

# Troubleshooting Extension Mobility in Cisco CallManager

Document ID: 18772

## Contents

### Introduction

#### Prerequisites

- Requirements
- Components Used
- Conventions

#### Device Profiles

- User Device Profile
- Device Profile Default
- Auto-Generated Device Profile
- How Device Profiles are Utilized

#### Login Call Flows

Login (hotel.aef)

Logout (hotelout.aef)

### Troubleshoot Extension Mobility

#### Common Problems

When a user reverts back to default profile, services are no longer available.

Extension Mobility logs out user after a few minutes, before the configured time.

After login, the user does not have any services available.

'Host not found' Error in IP Phone

After a login or logout is performed, the phone resets instead of restarting.

Services return HTTP [8] error.

"Login Unsuccessful:[101]" error returned on login.

Error No: -32

Services do not appear when "services" is pressed.

After a user logs in, the phone does not have any services.

After the username and password are entered, the phone returns to the login screen.

After username and password are entered, system generates "LoginServer Conn. error".

When logging in on a Cisco 7940 phone, the phone displays the error "Device profile does not exist".

XML Error [4] Parse Error is returned when selecting the login service.

Users are unable to log in to Extension Mobility and receive the login unsuccessful error 6.

"Login unsuccessful [9]" error message is generated on the phone.

Login unsuccessful Error [12]

Users are unable to log in to Extension Mobility and receive the "login unsuccessful error: [3]" or "error: [10]" or "error: [2]" after installing the Active Directory plug-in.

Error [18]- Another User logged in

Extension Mobility service returns error [100] login unsuccessful when the service to login to Extension Mobility is chosen.

Login unsuccessful error: [11]

Login unsuccessful Error:[6]

Unable to apply the Extension Mobility feature to an IP phone and receive the error "Already logged in to another phone"

Error: "Update failed. Could not insert new row – duplicate value in a UNIQUE INDEX column"

"Warning 7" Appears During Login to Extension Mobility IP Phone

Extension Mobility Access is Slow

IP Phones Stuck in "Registering" or "Configuring IP" Status After Log Out  
Extension Mobility Users Automatically Logged Out in Short Intervals  
No Results when Searching the DN Assigned to the Device Profile  
Unable to Logout an Entire Group of Users from Extension Mobility  
Extension Mobility

## Related Information

# Introduction

Extension Mobility (Hoteling) is a feature that allows you to log in to a phone and have the phone configuration available to you. Line appearances, speed dials, services, and message waiting indicator (MWI) information are present on the phone upon log in, as if the phone is assigned to the user. Extension Mobility also supports the configuration of Cisco 7914 expansion modules, if present on the phone device you are logged into.

This document describes how to troubleshoot the issue with extension mobility feature in Cisco CallManager 3.x and 4.x. Refer to these documents in order to troubleshoot extension mobility issues related to the later versions of CUCM:

- Cisco Unified Communications Manager 5.x/6.x/7.x : Extension Mobility Error Message
- CUCM 8.x: Extension Mobility Error Message

## Prerequisites

## Requirements

Cisco recommends that you have knowledge of these topics:

- Installation and configuration of Extension Mobility
- Installation and configuration for the Customer Response Application (CRA)
- Installation and configuration for the Cisco CallManager

## Components Used

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

- Cisco CallManager 3.x or 4.x
- Cisco Customer Response Application (CRA) version 2.2.1 (with Extension Mobility installed)

**Note:** With Cisco CallManager 3.3 (2) and later, the Cisco CallManager Extension Mobility application and the Cisco CallManager Extension Mobility service in Cisco CallManager provide the Extension Mobility functionality. The feature no longer requires the Cisco CRA engine. Refer to Understanding Cisco CallManager Extended Services for more details.

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.

## Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

# Device Profiles

Device Profiles can be viewed as configuring everything about a phone without being associated with a phone. Device Profiles contain the base device information (Cisco 7960/7940), Cisco 7914 add-on modules, services, speed dials, and line appearances. However, the device profiles are not associated with a physical phone.

Extension Mobility uses three types of profiles:

- User Device Profile
- Device Profile Default (4.x only)
- Auto-Generated Device Profile

## User Device Profile

The User Device Profile is the profile the system administrator configures for an individual user. This profile can be treated like any other phone device. The user can access this profile through the Cisco CallManager User page, add services, and speed dial in the same manner as a regular phone. The User Device Profile is the template that is applied to a phone when the user logs in. The profile can be used for both user login and the default (base) configuration for a phone.

## Device Profile Default

With Cisco CallManager 4.0 only, you configure a device profile default for each model of Cisco IP Phone that you want to support Cisco CallManager Extension Mobility. The device profile default is used whenever a user logs into a phone model for which no user device profile exists.

A device profile default comprises the set of attributes (services and/or features) that are associated with a particular device. Device profiles include device type, user locale, phone button template, softkey template and multilevel precedence and preemption (MLPP) information.

Use the Device Profile Default Configuration web page to create a device profile default for each phone model that supports Cisco CallManager Extension Mobility. A phone model can have a zero or one device profile default. The maximum number of device profile defaults cannot exceed the number of phone models that support Cisco CallManager Extension Mobility.

## Auto-Generated Device Profile

The Auto-Generated Device Profile is a special device profile that generates when a phone is configured for Extension Mobility and does not use a User Device Profile as the default device profile. When a phone is configured for Extension Mobility, the administrator must choose to **Use Current Device Settings** or **Select a User Device Profile** for the logout profile. If you choose **Use Current Device Settings**, the system creates the file `ADPxxxxxxxxx.cnf`, where `xxxxxxxxx` is the MAC address of the device configured for Extension Mobility.

**Note:** Cisco strongly recommends that you use the Auto-generated Device Profile and not assign a user device profile as the default device profile.

## How Device Profiles are Utilized

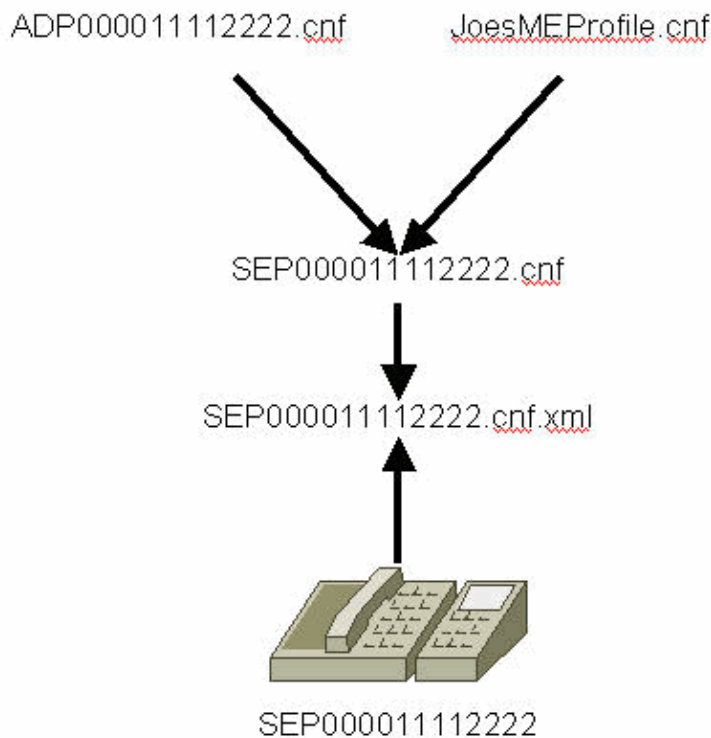
When a phone registers with Cisco CallManager, it sends a `tftp` request for the `SEPxxxxxxxxx.cnf.xml` file in the `TFTP` path. Extension Mobility works by swapping the

SEPxxxxxxxxxxxx.cnf file with either the User Defined Profile or the Auto Generated Profile, which then generates the SEPxxxxxxxxxxxx.cnf.xml file for the phone.

In this example, the phone has a MAC address of SEP000011112222. The phone is configured for Extension Mobility and the Log Out Profile is Use Current Device Settings. When the administrator chooses the current device settings for the logout profile, three things occur:

- It causes the file ADP000011112222.cnf to be created.
- The file SEP000011112222.cnf is generated based on the ADP000011112222.cnf file.
- A new SEP000011112222.cnf.xml file is generated based on the new SEP000011112222.cnf file.

**Figure 1**



The user wants to log into a phone that is configured for Extension Mobility. When the user logs into the phone, these operations take place.

- The `SEP000011112222.cnf` file is created from the `JoesMEProfile.cnf` file.
- The `SEP000011112222.cnf.xml` file is generated for the phone.
- The database layer (DBL) sends a restart request to the phone.

When the phone requests its configuration file, the file now contains the device profile for this user's phone.

The key to understanding devices and Extension Mobility is that once Extension Mobility has been enabled for a device, the device uses the device profile at all times. If no one is logged in, the phone uses either an Auto Generated Profile or a User Defined Profile. When logged in, the device uses the Logged In Device profile.

# Login Call Flows

The /LoginService performs many tasks to make Extension Mobility work. These tasks include DBL interaction. First, it modifies a device's loginuserid and loginTime fields in the Microsoft SQL Server database. Second, the system creates a new cnf.xml based on the profile chosen. After this new XML file is created, a Restart is issued to the phone and the new XML file is ready to use the line appearances and speed dials.

## Login (hotel.aef)

Complete these steps:

1. Click **Services**.

This queries services for the phone user that wants to login. If login/logout is defined for the phone device, those services are presented.

2. Click **Login**.

The service sends an HTTP request to the application server to the /login trigger.

3. If the device name is not presented during the /login request, the /login script discovers the device name by querying \\ip\_addr\DeviceInformationX and extracting the Hostname field.
4. After discovery, check to see if a UserID/Password is passed.

The first time selection of the login service does not have a UserID/Password, the script sends XML input to the phone to get the UserID and Password. The phone displays "Please sign on" and the script ends.

5. Once the UserID/Password is entered, the information is sent to the application in the form of a new /login trigger that contains the UserID/Password.
6. The UserID/Password is received by the application. It then performs an authentication to the DC Directory (locally) for the UserID/Password to verify the user.
7. The /login script sends an HTTP request to the publisher Cisco CallManager /LoginService to perform the appropriate DBL operations. The information passed to the /LoginService includes:
  - ◆ ApplicationUserID, ApplicationUserPassword
  - ◆ Device Identifier (MAC Address)
  - ◆ Mobility Extension UserID/Password
8. The Cisco CallManager /LoginService uses the ApplicationUserID and ApplicationUserPassword to perform a user login on behalf of the user. This is why Authentication Proxy Rights are required for the ApplicationUserID.
9. The /LoginService adds the UserID and login time to the device.
10. The /LoginService then fires off a DBL notification to restart the affected device to get the new profile.
11. The /LoginService registers the login with Logout Service (for automatic logout).
12. The user is now logged in.

## Logout (hotelout.aef)

Complete these steps to logout:

1. Click **Services**.

This queries services for the phone the user wishes to logout on. If login/logout is defined for the phone device, those services are presented.

## 2. Click **Logout**.

This service sends an HTTP request to the application server to the /logout trigger.

3. The device name (MAC Address) is not present during the /logout request. Therefore, the /logout application issues an `\\ip_addr\DeviceInformationX` and extracts the Hostname field to determine what phone requests logout services.
4. After the device name is retrieved, the /logout script sends an HTTP request to the publisher Cisco CallManager /LoginService to perform the appropriate DBL operations for logout. The information passed to the /LoginService includes:

- ◆ ApplicationUserID, ApplicationUserPassword
- ◆ Device Identifier (MAC Address)

**Note:** There is no bulk Extension Mobility logout capability until Cisco CallManager 4.2(3) administration pages based on Device pool, location and DN range.

5. Cisco CallManager /LoginService uses the ApplicationUserID and ApplicationUserPassword to perform a logout on behalf of the user. This is why Authentication Proxy Rights are required for the ApplicationUserID.
6. The /LoginService removes the UserID and login time to the device that is logged into, and removes the logout request from the Logout Service.
7. The /LoginService then fires off a DBL notification to restart the affected device to get the new profile.

**Note:** In order to allow the users to enter only numeric characters when they attempt to log in to extension mobility, you can use this Extension Mobility service parameter: `Alphanumeric User ID`.

## Troubleshoot Extension Mobility

When you troubleshoot Extension Mobility problems, there are check points along the way to determine where a problem occurs. Here are the steps and where to look for the problem.

<b>Problem</b>	<b>What to Check</b>
Services returns invalid host or nothing.	Check the Services URL entry in Enterprise Parameters.
Services returns "No services Configured..."	Check the services for the phone or user profile selected. Also, ensure that voice VLAN is configured correctly.
After "login" or "logout" is selected, the phone displays "requesting".	Check to make sure the Application Engine is running. Check the URL specified for the service. Make sure it points to the right IP address (CRA server) and port 8080. Also check to see if port 80 is blocked from the CRA server to the IP phone. If the CRA server is co-located with the Cisco CallManager, check to make sure the Application server does not have proxy enabled and that a proxy server is not configured in Microsoft Internet Explorer for the account the service uses to login.
After "login" or "logout" is	Check the trigger in CRA. The trigger name and URL in Cisco CallManager must match exactly.

selected, nothing happens.	<b>Note:</b> The trigger name and URL are case sensitive.
After the user name and password are entered, the phone displays login screen again.	The service port is not set correctly. Replace the existing form.jsp with form.jsp.
After the user name and password are entered, the phone displays "authentication error".	Check the userid and password. Also check the DC Directory on the CRA server for replication issues. If you run CRA Server 2.2.(3a) or earlier, <del>and use the Active Directory Plugin, check to</del>
After the user name and password are entered, the phone displays "App authentication error".	make sure the user is located directly underneath the User Base, and not under a Sub-OU of the User Base.  Check the Application user ID and password on the CRA server.
After the user name and password are entered, the phone displays "Proxy Not Allowed".	Check the application user ID in Cisco CallManager has <del>Enable Authentication Proxy</del>
After user name and password are entered, the phone displays "LoginServer conn. error".	<b>Rights</b> selected.  <del>Check Common Problems for a solution.</del>
Login and Logout are successful but experiences a significant delay.	Check if a proxy is used. If this is the case, try to disable it. This is located under <b>Tools &gt; Internet Options &gt; Connections &gt; LAN settings</b> in Microsoft Internet Explorer. You must restart for the change to take effect.

Whenever there is a problem with the authentication of any user (either an Extension Mobility user or the application userid), use `http://cm_ipaddr/ccmuser` and attempt to log in. If login fails, then the problem is not related to Extension Mobility. The problem is a more generic authentication issue. Verify the username / password in your directory.

Another test to verify that the LoginService functions properly is to access `http://cm_ipaddr/LoginService/Tools/sampleloginapp.asp` for Cisco CallManager releases 3.x and `http://cm_ipaddr/emservice/jsp/Tools/sampleloginapp.jsp` for Cisco CallManager releases 4.0 and later. Input the appropriate values for the fields. The profile ID is the Extension Mobility device profile to log in. The sample login test eliminates any dependencies on the CRA server and ensures that the directory services work.

## Common Problems

### When a user reverts back to default profile, services are no longer available.

- **Problem:** After the services are added to the phone, the **Update** button is not pressed and the AutoGenerated Default profile is out of sync with the phone.
- **Solution:** Reselect the phone, add the services on the phone and update the phone configuration.

### Extension Mobility logs out user after a few minutes, before the configured time.

- **Problem:** When the user is logged in using Extension Mobility, the user is logged out after a few minutes, even though the default maximum time for the login is set to 8 hours.
- **Solution:** If you do not need to specify the maximum time the user is allowed to be logged into Extension Mobility, always keep the Enforce Maximum Login Time\* parameter to **False**. In order to do this, complete these steps:

1. Go to the Cisco CallManager Administration page
2. Choose **Service > Service Parameters** and select **Cisco Extension Mobility**.
3. Make sure that the Enforce Maximum Login Time\* parameter is set to **False**.
4. Click **Update**.

### After login, the user does not have any services available.

- **Problem:** The User Profile did not have any services associated with it when loaded on the phone.
- **Solution:**

1. Change the User Profile to include the **login/logout** services.
  2. Change the phone the user is logged in on to include the **login/logout** services.
- Once updated, the user gets the logout service.

## 'Host not found' Error in IP Phone

- **Problem:** The IP phone displays the "Host not found" error when the **Services** button is pressed.
- **Solution:** Choose **System > Enterprise Parameters**. Check the **URL services**, and if it is set to the CallManager Server name, replace the CallManager Server name with the IP address as shown in this example.

**Example:** `http://10.10.10.1/CCMCIP/getservicesmenu.asp` , where 10.10.10.1 is the Cisco CallManager IP address.

Stop/start the TFTP, Internet Information Server (IIS), and Computer Telephony Integration (CTI) services and reboot the phones for the change to take affect.



## After a login or logout is performed, the phone resets instead of restarting.

- **Problem:** The phone uses DNS to resolve the Cisco CallManager name.
- **Solution:** Change **System > Server name** to an IP address. Reset the phone and try the login/logout procedure again.

## Services return HTTP [8] error.

- **Problem:** The phone is attacked by the Code Red Virus and the HTTP services no longer function.
- **Solution:** Apply the latest phone loads from the Cisco Web site to correct this problem.

## "Login Unsuccessful:[101]" error returned on login.

When you launch the Extension Mobility (EM) service on the IP phone, this error message appears: Login Unsuccessful Error:[101].

**Note:** This error can be related to one of these problems.

- **Problem:** The username entered is not found in the DC Directory which can be also due to DC Directory replication issues.
- **Solution:** Add the user through the Cisco CallManager global directory. Also verify that DC Directory replicates between servers. For more information on how to resolve DC Directory replication problems between DC Directory server services that run on Cisco CallManager servers involved in a Cisco CallManager cluster, refer to Fixing Problems with DC Directory.

- **Problem:** The IP address for the Cisco CallManager Publisher changed.
- **Solution:**

1. Select **cisco.com > CCN > systemProfiles** in DC Directory Administration.
2. Select **Hoteling Profile**.
3. Verify the IP address in the URL field. This should be the IP address of the Cisco CallManager publisher.

**Note:** Refer to Changing the IP Address for Cisco CallManager for more information on how to change the IP address.

- **Problem:** An error during the setup of the Extension Mobility Service Virtual Directory.
- **Solution:** The Virtual Directory can be recreated with these steps.

1. Complete these steps to delete the existing Virtual Directory.
  - a. Select **Start > Programs > Administrative Tools > Internet Information Services (IIS)**.
  - b. Expand **PC > DefaultWebsite** in the left pane.
  - c. Right click **Login Service**, and select **Delete**.
2. Complete these steps to clean up the directory.
  - a. Rename the directory *C:\CiscoWebs\LoginService\* to **C:\CiscoWebs\OldLoginService\**.
  - b. Create the directory **C:\CiscoWebs\LoginService\**.
  - c. Copy these files from the *C:\CiscoWebs\OldLoginService\* to the **C:\CiscoWebs\LoginService\** directory.

- a. Tools\ (directory and its contents)
  - b. login.asp
  - c. query.asp
  - d. loginSecure.asp
  - e. querySecure.asp
  - f. \*.dtd
3. Complete these steps to re-create the Virtual Directory.
  - a. In the Internet Services Manager (opened in step 1), right-click **Default Web Site**, and select **Virtual Directory**.
  - b. Follow the wizard.
    - a. Alias: **LoginService**
    - b. Directory: Browse to **C:\CiscoWebs>LoginService**
    - c. Select **Read, Run, and Execute**
4. Complete these steps to configure the Virtual Directory.
  - a. Right-click **Login Service**, and select **Properties**.
  - b. Select the Virtual Directory tab.
    - a. Verify that **Read** and **Log Visits** are checked, no others.
    - b. Verify that Execute Permissions is set to **Scripts and Executables**.
    - c. Verify that Application Protection is set to **Low (IIS Process)**.
  - c. Select the Documents tab, and verify that the only enabled default document is **Default.asp**.
  - d. Select the Directory Security tab and click **Edit** under Anonymous Access and Authentication Control.
    - a. Verify that **Anonymous Access** is the only option that is checked.
    - b. Click **Edit** under Anonymous Access.
    - c. Set the username to **CCMEML**.
    - d. Set the password to **CCMEML**.
    - e. Click **OK**.
  - e. Click **OK**.
5. Restart the IIS services.

## Error No: -32

When a user clicks on **Device Association** or **Extension Mobility** in an attempt to associate a user profile from the Cisco CallManager Administration User Configuration page, the user receives the Error No: -32 error.

This error can occur when the users in Active Directory are modified or renamed, even if you rename the user back to the original userid. Every time a user is modified, the `ciscoAtUserProfile` and `ciscoAtAppProfile` attribute is created and updated for the user. If the `ciscoAtGUID` attribute is not present, the new user profile DN is created. In order to solve this issue you need to use the Active Directory Services Interface (ADSI) edit utility. On the Active Directory (AD) server, you can browse your directory schema when you open the ADSI edit utility. Drill down to `dc=xxxxx, dc=com, ou=Cisco` (or whichever OU you specified during the installation of the AD plugin on Cisco CallManager), `ou=Profiles`. All the profiles can be found in that directory.

In order to install the ADSI edit utility on the system, install the support tools from the Windows 2000 CD located at `<CD drive>:\SUPPORT\TOOLS\setup.exe`. Copy `adsiedit.exe` and `adsiedit.dll` into a folder on the system. The folder should be named `c:\adsiedit\`. Register `adsiedit.dll` by running `regsvr32.exe`

c:\adsis\adsiedit.dll after the c:\winnt\system32 command prompt.

Complete these steps:

1. Launch the ADSI edit utility in order to directly look at the attributes in the Active Directory for the user that has a problem with association.
2. Navigate to the user entry (for example, CN=user1, OU=yourOU, DC=yourDC, DC=com). Right-click the object, and choose **Properties**. Under Select a property to view, select the **ciscoatGUID**.
3. Clear the current value present for the **ciscoAtGUID** attribute.
4. Select the **ciscoatUserProfile** attribute for this same user, and clear it.
5. Select the **ciscoatUserProfileString** attribute for the same user, and clear it.
6. Then try to associate a device to the user from the Cisco CallManager Administration pages.

## Services do not appear when "services" is pressed.

- **Problem:** The phone device used does not have the services selected.
- **Solution:** Reselect the services on the phone and update the phone page.

## After a user logs in, the phone does not have any services.

- **Problem:** The user that has logged in does not have any services associated with their User Device Profile.
- **Solution:** Either through the Cisco CallManager User page or the User Device configuration page, add the desired services to the User Device table.

## After the username and password are entered, the phone returns to the login screen.

- **Problem:** The form.jsp that is sent to the phone for the login is not able to resolve the port to be used for the login. As a result, the login request is never seen by the application.
- **Solution:** Download form.jsp. Replace the existing C:\Program files\wfaavid\tomcat\webapps\ROOT\form.jsp with the downloaded file. This new form hard sets the service port number to 8080.

## After username and password are entered, system generates "LoginServer Conn. error".

**Note:** This error can be related to one of these problems.

- **Problem:** The IBM 340 series servers do not have anonymous access correctly configured for login (Cisco bug ID CSCdu62820 (registered customers only)).
- **Solution:** Enable Microsoft IIS to control the password for anonymous devices.
- **Problem:** The IP address for the Cisco CallManager Publisher changed.
- **Solution:**
  1. In DC Directory Administration, go to **cisco.com > CCN > systemProfiles**.
  2. Select **Hoteling Profile**.
  3. Verify the IP address in the URL field. This should be the IP address of the Cisco CallManager publisher.

- **Problem:** When integrating with Microsoft Active Directory, the base context for the applications engine is incorrect.
- **Solution:** On the Application Server, set the base context to include a cisco ou (not just a cisco dc). So, for the company mycompany.com, the base context is ou=cisco, dc=cisco, dc=mycompany, dc=com (change the mycompany entry to the site specific name).

**Note:** When the base context is changed, the application settings must be reconfigured to find the directory information in the new context.

- **Problem:** Check the `http:\\cm_ipaddr\LoginService\Tools\sampleloginapp.asp` for Cisco CallManager releases 3.x and earlier. For Cisco CallManager releases 4.0 and later use `http:\\cm_ipaddr\emservice\jsp\Tools\sampleloginapp.jsp`. If the error returned is `Error Parser Class Not Found org.apache.xerces.parsers.SAXParser null`, then during installation, the Virtual directory is not created and the ClassPath is not inserted.
- **Solution:** The installation failed in some manner (root cause not yet determined).
  1. Under Default Web Site, create a new virtual web named LoginService. The local path should be `C:\CiscoWebs\LoginService`. Change the application protection to **High** (Isolated). Next, follow the steps to allow Microsoft IIS to control the password for Anonymous devices.
  2. Once the virtual web is created, the system variables for ClassPath must be added to allow the SAX parser to perform its tasks. Right-click and select **My Computer > Properties > Advanced > Environment Variables**. If the ClassPath variable does not exist, create the variable. The value for ClassPath should be: `C:\WINNT\Java\Lib\DirUser.jar;`  
`C:\WINNT\Java\Lib\Xerces.jar;`  
`C:\WINNT\Java\Lib\DirUserNotification.jar`. Click **OK** three times to save the new environment variable.
  3. Stop and restart the IIS services.

## When logging in on a Cisco 7940 phone, the phone displays the error "Device profile does not exist".

- **Problem:** Extension Mobility requests a fixed name for the device template that must be used on a Cisco 7940 phone when logging in. The name of the device template for the 7940 must exist and have the exact name of the template when the server is installed.
- **Solution:** Make sure the device template for the Cisco 7940 is 7940 1-Line or 7940 2-Line. Ensure that a dash is used and the capitalization is correct.

## XML Error [4] Parse Error is returned when selecting the login service.

- **Problem:** The form.jsp downloaded includes HTTP header information.
- **Solution:** On this page, right-click on the **form.jsp**, then select **Save Link As** or **Save Target As**. Select the location to download the form. Ensure that the first line of the form.jsp page reads: `<%@page import="java.net.InetAddress" %>`

## Users are unable to log in to Extension Mobility and receive the login unsuccessful error 6.

- **Problem:** User receives the `login unsuccessful error: [6]` error when pressing **Select** for the Extension Mobility service on the phone.
- **Solution:** Error 6 indicates an error when communicating with the database. This can be caused by many different things depending on whether DC Directory or Active Directory is used. In the case of

Active Directory, this issue can be resolved when you run the Active Directory plugin again. For more information on the Active Directory installation, refer to Active Directory 2000 Plugin Installation for Cisco CallManager.

This issue can also occur if there is no device profile associated with the user that attempts to log in. Check if the users have device profiles associated with them under the User Configuration > Extension Mobility page. If not, update users with device profiles for Extension Mobility login.

## "Login unsuccessful [9]" error message is generated on the phone.

- **Problem:** The user is unable to login to a phone, and receives a Login unsuccessful [9] error message when trying to login using Extension Mobility.
- **Solution:** This is normally a directory integration error. This could be LDAP, Active Directory, or DC Directory for example. Based on what method of directory integration is used, troubleshooting can vary.

Check that the Active Directory server is running. If there is an issue here, run the Directory plugin, and Adminutility from Cisco CallManager.

If the problem exists with LDAP, check that the DirUser.jar file is present.

This issue can also occur if there is no device profile associated with the user that attempts to login. Check if the users have device profiles associated with them under the User Configuration > Extension Mobility page. If not, update users with device profiles for Extension Mobility login.

## Login unsuccessful Error [12]

- **Problem:** When logging into an IP phone enabled with Extension Mobility, the login fails and the phone displays Error[12].
- **Solution:** This error occurs when the User Device Profile is improperly configured. Either the Device Profile does not exist, is mis-configured, or is not associated with the user profile. Check all the User Device Profile settings, and ensure that there is a properly specified device profile, and a correct association with the user profile.

## Users are unable to log in to Extension Mobility and receive the "login unsuccessful error: [3]" or "error: [10]" or "error: [2]" after installing the Active Directory plug-in.

- **Problem:** The Extension Mobility phone login is unsuccessful with the Active Directory because the Password field for all of the application users in the registry is empty.
- **Solution:** Complete these steps to resolve this issue:

1. Select **Start > Run**, type **regedit**, and click **OK**.
2. Check the registry entry for Cisco CallManager Extension Mobility located at **HKEY\_LOCAL\_MACHINE\SOFTWARE\Cisco Systems Inc.\Directory Configuration\AppUsers\CCMSysUser**.
3. Make sure that an entry exists for the Password field, and that the userID is **CCMSysUser**. If this entry is not there or the entry is wrong, a problem exists with the installation. You can now reset or add a password for this user. Complete these steps to change the CCMSysUser password.
  - a. Go to **C:\dcdsrvr\bin** and execute the **CCMPWDChanger.exe** application.

- b. Specify your Active Directory password. At this point you can choose to change the userID (in this case, CCMSysUser) and set a password for this user.
- c. Restart the **IIS Admin** service and the **Cisco Tomcat** service from **Start > Programs > Administrative Tools > Services**.

If this procedure does not resolve the issue, you might need to uninstall and reinstall the Active Directory plugin. Refer to the Active Directory 2000 Plugin Installation for Cisco CallManager for more information on how to install the Active Directory plugin.

**Note:** If the issue started to occur after a Cisco CallManager upgrade, refer to Cisco bug ID CSCdz60740 (registered customers only).

## Error [18]– Another User logged in

- **Problem:** When you try to log in to the IP phone using Extension Mobility, the error message `error [18] - Another user logged in` is received even though no user is logged in. The userID of the Extension Mobility user logged in is shown as None. When you try to delete the phone, it fails with the error `Delete Failed [438] User defined Device Profile cannot be deleted if it is in use`.
- **Solution:** This issue can occur if any application user has control of the phone and the Application User ID is shown as None. Go to **User Management**, select **Application User**, and unassociate it. You are now able to delete the phone.

## Extension Mobility service returns error [100] login unsuccessful when the service to login to Extension Mobility is chosen.

- **Problem:** When a user presses the **Services** button, the phone displays `Error [100]`.
- **Solution:** This error occurs if the URL for the Cisco Extension Mobility service does not include the last parameter (shown in bold):

`http://<IPAddressofCallManager>/emapp/EMAppServlet ?device=#DEVICENAME#`

<IPAddressofCallManager> specifies the IP address of the Cisco CallManager server where Cisco CallManager Extension Mobility is installed. Make sure that the URL is correct and complete.

For example, `http://10.45.67.89/emapp/EMAppServlet?device=#DEVICENAME#`: the URL is case-sensitive; make sure that you enter the name exactly as described.

## Login unsuccessful error: [11]

- **Problem:** When a user tries to login to Extension Mobility, the IP phone displays: `Login Unsuccessful Error:[11]`.
- **Solution:** This error occurs if the URL for the Cisco Extension Mobility service is not entered correctly in the IP phone service parameter.

On **CCMAdmin**, go to **Feature > IP Phone services**. Then do a search for your Extension Mobility service. Make sure that the URL matches this one:

`http://<IPAddressofCallManager>/emapp/EMAppServlet ?device=#DEVICENAME#`

## Login unsuccessful Error:[6]

**Problem** When the Extension Mobility (EM) service was launched on the IP phone, the IP phone displays: `Login unsuccessful Error:[6]`. The issue is only in the Publisher.

**Solution** Error 6 indicates an error when communicating with the database. Complete these steps in order to resolve the issue.

1. Make sure the **C:\dcdsrvr\DirectoryConfiguration.ini** file is populated and that this file is identical on all the Cisco CallManager servers in the cluster. If this file is absent or not populated in any of the servers in the cluster, the login fails.
2. Change the **UserSSL** setting in the **C:\dcdsrvr\DirectoryConfiguration.ini** file from True to **False**.

## Unable to apply the Extension Mobility feature to an IP phone and receive the error "Already logged in to another phone"

- **Problem:** When you try to apply the Extension Mobility feature to an IP phone, the request is denied with an error that says you are already logged in to another IP phone. This situation arises when you are already logged in to an IP phone and want to log in to a new IP phone before you log out from the previous phone.
- **Solution:** The best way to log out from the previous phone and log in to the new one is to change several service parameters in the Cisco CallManager Administration page as shown:

1. In the Cisco CallManager Administration window, go to **Service > Service Parameters**.
2. Choose the Extension Mobility service, and, in the **Multiple Login Behavior** box, change it to **Auto Logout**. Click **Update**.

**Auto Logout:** After a user logs in to a second device, the Cisco CallManager automatically logs the user out of the first device.

**Note:** In order to find which IP phone the user is logged in to, go to **Microsoft SQL Server > Enterprise Manager > Databases > Tables**; open the table **Device**, and check for the field called **loginUserID**. This shows the IP phone to which the user is logged into and, once you find the phone, you can also log off the user from the phone itself.

## Error: "Update failed. Could not insert new row – duplicate value in a UNIQUE INDEX column"

If a phone configured for Extension Mobility (EM) is deleted when a user is logged, the CallManager allows the Administrator to delete the phone through bulk administration. When an attempt is made to add the phone back with the EM option along with "Log Out Profile" checked, it may give this error message: Update failed. Could not insert new row – duplicate value in a UNIQUE INDEX column.

**Note:** Removing a phone that has a logged in user through the phone page is prevented by the GUI.

**Solution**– This problem seems to happen when the deleted phone is configured for EM and a user is logged in at the time of deletion. In order to resolve this issue, remove the old ADP[mac-address] profile from the route plan report.

This is documented in Cisco Bug ID CSCsj63279 (registered customers only) .

- **Problem:** Extension Mobility cannot be turned on for a Cisco 7900 IP Phone, and this error message appears:

Update failed. Could not insert new row – duplicate value in a UNIQUE INDEX column

The root cause of the problem is the intermittent failure to delete the auto-generated device profiles (ADP) for a phone. If you delete phones that are configured for extension mobility with the logout profile set to use `current`, it leaves an ADP in the database. This results in the inability to reinsert this phone into the database.

- **Solution:** In order to workaround this issue, complete these steps:

1. Use CallManager Administration in order to find and delete the orphaned auto-generated device profile. In order to do this:
  - a. Choose **Device > Device Settings > Device Profile**.
  - b. Click **Find > All**.
  - c. Delete the ones that are not associated to any of the IP phones.
2. Restart the device.

## "Warning 7" Appears During Login to Extension Mobility IP Phone

- **Problem:** When you log into Extension Mobility IP phone, the `Warning 7` message appears.
- **Solution:** Complete these steps in order to resolve this issue:

1. You can see all the the applications served by Tomcat at `http://<IPAddr of the server>/manager/list`. Determine whether Extension Mobility is listed here and running.
2. Restart the Extension Mobility and Tomcat services during the off-peak hours.

## Extension Mobility Access is Slow

- **Problem:** Extension Mobility Access is slow in Callmanager.
- **Solution:** Low memory resource on the Callmanager could cause this issue. Make sure that your CallManager server meets the minimum hardware requirements when you upgrade to higher version.

## IP Phones Stuck in "Registering" or "Configuring IP" Status After Log Out

If the IP phone stays in `Registering` or `Configuring IP` status after the user logs out of Extension Mobility, check to see if the Logout Profile is assigned to the device. Also, restart the Cisco Tomcat service.

**Note:** If you use Cisco CallManager 6.x, you can restart the Cisco Tomcat service from the CLI with this command: **admin: utils service restart Cisco Tomcat**

## Extension Mobility Users Automatically Logged Out in Short Intervals

Extension Mobility users are kicked out of the system every 5 minutes and the event log shows the `Error: DeviceTransientConnection - Transient connection attempt error` message. This issue can occur if the time on the Cisco CallManager Publisher and Subscriber are out of sync. In order to resolve this issue, you need synchronize the clock on all servers or configure `ntp` in the cluster for time synchronization. Also, change the Extension Mobility Service Parameter **Multiple Login Behavior** to **Multiple Login's Not Allowed** and restart the Extension Mobility Service.

## No Results when Searching the DN Assigned to the Device Profile

When an Extension Mobility user logs into a phone, searching the directory number (DN) assigned to the device profile yields no results.



1. Go to **Device > Phone**.

The Find and List Phones window appears.

2. Choose **Actively Logged In Device Report** from the drop-down list, and click **Go**.

The Find and List Actively Logged In Device window appears.

3. Choose the directly number, and click **Find**.

Refer to Finding an Actively Logged-In Device for more information.

## Unable to Logout an Entire Group of Users from Extension Mobility

Complete these steps in order to log out an entire group of users from Extension Mobility:

1. Disable the Extension Mobility service under **Serviceability > Tools > Control Center**.
2. Reset the device pool that contains all the phones that needs to be logged out. This will log out all the users that currently use Extension Mobility.

## Extension Mobility

Extension Mobility does not work after the Cisco CallManager 8.6 upgrade.

### Solution

Complete these steps in order to resolve the issue:

1. Choose **OS Administration page > Security > Certificate management** in order to regenerate Cisco Tomcat.pem certificates on all the servers and work on the publisher first and then the subscribers.
2. Restart the Trust verification service (TVS) on all the servers and start from the publisher.
3. Restart the TFTP service on all the servers and begin first with the publisher.
4. Restart the Cisco Tomcat Service on all the servers and start first with the publisher. Use the **utils service restart Cisco Tomcat** command in order to restart the service from the CLI of a server.

### Problem

Here are some of the common issues that you can face when you use the Extension Mobility. The solution is also provided.

- You are not able to log into extension mobility.
- You are unable to log into Extension Mobility with the UserID and PIN and the `Error = [ 201 ] - Authentication Error` error message appears.
- You are unable to login to Extension Mobility and the 205 error message appears.

### Solution

Complete these steps in order to resolve the issue:

1. Ensure that the End User is associated with the appropriate Device Profile to the Extension Mobility.
2. On **Cisco Unified Serviceability** page, choose **Tools > Service Activation**.
3. Ensure that **Cisco Extension Mobility** is activated.

**Cisco Unified Serviceability**  
For Cisco Unified Communications Solutions

Alarm Trace Tools Samp Help

**Service Activation**

Save Set to Default Refresh

**Status**  
Status: Ready

**Select Server**  
Server: [dropdown] Go  
 Check All Services

**CM Services**

	Service Name	Activation Status
<input checked="" type="checkbox"/>	Cisco CallManager	Activated
<input type="checkbox"/>	Cisco Tftp	Deactivated
<input type="checkbox"/>	Cisco Messaging Interface	Deactivated
<input type="checkbox"/>	Cisco Unified Mobile Voice Access Service	Deactivated
<input type="checkbox"/>	Cisco IP Voice Media Streaming App	Deactivated
<input type="checkbox"/>	Cisco CTIManager	Deactivated
<input checked="" type="checkbox"/>	Cisco Extension Mobility	Activated
<input type="checkbox"/>	Cisco Extended Functions	Deactivated
<input type="checkbox"/>	Cisco Dialed Number Analyzer	Deactivated
<input checked="" type="checkbox"/>	Cisco DHCP Monitor Service	Activated

**CTI Services**

4. Choose **Tools > Control Center – Feature Services** and choose the service in order to restart the **Cisco Extension Mobility** service.

Status: Ready  
Status: Ready

**Select Server**  
Server: 10.78.177.6 Go

**Database and Admin Services**

	Service Name	Status*	Activation Status	Start Time	Up Time
<input type="checkbox"/>	Cisco AXL Web Service	Not Running	Deactivated		
<input type="checkbox"/>	Cisco Bulk Provisioning Service	Started	Activated	Wed Jul 27 03:38:30 2011	30 days 22:08:15
<input type="checkbox"/>	Cisco TMS Service	Not Running	Deactivated		

**Performance and Monitoring Services**

	Service Name	Status*	Activation Status	Start Time	Up Time
<input type="checkbox"/>	Cisco Serviceability Reporter	Not Running	Deactivated		
<input type="checkbox"/>	Cisco CallManager SNMP Service	Not Running	Deactivated		

**Directory Services**

	Service Name	Status*	Activation Status	Start Time	Up Time
<input type="checkbox"/>	Cisco DirSync	Not Running	Deactivated		

**CM Services**

	Service Name	Status*	Activation Status	Start Time	Up Time
<input type="checkbox"/>	Cisco CallManager	Started	Activated	Thu Jul 21 08:45:29 2011	36 days 19:01:16
<input type="checkbox"/>	Cisco Tftp	Not Running	Deactivated		
<input type="checkbox"/>	Cisco Messaging Interface	Not Running	Deactivated		
<input type="checkbox"/>	Cisco Unified Mobile Voice Access Service	Not Running	Deactivated		
<input type="checkbox"/>	Cisco IP Voice Media Streaming App	Not Running	Deactivated		
<input type="checkbox"/>	Cisco CTIManager	Not Running	Deactivated		
<input checked="" type="checkbox"/>	Cisco Extension Mobility	Started	Activated	Sat Aug 27 00:08:41 2011	6 days 03:38:04
<input type="checkbox"/>	Cisco Dialed Number Analyzer	Not Running	Deactivated		
<input type="checkbox"/>	Cisco DHCP Monitor Service	Started	Activated	Thu Jul 28 23:14:41 2011	20 days 04:32:04

## Problem

Cisco Extension Mobility Cross Cluster restriction is not happening while a user of different Profile is logged in to a different cluster.

## Solution

You need to set **Enable Logical Partitioning = True** in order to resolve this issue.

The system default policy shall be Deny for an enterprise, Logical Partitioning Default Policy = Deny so calls or features are blocked between VoIP device participants' the Allow policies must be configured through **System-> Logical partitioning configuration** on the CUCM.

### **Problem–Login is unavailable(213)**

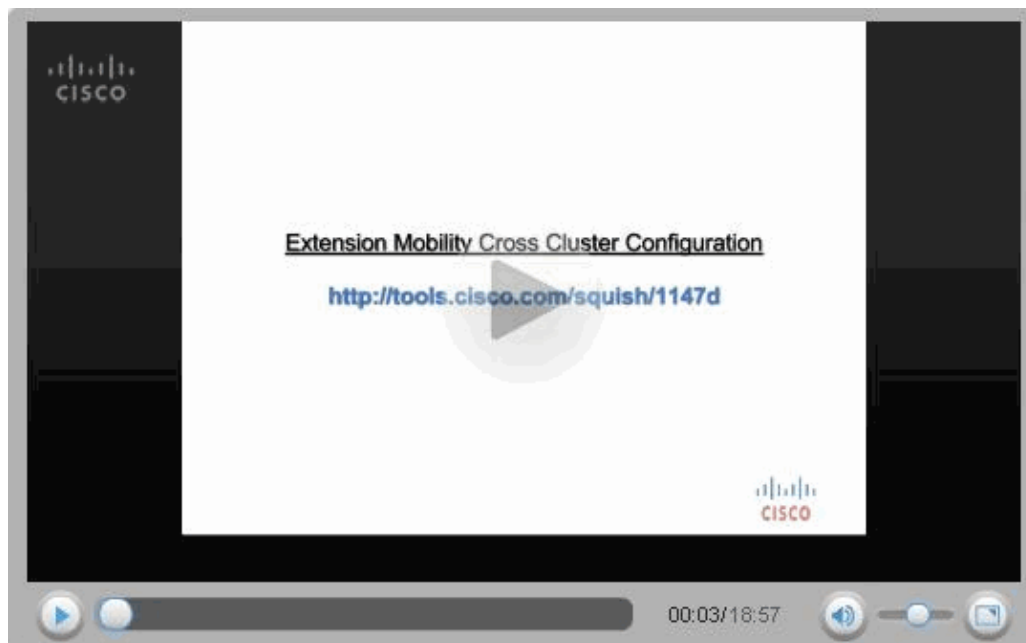
Extension Mobility is configured between two clusters. However, when logging in with a remote cluster UserID, you receive this error message: Login is unavailable(213).

**Note:** New configuration of Extension Mobility Cross Cluster (EMCC).

### **Solution**

The Login is unavailable(213) error message can occur if the device does not support EMCC. This error is displayed when the device or phone load does not support EMCC (for example, non–supported phone models and supported phone models with an older phone load).

Refer to this video on the Cisco Support Community for configuration details: Extension Mobility Cross Cluster Configuration [🔗](#)



## **Related Information**

- **Installing and Configuring Extension Mobility Using Either: Extended Services 2.2; CRA 2.2 or CRS 3.0(2) and CallManager 3.2**
  - **Configuring Cisco CallManager Extension Mobility**
  - **Understanding Cisco CallManager Extension Mobility**
  - **Troubleshooting Cisco CallManager Extended Services**
  - **Extension Mobility and Phone Login Features**
  - **Voice Technology Support**
  - **Voice and Unified Communications Product Support**
  - **Troubleshooting Cisco IP Telephony** [🔗](#)
  - **Technical Support & Documentation – Cisco Systems**
-

