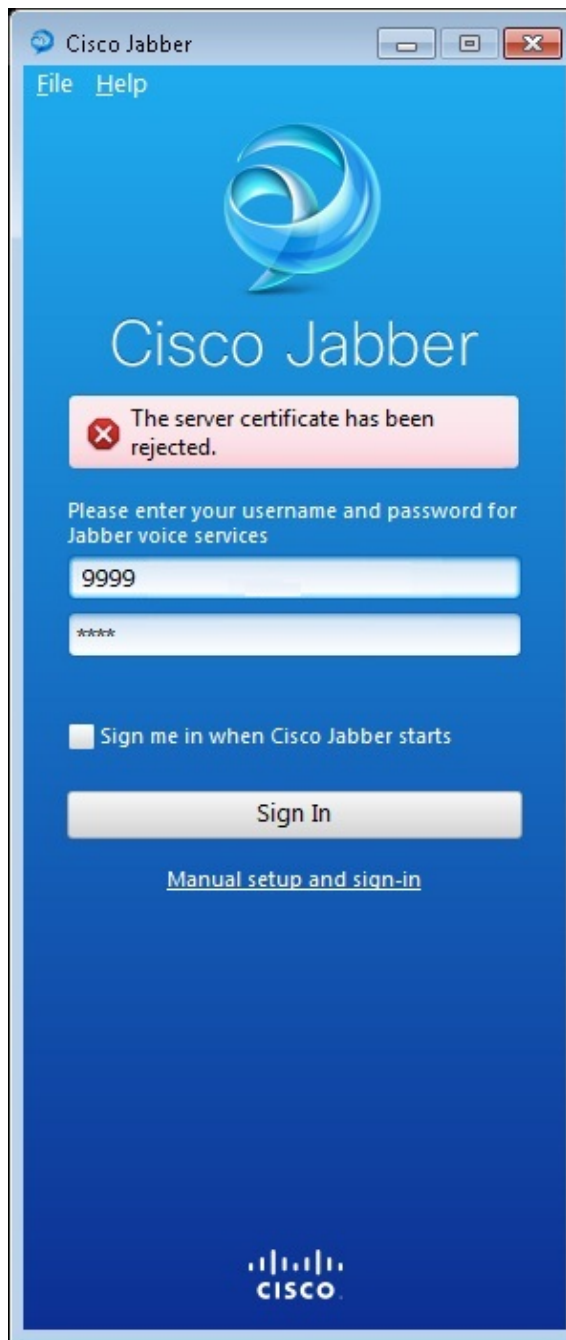Enter the *debug ip http all* command in order to get this output:

```
019193: *Jul  1 08:59:02.561: %HTTPS: http ssl get context fail (-41104)
019194: *Jul  1 08:59:02.561: HTTP: ssl get context failed (-40407)
```

Solution

As seen in the ouput above, it is a problem with the HTTPS certificate.

In order to solve this, log into the CLI and remove the HTTPS configuration commands. Also remove the self−signed certificate generated by the CME for HTTPS.

```
CMEconfig)#no ip http secure-server
CME(config)#no ip http secure-port 8443
CME(config)#no crypto pki certificate chain TP-self-signed-3120869618
This will remove all certificates for trustpoint TP-self-signed-3120869618
```

```
Are you sure you want to do this? [yes/no]: yes
```

Then, reconfigure the HTTPS configuration and confirm a new self−signed certificate has been created.

```
CME(config)#ip http secure-server
CME(config)#ip http secure-port 8443


!
crypto pki trustpoint TP-self-signed-3120869618
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3120869618
 revocation-check none
 rsakeypair TP-self-signed-3120869618
!
```

After this, Jabber will be able to register with the CME.

Caveat

A new phone type, "Jabber−CSF−Client" has been added to configure the Cisco Jabber client under the voice register pool. This can be used for the configuration of any Client Services Framework (CSF)−based Cisco Jabber client. In CME Version 10.0, the type "Jabber−Win" is used in order to configure the Cisco Jabber client. In CME Version 10.5 this type is deprecated and the new "Jabber−CSF−Client" should be used for the configuration of the Cisco Jabber client as well.

For more information, see Support for Cisco Jabber.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

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

Related Information

- *Cisco Jabber for Windows*
- *Cisco Unified CME Features Roadmap*
- *Cisco Jabber for Windows 9.2.x Installation and Configuration Guide*
- *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix*
- *Technical Support & Documentation − Cisco Systems*

Updated: Jan 14, 2015   Document ID: 118715