Administration Guide

06 May 2024

TM and copyright © 2010-2024 Imagicle spa

Table of Contents

Administration Guide 1/42
- Description and Architecture 1/42
- Configuration Task List 9/42
- XML Service Configuration 10/42
- Configuration for TAPI 13/42
- Configuration For Curri - ECC 15/42
- Product Configuration 31/42
- Phone Lock Administration 33/42
- License Activation 34/42
- StoneLock REST APIs 35/42
- Troubleshooting 38/42

imagicle

Administration Guide

Description and Architecture

In companies with a large number of phones, unattended phones could be used to make personal calls. Imagicle Phone Lock is the most effective solution to avoid this kind of abuse. Thanks to Phone Lock, company employees can easily lock their phone line, preventing unauthorized people to use it and avoiding any surprise on the company's phone bill.

Phone Lock allows the users to lock or unlock own phone line, on all phone devices associated to it, by hitting IP Phone's Services button, select Phone Lock XML service and entering a PIN code. When the phone is locked, incoming calls may still be answered (or dropped), while outgoing calls are dropped or re-routed to any number (i.e. a voicemail service). Calls to emergency numbers or other specific numbers/ranges might be still available, depending on applied Global Settings.

The users can verify own locking status from a padlock icon or a text message appearing on phone display.

If a user forgets his/her PIN, the UC Suite administrator can reset it through the web interface.

Locking the phone can optionally clear call registry, including the list of missed, received and placed calls.

Phone Lock supports Cisco Unified Call Manager (CUCM/BE6K/BE7K), Cisco HCS or Webex Calling Dedicated. Webex Calling MultiTenant and Cisco Call Manager Express (CCME) are not supported.

Phone Lock is a server based application which can control the telephony traffic using either:

- TAPI (Telephony Application Programming Interface)
- CURRI (Cisco External Call Control Profile)

Note: Starting from Imagicle 2020.Spring.1 release, Phone Lock TAPI engine can selectively lock overlapping extensions, if associated to different partitions and different phone devices.

Product architecture

When Phone Lock detects a call being initiated, it retrieves the user associated to relevant phone line in the UC Suite users' list. Some of the user's properties control the status of the IP phone.

The phone line can be locked by the user for privacy reasons or fraud prevention, either from the phone services interface, from Jabber/Webex client's "Phone Lock" gadget or through the UC Suite web interface. The phone line can also be locked by the administrator.

The phone status is stored in Phone Lock users' list and it can be easily checked and changed through the web interface. When the user accesses the XML service on the IP phone, lock icon is toggled in the list accordingly.

Note: If you are leveraging FAC (Forced Authorization Codes) or CMC (Client Matter Codes) to initiate an outbound call, please do not enable Phone Lock feature. Phone Lock operates at phone device or line level, so other phone devices/lines can still initiate outbound calls using FAC/CMC code of a blocked user.

Available Blocking Methods

Imagicle Phone Lock allows phone line locking by means of below three methods:

User's Lock

Each user can autonomously lock own phone line/device from the following interfaces:

- User's web portal
- Administrator's web portal

- Jabber/Webex Phone Lock gadget
- XML Phone service
- Imagicle One Desktop PC tool (manual or automatic)

Administrator's Lock

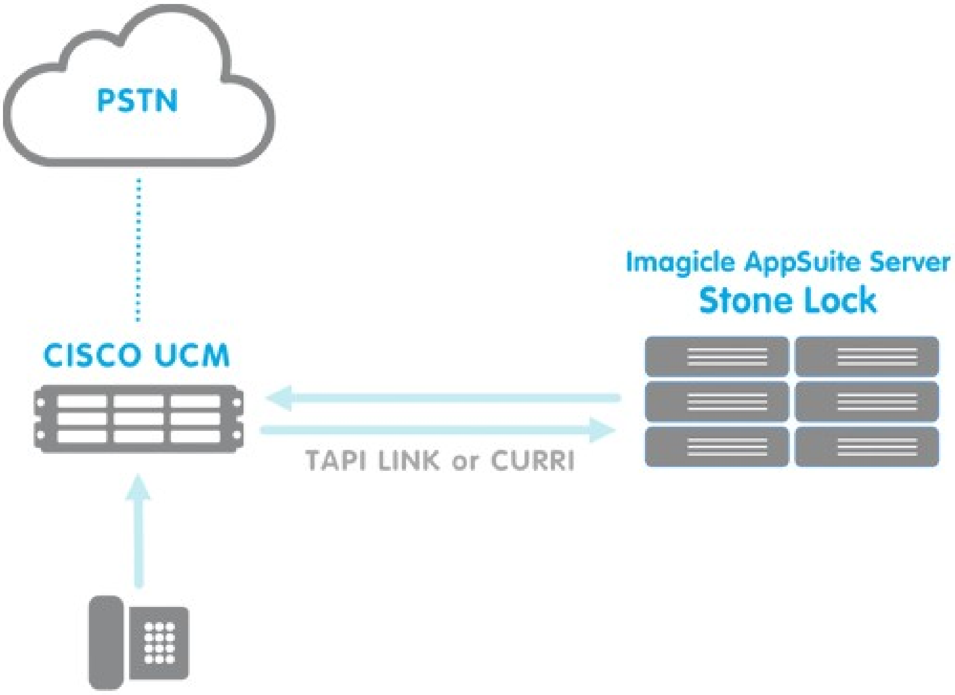
Phone Lock administrator can access to a specific Phone Lock web page called "Users". From this page, administrator can lock any phone line/device. Two option available:

- Standard phone block, by clicking on padlock icon to toggle lock status. This locking method can be reverted by relevant user.
- Administrative phone block, by checking user's "ADMIN LOCK" flag. This locking method does NOT allow user to revert own lock status. User should contact administrator to unlock own line.

In both cases, phone lock behaviour is the same as user's lock.

Budget's Lock

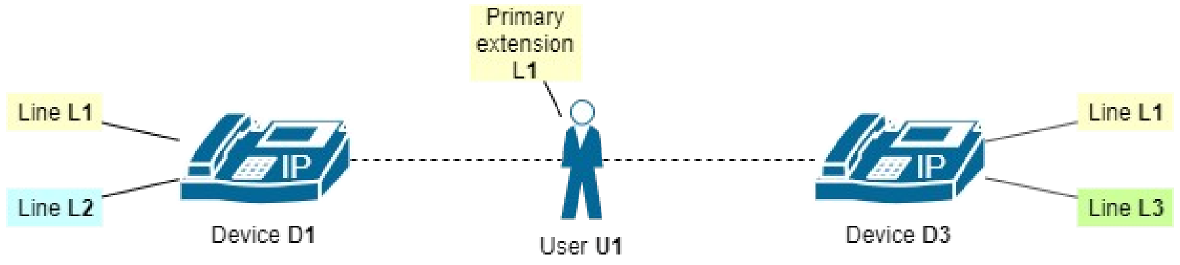
Third locking method implies having Budget Control module enabled, included in Imagicle call Analytics Enterprise license. If a user, or a group of users associated to same department/cost center, reach the assigned budget, the phone line(s) are locked in administrative mode, so if user wants to keep on calling, he/she needs to contact the administrator or wait for the beginning of next budget period.

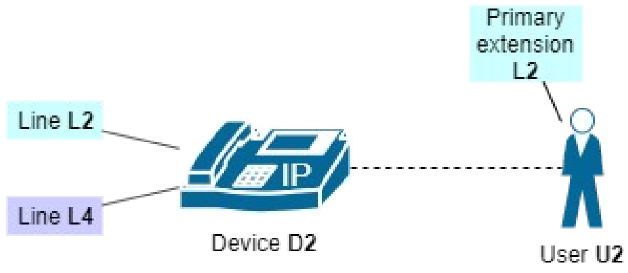


Phone Behaviours

By default, Imagicle Phone Lock only acts on outgoing calls, but you can also enable incoming calls block by checking "**Block Incoming calls when phone is locked**" flag, available in Phone Lock's Global Settings.

Let's consider the following configuration:





Dotted lines represent device - user association, as detected by Imagicle Phone Lock + AXL services.

Some examples

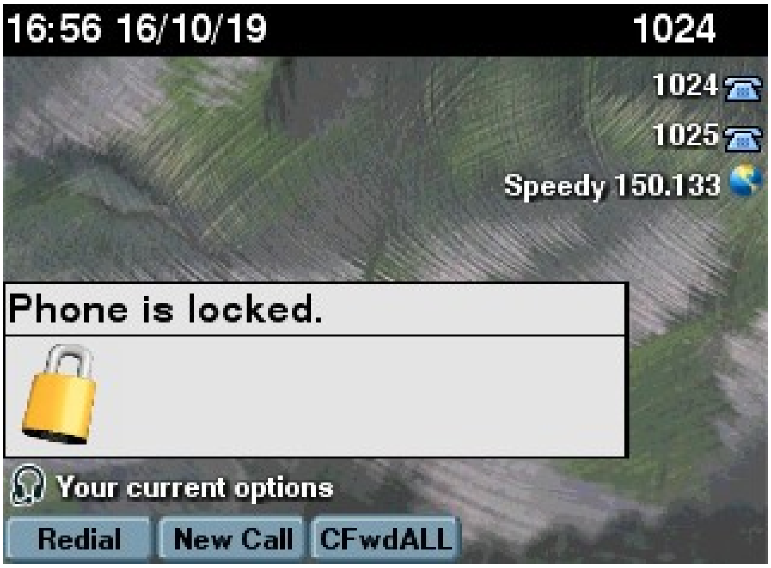
- User **U1** is locked:
  - TAPI
    - On **D1** and **D3** phone sets appear *"Phone is locked"* message
    - All outbound calls from **D1** and **D3** devices are dropped
    - Outbound calls from other devices are allowed
  - CURRI
    - On **D1** and **D3** phone sets appear *"Phone is locked"* message
    - Outbound calls from line **L1** (on both **D1** and **D3**) are dropped
    - Outbound calls from other lines are allowed
- User **U2** is locked:
  - TAPI
    - On **D2** phone set appears *"Phone is locked"* message
    - All outbound calls from **D2** device are dropped
    - Outbound calls from other devices are allowed (even those performed from line **L2** on **D1** phone set)
  - CURRI
    - On **D2** phone set appears *"Phone is locked"* message
    - Outbound calls from line **L2** (on both **D1** and **D2**) are dropped
    - Outbound calls from other lines are allowed
- User **U1** is locked, **L2** is included in the whitelist, conference call
  - TAPI
    - On **D1** and **D3** phone sets appear *"Phone is locked"* message
    - Outbound/inbound calls on line **L2** are allowed
    - If **L2** starts a conference call by including **U1**, conference is allowed
    - If **U1** starts a conference call by including anybody but **L2**, conference is dropped
    - If anybody but **L2** starts a conference by including **U1**, conference is dropped

Lock status on the IP Phone

Depending on Cisco IP Phone model/series, different notification methods are available to show a graphical "lock" icon or a text message on phone display.

Status icon + text popup

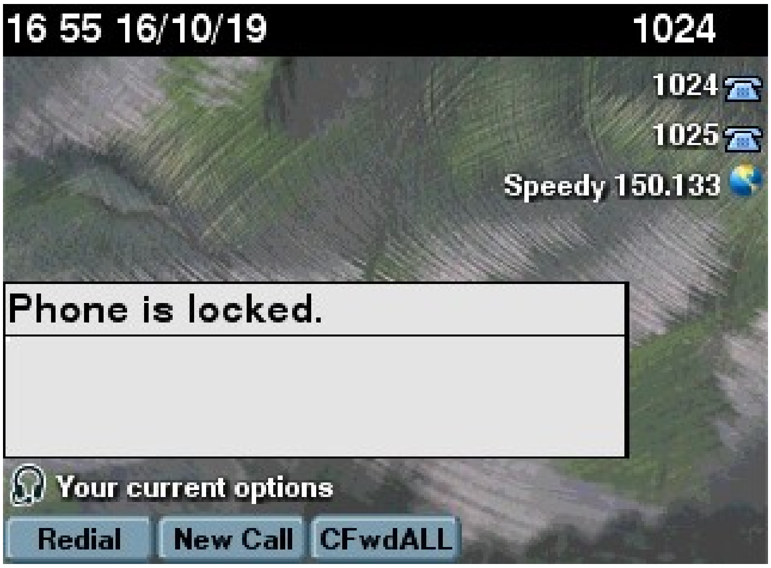
If IP phone supports XML popup message/graphic push, then the following notification appears:



Phone is locked.

Text-only popup

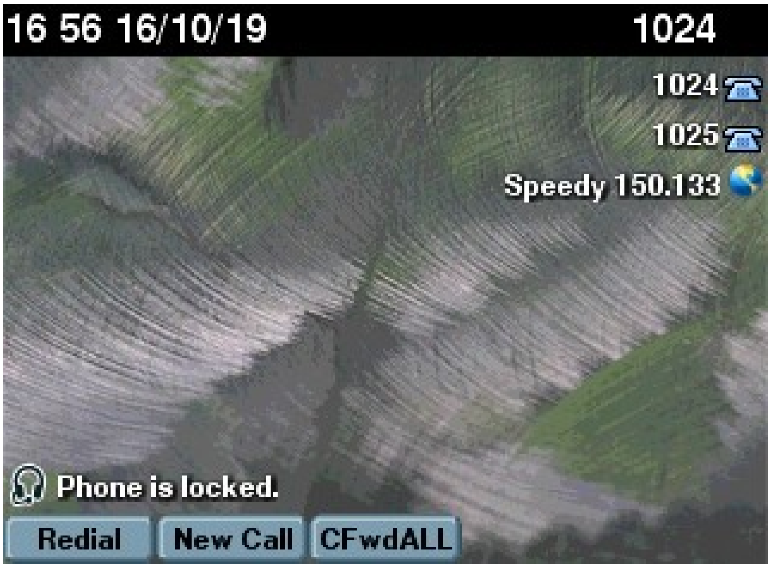
If IP phone supports XML popup message push, then the following notification appears:



Phone is locked.

TAPI-based text notification

If IP phone is monitored via CTI/TAPI, then the following notification might appear:



16 56 16/10/19 1024

1024 ☎

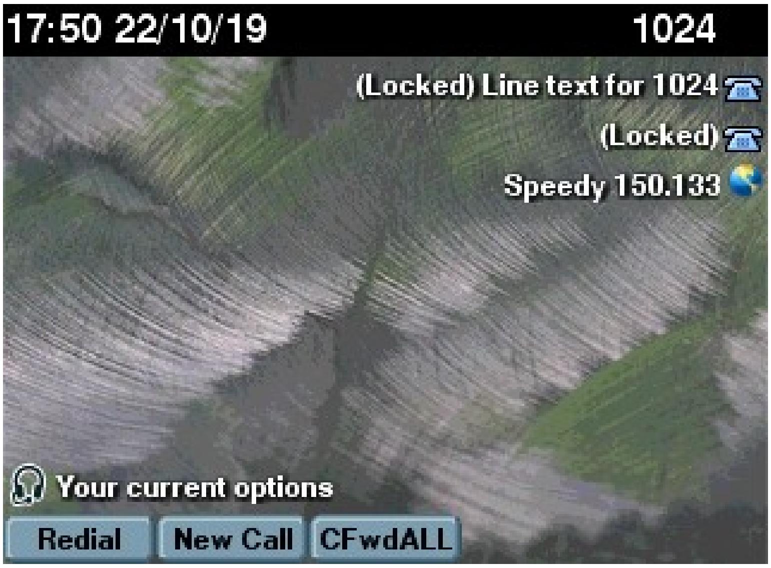
1025 ☎

Speedy 150.133

Phone is locked.

Lock notification included into Phone line text

This new method, available starting from 2020.Winter.1 release, adds phone line's lock status beside existing phone line label. This is the most compatible method, available to any IP Phone with an embedded display. See below screenshot sample:



17:50 22/10/19 1024

(Locked) Line text for 1024 ☎

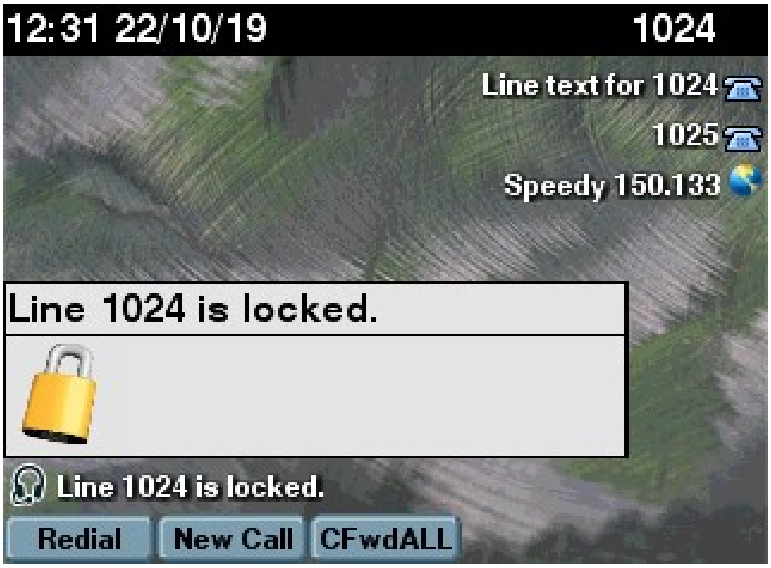
(Locked) ☎

Speedy 150.133

Your current options

Budget Lock Notification

If a user has been locked due to own Budget overrun, all phone devices associated to user's line show *"Line DN is locked"* message, where DN is the primary extension number.



Line 1024 is locked.

Line 1024 is locked.

TAPI-based locking engine

With this configuration you need to install Cisco TSP on the UC Suite Server. Through it, Phone Lock is notified about events related to the monitored IP Phones.

Main advantages of this architecture is an easy configuration on the CuCM. You only have to associate all the phones to an Application User. This method also allows to selectively lock phone devices associated to overlapping extension numbers.

ECC-based (CURRI) locking engine

Cisco Unified Communication Manager (Unified CM) 8.0(1) and later support the External Call Control (ECC) feature. This feature enables an external route server to take some call routing decisions in place of the CallManager.

Whenever a call is performed, if the called number matches an external call control enabled pattern, Cisco unified CallManager issues a routing request towards the external route server. The call routing request contains the calling party and called party information.

Imagicle UC Suite receives the request, applies business logic, and returns a call routing response that informs CUCM about call allowance.

This allows Phone Lock to route or block a call based on the lock status of the device.

Blocking Technology Comparison

The following table summarizes the differences between the blocking technologies available since Imagicle UC Suite Winter 2014:

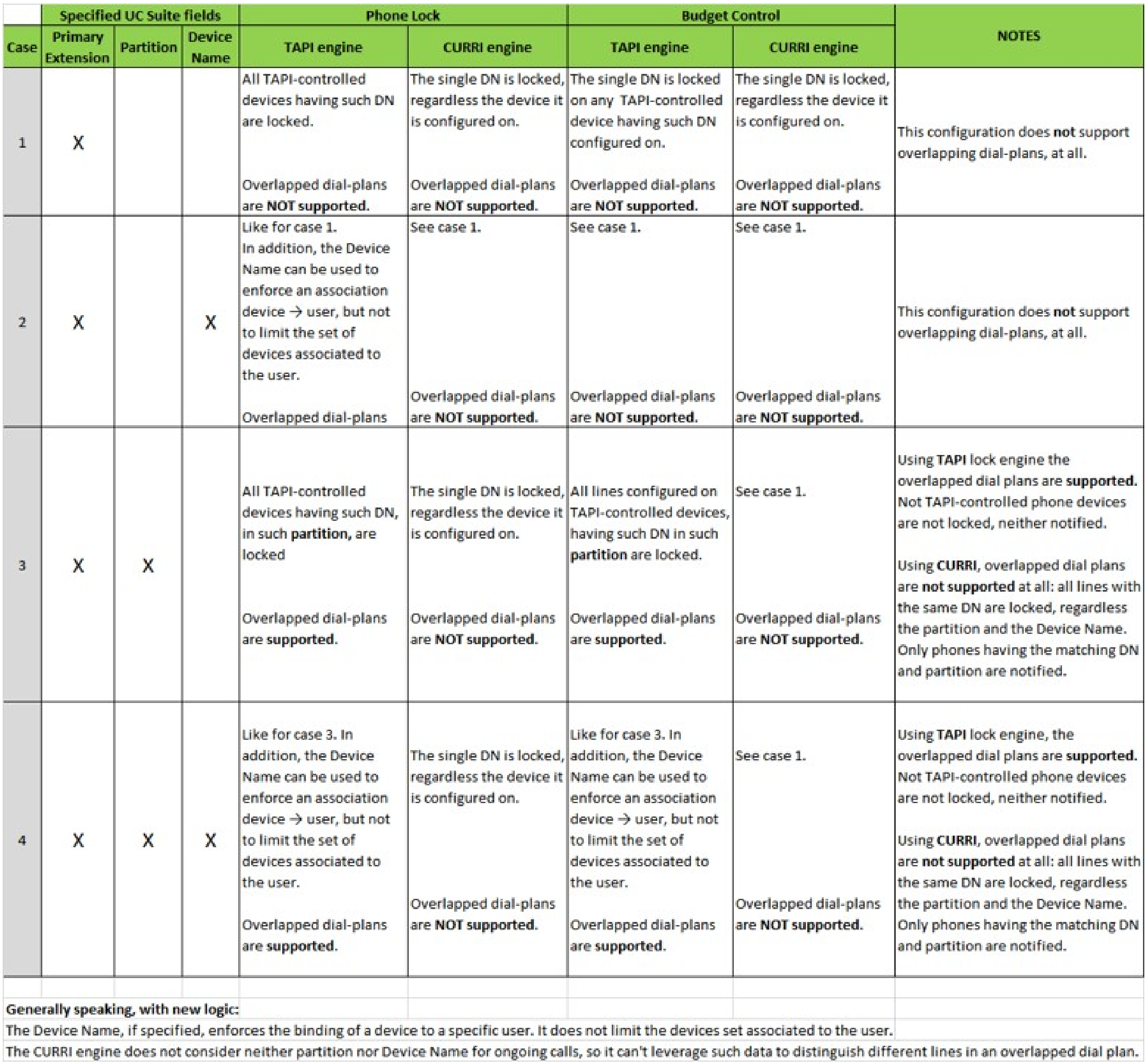
Feature	TAPI	ECC-CURRI
Requires PNP modifications	No	Yes
Requires CTI Phone Control	Yes	No
High Availability (Active - Standby)	No	Yes
Load Balancing (Active - Active)	No	Yes
Block Time (time elapsed before blocking the call)	few milliseconds	Instantaneous (calls are blocked during routing)
Support Shared Lines	Yes	No
Support overlapping numbering plans	Yes	No

- ECC-Curri is more scalable than TAPI, it has been successfully tested with more than 100 requests per second

- ECC-Curri might need Numbering Plan configuration changes
- ECC-Curri blocks call before routing, there is no ringback neither missed call notifications for the called
- ECC-Curri doesn't need any additional module to install on UC Suite
- ECC-Curri supports Load Balancing out of the box

- TAPI blocks the call after call has been already routed. The caller could hear a short ringback and the called party could get a missed call
- TAPI needs a CTI-enabled Users that monitors all the involved phones
- TAPI doesn't support Load Balancing
- TAPI needs Cisco CallManager CTI manager service running
- TAPI supports shared lines and overlapping numbering plans

Locking logics Summary table



	Specified UC Suite fields			Phone Lock		Budget Control		NOTES
Case	Primary Extension	Partition	Device Name	TAPI engine	CURRI engine	TAPI engine	CURRI engine	
1	X			All TAPI-controlled devices having such DN are locked. Overlapped dial-plans are **NOT supported**.	The single DN is locked, regardless the device it is configured on. Overlapped dial-plans are **NOT supported**.	The single DN is locked on any TAPI-controlled device having such DN configured on. Overlapped dial-plans are **NOT supported**.	The single DN is locked, regardless the device it is configured on. Overlapped dial-plans are **NOT supported**.	This configuration does **not** support overlapping dial-plans, at all.
2	X		X	Like for case 1. In addition, the Device Name can be used to enforce an association device → user, but not to limit the set of devices associated to the user. Overlapped dial-plans	See case 1. Overlapped dial-plans are **NOT supported**.	See case 1. Overlapped dial-plans are **NOT supported**.	See case 1. Overlapped dial-plans are **NOT supported**.	This configuration does **not** support overlapping dial-plans, at all.
3	X	X		All TAPI-controlled devices having such DN, in such **partition**, are locked Overlapped dial-plans are **supported**.	The single DN is locked, regardless the device it is configured on. Overlapped dial-plans are **NOT supported**.	All lines configured on TAPI-controlled devices, having such DN in such **partition** are locked. Overlapped dial-plans are **supported**.	See case 1. Overlapped dial-plans are **NOT supported**.	Using **TAPI** lock engine the overlapped dial plans are **supported**. Not TAPI-controlled phone devices are not locked, neither notified. Using **CURRI**, overlapped dial plans are **not supported** at all: all lines with the same DN are locked, regardless the partition and the Device Name. Only phones having the matching DN and partition are notified.
4	X	X	X	Like for case 3. In addition, the Device Name can be used to enforce an association device → user, but not to limit the set of devices associated to the user. Overlapped dial-plans are **supported**.	The single DN is locked, regardless the device it is configured on. Overlapped dial-plans are **NOT supported**.	Like for case 3. In addition, the Device Name can be used to enforce an association device → user, but not to limit the set of devices associated to the user. Overlapped dial-plans are **supported**.	See case 1. Overlapped dial-plans are **NOT supported**.	Using **TAPI** lock engine, the overlapped dial plans are **supported**. Not TAPI-controlled phone devices are not locked, neither notified. Using **CURRI**, overlapped dial plans are **not supported** at all: all lines with the same DN are locked, regardless the partition and the Device Name. Only phones having the matching DN and partition are notified.

Generally speaking, with new logic:
The Device Name, if specified, enforces the binding of a device to a specific user. It does not limit the devices set associated to the user.
The CURRI engine does not consider neither partition nor Device Name for ongoing calls, so it can't leverage such data to distinguish different lines in an overlapped dial plan.

Extension mobility support

Phone Lock supports extension mobility. In this case, it blocks the line entered in the First Extension Number field of the user associated to the CUCM End User.

Compatible devices

While using ECC-based locking engine, ANY phone device can be locked, including analog sets. If TAPI-based engine is chosen, it works with CTI-monitorable phone devices only. Visual notification of locking status is obviously available to IP Phones with a display only.

Configuration Task List

Warning: you must install and configure the Application Suite before being able to configure the single applications.
Please go through the AppSuite Deployment, Main Configuration, and User Management sections before reading on.

For best results, we recommend configuring Phone Lock by following below procedure in exact order:

- Install and configure Cisco TSP on Imagicle UC Suite server
- Configure UC Suite System Parameters (CuCM IP address and AXL parameters)
- Populate Users' list, leveraging synchronization against external source
- Configure Phone Lock using TAPI or CURRI (ECC) engine
- On the CuCM, subscribe Phone Lock XML service to all IP Phones
- Enable Jabber/Webex Phone Lock gadget, if required
- Configure CUCM as described in the following pages of this guide. The configuration slightly changes depending on the blocking engine in use (TAPI or CURRI)
- Verify that the users devices can be monitored, accessing the Admin â Support â Telephony Information â (Details). Registered phone devices should be detected by AXL, even if you use CURRI
- If you have a valid license, activate it now using the License page. If you do not have it yet, the application will run in evaluation mode for 30 days
- Perform a Phone Lock service restart through the web interface

XML Service Configuration

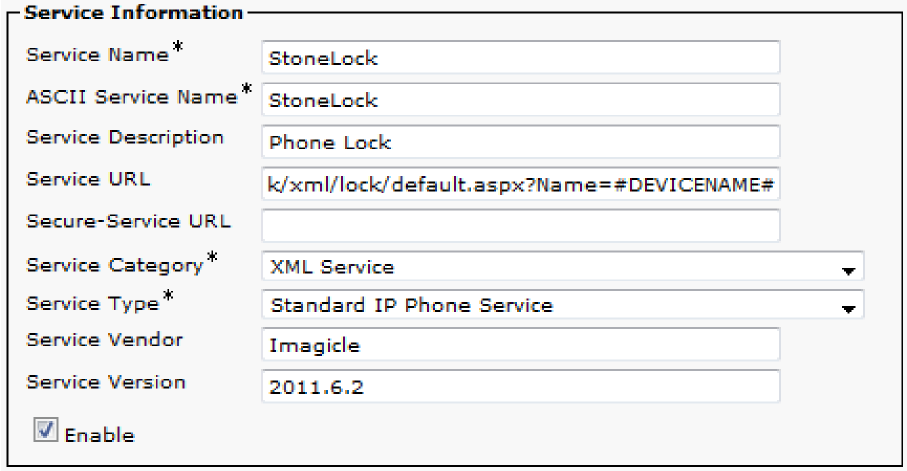
XML Service Subscription For CuCM 6.x and later

Log onto the CuCM web interface. Click on Device -> Device Settings -> Phone Services.

Define a new Phone Service with following parameters:

- Name: StoneLock service
- Description: StoneLock service
- Service Category: XML Service
- Service Type: Standard IP Phone Service
- Service URL: http://<IAS_ip_address>/fw/apps/StoneLock/xml/Lock/Default.aspx?name=#DEVICENAME#
- Flag "Enable": set

TIP: You can automatically get the right URL to be pasted, with the right IP address, directly form the Application Suite web interface. Just open the Phone Lock -> Global setting page.

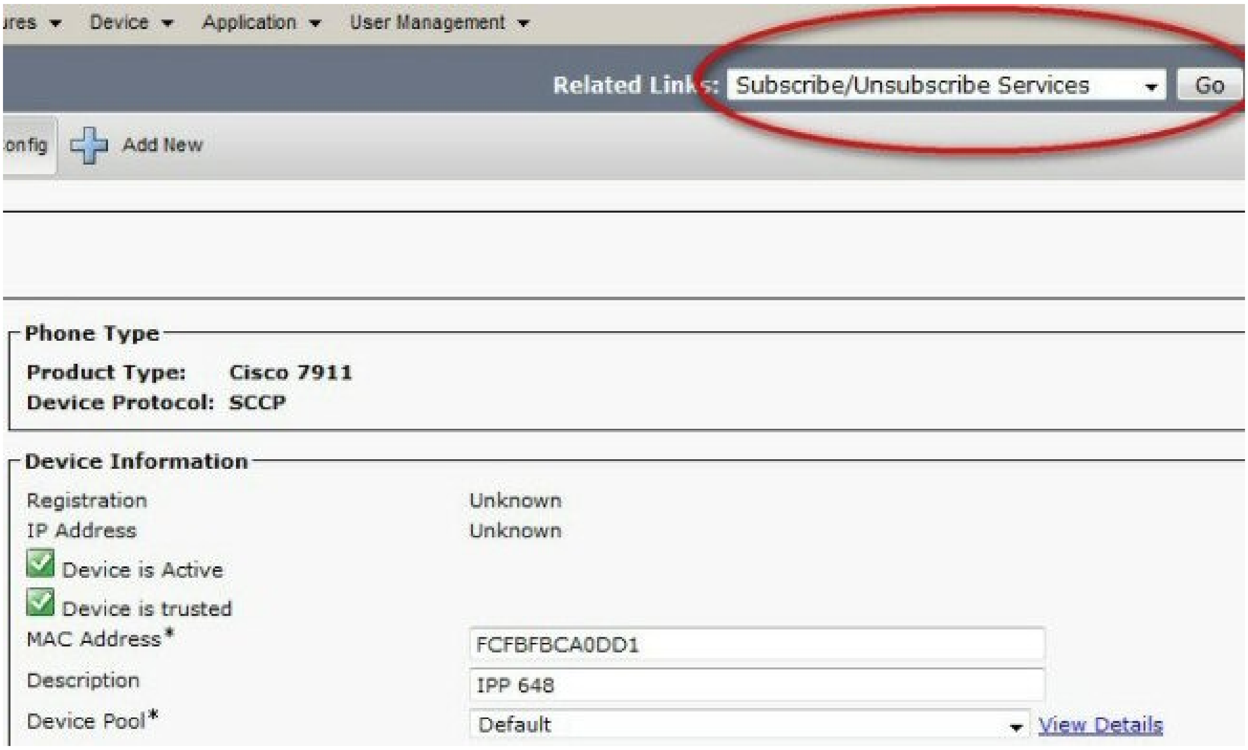


Service Information

Service Name*	StoneLock
ASCII Service Name*	StoneLock
Service Description	Phone Lock
Service URL	k/xml/lock/default.aspx?Name=#DEVICENAME#
Secure-Service URL	
Service Category*	XML Service
Service Type*	Standard IP Phone Service
Service Vendor	Imagicle
Service Version	2011.6.2

☑ Enable

Then subscribe each phones that need to use the Stonelock service you just created. Click Device -> Phone, select the phone you want to activate StoneLock for).



ıres ▾ Device ▾ Application ▾ User Management ▾

Related Links: Subscribe/Unsubscribe Services ▾ Go

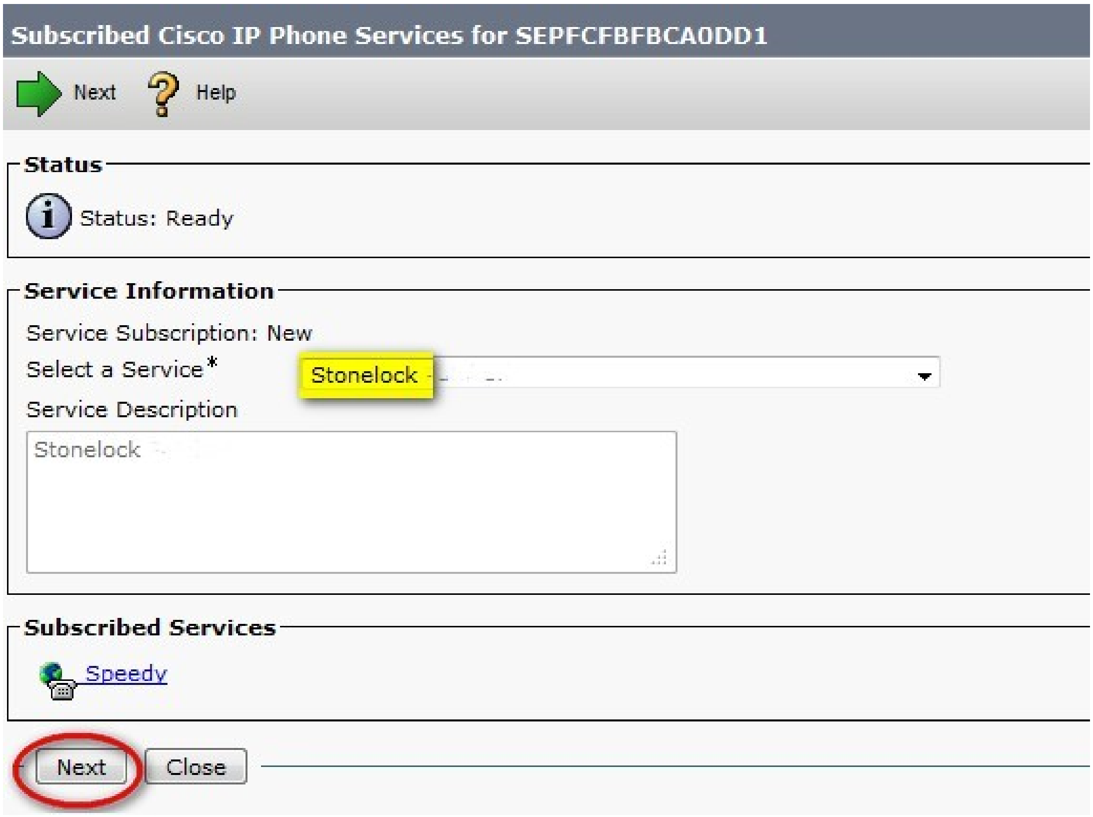
onfig Add New

Phone Type

Product Type: Cisco 7911
Device Protocol: SCCP

Device Information

Registration	Unknown
IP Address	Unknown
☑ Device is Active	
☑ Device is trusted	
MAC Address*	FCFBFBCA0DD1
Description	IPP 648
Device Pool*	Default ▾ View Details



Subscribed Cisco IP Phone Services for SEPFCFBFBCA0DD1

Status

Status: Ready

Service Information

Service Subscription: New

Select a Service* Stonelock [redacted] ▾

Service Description

Stonelock [redacted]

Subscribed Services

Speedy

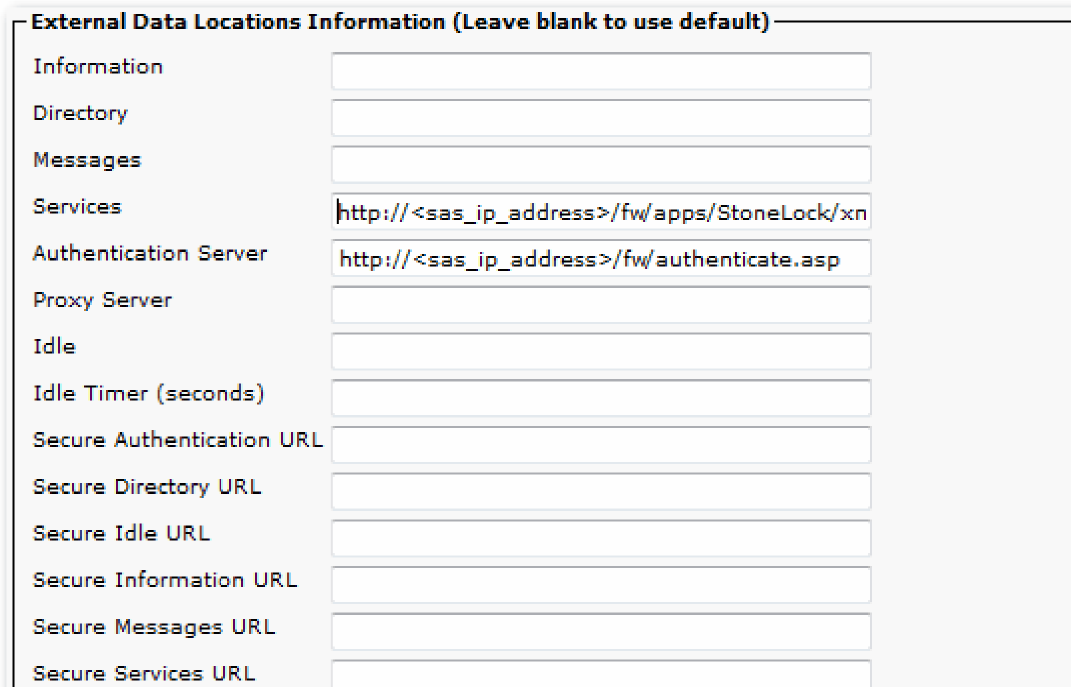
Continue the configuration

PBX configuration is not done! You must also configure TAPI and, optionally, CURRI. Please read ahead.

XML Service Subscription For CCM 4.x

Log onto the CuCM web interface. Click on Device -> Device -> Phone. Select the phone you want to edit. Add a direct link to the StoneLock service in the phone configuration parameters:

- Authentication: http://<IAS_ip_address>/fw/authenticate.asp
- Services URL: http://<IAS_ip_address>/fw/apps/StoneLock/xml/Lock/Default.aspx?name=#DEVICENAME#



External Data Locations Information (Leave blank to use default)

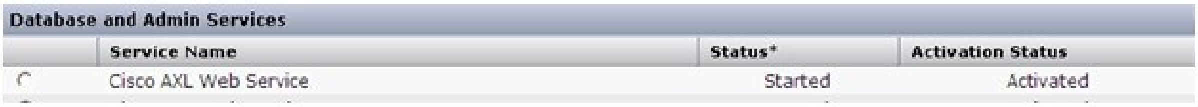
Information	
Directory	
Messages	
Services	http://<sas_ip_address>/fw/apps/StoneLock/xn
Authentication Server	http://<sas_ip_address>/fw/authenticate.asp
Proxy Server	
Idle	
Idle Timer (seconds)	
Secure Authentication URL	
Secure Directory URL	
Secure Idle URL	
Secure Information URL	
Secure Messages URL	
Secure Services URL	

TIP: You can automatically get the right URL to be pasted, with the right IP address, directly form the Application Suite web interface. Just open the Phone Lock -> Global setting page.

Troubleshooting tips

1. If a device IP does not appear in Admin -> Support -> (details) page, it cannot display the phone status. Double check device association and configuration. The device must be both "detected by AXL" and "detected by TAPI".

2. Check that the AXL Service is active on the CuCM. In case of CuCM cluster installations, check that the IP address you entered in the IAS telephony services mask is the one of the node on which the AXL service is activated.



Database and Admin Services

	Service Name	Status*	Activation Status
○	Cisco AXL Web Service	Started	Activated

3. Check that Imagicle AXL Client Service is active since it retrieves the phone IP addresses. Let it run for some minutes before testing StoneLock.

4. Also check that the following services are running: Imagicle Phone Control, Imagicle Service Host, Imagicle Licensing.

Configuration for TAPI

Additional Cisco Unified CallManager configuration when using TAPI

Device Association

For a telephone to be locked, it must be monitored through TAPI. Associate all the devices you want to use with StoneLock to the ImagicleCTI user you created during TSP setup.

Note: device association may required by other Imagicle applications leveraging the TAPI technology, such as Speedy, Queue Manage Enterprise, Blues Attendant. We advise to complete this configuration steps even if you choose the CURRI blocking technology.

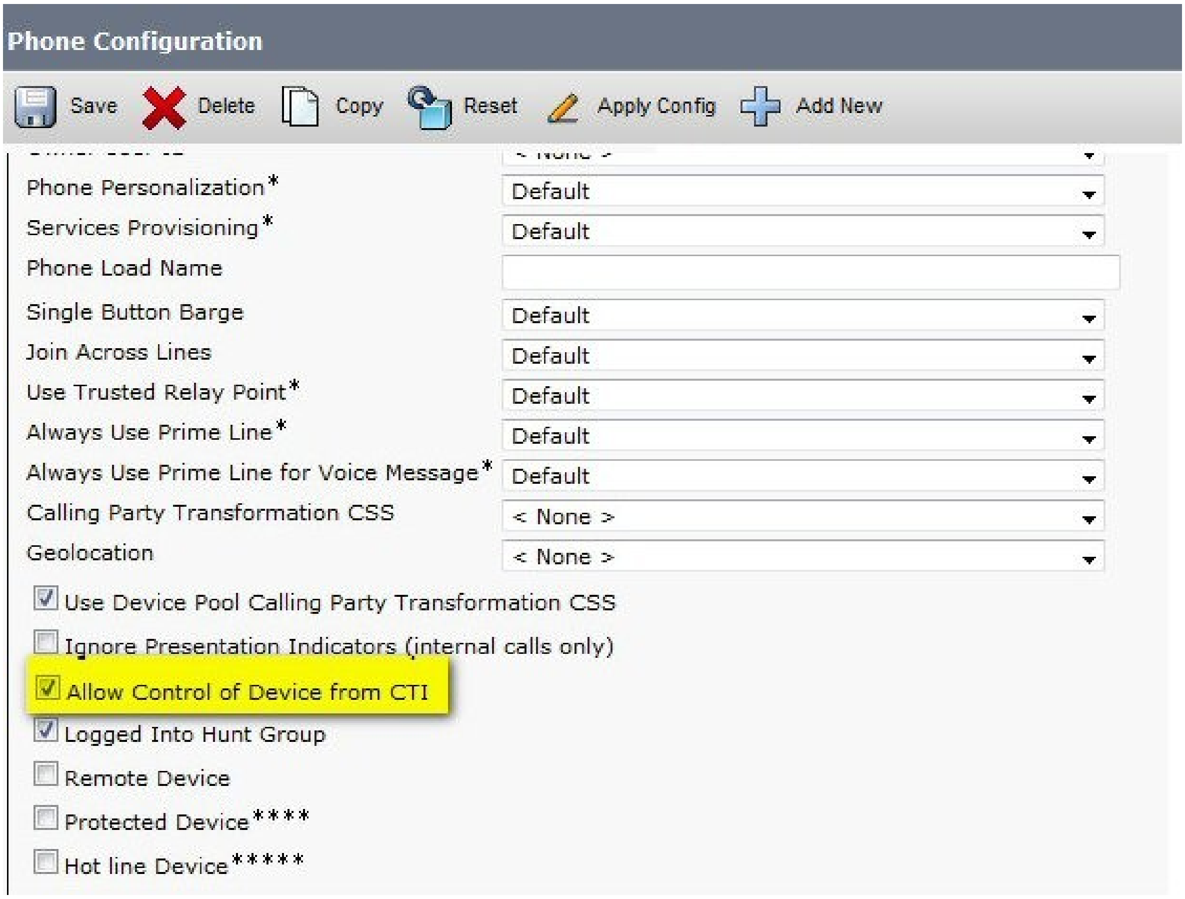
Lock overlapping phone lines

Starting from Imagicle 2020.Spring.1 release, StoneLock TAPI engine can selectively lock overlapping extensions, if associated to different partitions and different phone devices. To enable this feature please populate relevant "Partition" field in Imagicle Users' list.

Troubleshooting tips

1. If an IP Phone does not appear in Admin -> Support -> (details) page, it cannot be monitored by Stonelock. It must have both the "Detected by AXL" and "Detected By TAPI" flags. If not, please double check device association on the CallManager, and AXL configuration on the IAS server.

2. Check that the option "Allow Control of Device from CTI" is enabled in the phone configuration (Device --> Phone)



Phone Personalization*	Default
Services Provisioning*	Default
Phone Load Name	
Single Button Barge	Default
Join Across Lines	Default
Use Trusted Relay Point*	Default
Always Use Prime Line*	Default
Always Use Prime Line for Voice Message*	Default
Calling Party Transformation CSS	< None >
Geolocation	< None >

☑ Use Device Pool Calling Party Transformation CSS

□ Ignore Presentation Indicators (internal calls only)

☑ Allow Control of Device from CTI

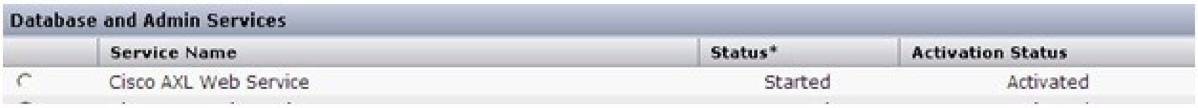
☑ Logged Into Hunt Group

□ Remote Device

□ Protected Device****

□ Hot line Device*****

3. Check that the AXL Service is active. In case of CuCM cluster installations, check that the IP address you entered in the IAS telephony services mask is the one of the node on which the AXL service is activated.



Database and Admin Services

	Service Name	Status*	Activation Status
○	Cisco AXL Web Service	Started	Activated

Configuration For Curri - ECC

Additional configuration when using ECC-CURRI

System Requirements for External Call Control - CURRI

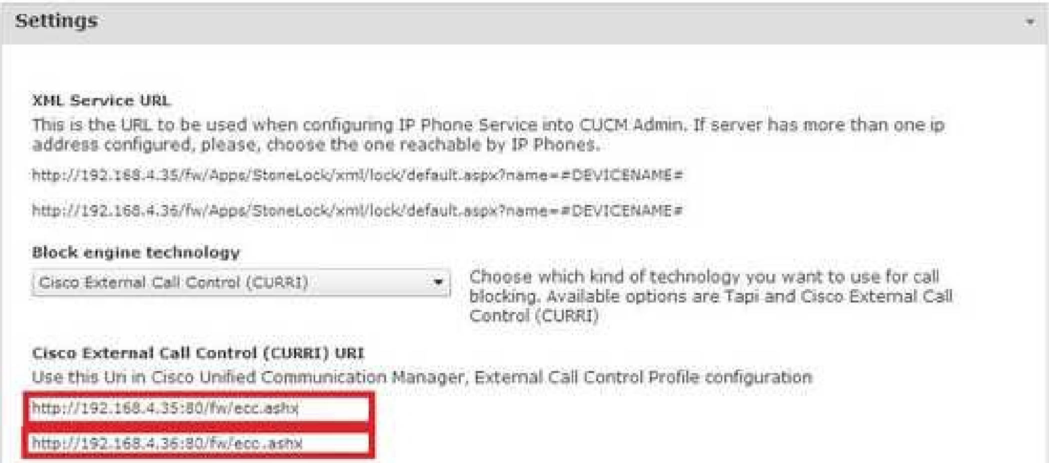
- Cisco Unified Communications Manager 8.0(2) or higher
- Imagicle Application Suite Winter 2014 edition or later

Imagicle Application Suite Configuration

Go to the Imagicle Application Suite Web configuration portal, **Phone Lock** -> **Global Settings**

Choose Cisco External Call Control (also known as CURRI) as Block engine technology. You will need the **Cisco External Call Control URI** generated from web page for configuring External Call Control Profile URI later, in Cisco CallManager configuration. The URI will be similar to:

```
http://<Imagicle_server_IP_address>:80/fw/ecc.ashx
```



Settings

XML Service URL

This is the URL to be used when configuring IP Phone Service into CUCM Admin. If server has more than one ip address configured, please, choose the one reachable by IP Phones.

http://192.168.4.35/fw/Apps/StoneLock/xml/lock/default.aspx?name=#DEVICENAME#

http://192.168.4.36/fw/Apps/StoneLock/xml/lock/default.aspx?name=#DEVICENAME#

Block engine technology

Cisco External Call Control (CURRI)

Choose which kind of technology you want to use for call blocking. Available options are Tapi and Cisco External Call Control (CURRI)

Cisco External Call Control (CURRI) URI

Use this Uri in Cisco Unified Communication Manager, External Call Control Profile configuration

http://192.168.4.35:80/fw/ecc.ashx

http://192.168.4.36:80/fw/ecc.ashx

Note: you must enter the URI generated form this page. If you enter a different URI (e.g. without the specified port) the configuration won't work**.**

Note: Phone Lock ECC-CURRI method does not allow to lock overlapping phone lines, even on different partitions. This feature is available starting from Imagicle 2020.Spring.1 release, only when using TAPI method.

Cisco CallManager ECC Configuration

Warning: Due to a Cisco CallManager known issue, every modification on a External Call Control Profile requires a Cisco CallManager service restart. This can drop all the calls in progress.

External Call Control Profile

The External Call Control Profile (ECCP) is how Imagicle Application Suite is linked with Unified CM. Configuring an ECCP adds your application's URL to the Unified CM database. The ECCP can then be added to *Trigger Points* in Unified CM. Available Trigger Points are:

- Translation Pattern (CM 8.0 (2) or higer)
- Route Pattern (CM 10.0 or higer)
- Directory Number (CM 10.0 or higer)

When one of this Trigger Points is involved in routing process (e.g. a phone makes an outgoing call and tries to pass through a Translattion Pattern) Unified CM sends a request to the ECCP configured link (Imagicle Application Suite) that elaborates the request and answers making a routing decision. The possibile decisions are:

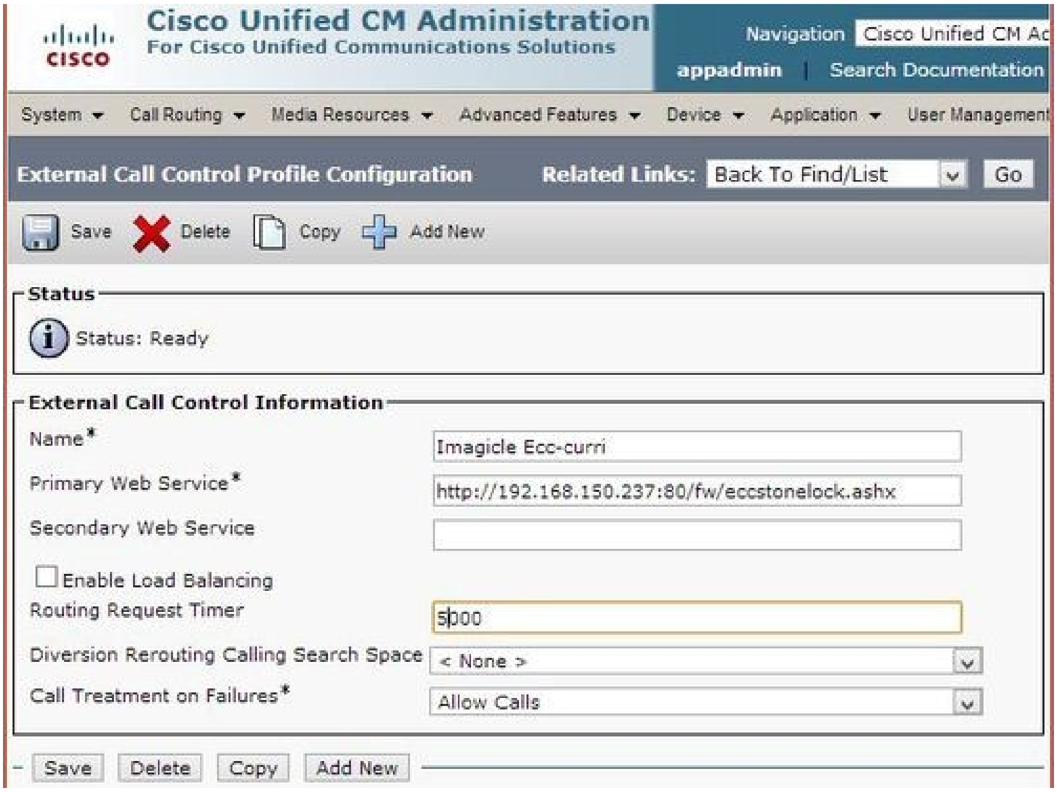
- Continue: the call will be routed applying the involved triggering point
- Deny (i.e. block with optional message): the involved triggering point is not applied and unified CM stops call routing
- Divert call

Warning: The Directory Number ECC profile is triggered only for incoming calls (i.e. calls that ring on that DN). Besides, calls routed to the DN by an Hunt pilot do not trigger the ECC profile call.

Configuration in UCM

In Cisco Unified CM Administration, specify the following information in the Call Routing -> "External Call Control Profile Configuration" window:

- **Name** of the External Call Control Profile (ECCP)
- **Primary Web Service:** URI of the Imagicle Application Suite (the one generated during Application Suite configuration in Global Settings page)
  - permits configuration of two URIs, for redundancy (active & standby) and for load balancing (where Imagicle High Availability options is available)
  - supports HTTP
- **Timeout** value for call routing response (suggeste value is 5000 ms)
- **Diversion rerouting calling search space**: this CSS is applied in case of diversion to a number for a blocked call
- **Call treatment on failures**: choose the treatment if Imagicle Application Suite is unresponsive o response timeout has been reached (Allow Calls is suggested)


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Ac
appadmin | Search Documentation
System Call Routing Media Resources Advanced Features Device Application User Management
Related Links: Back To Find/List Go
Save Delete Copy Add New

External Call Control Profile Configuration

Status

Status: Ready

External Call Control Information

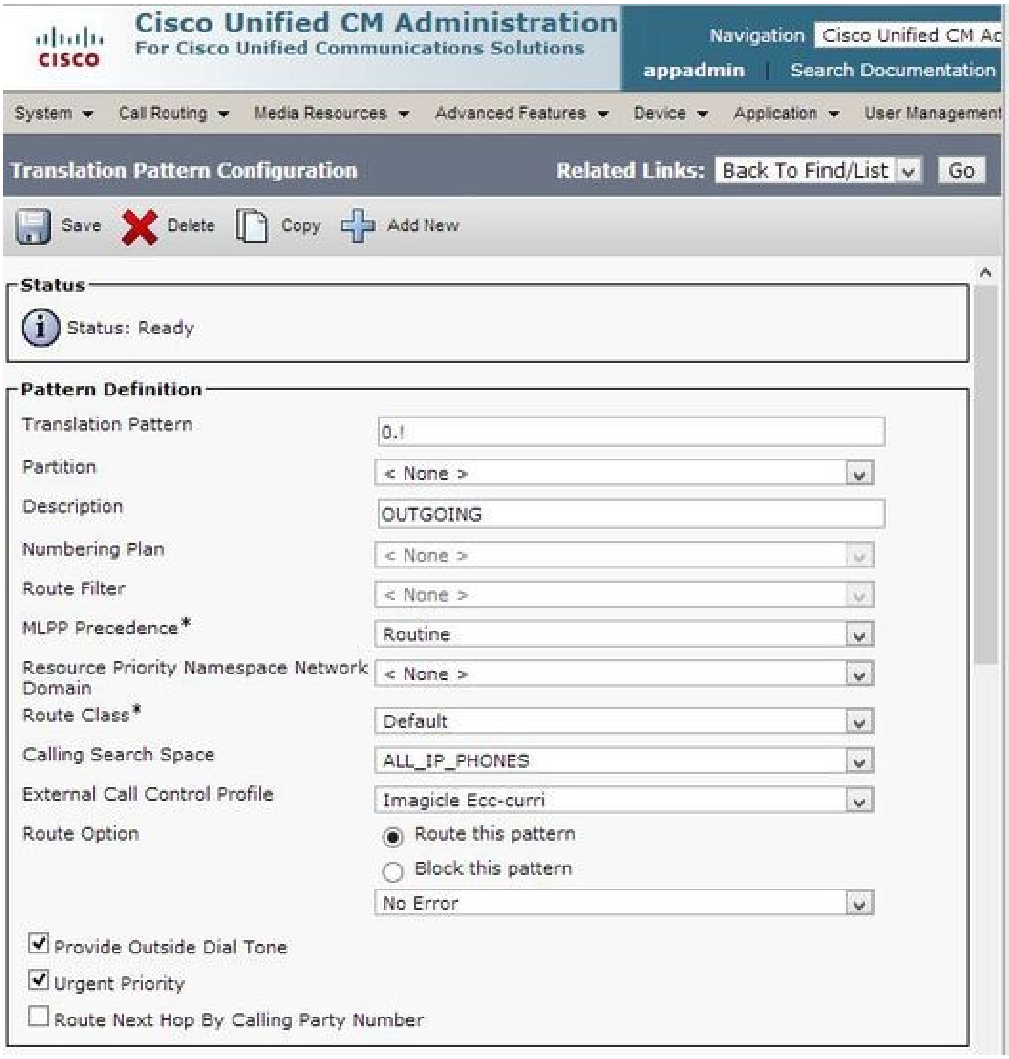
Name*	Imagicle Ecc-curri
Primary Web Service*	http://192.168.150.237:80/fw/eccstonelock.ashx
Secondary Web Service	
□ Enable Load Balancing	
Routing Request Timer	5000
Diversion Rerouting Calling Search Space	< None >
Call Treatment on Failures*	Allow Calls

Trigger Points

A Trigger Point is the point in Unified CM's routing logic at which Unified CM issues a Route Request.

- *Translation Pattern* trigger points are available in Unified CM 8.0(1) and later
- *Route Patterns* and *Directory Numbers* are trigger points in Unified CM 10.0 and later

Enable ECCP in Translation Pattern Trigger point


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Ac
appadmin | Search Documentation
System Call Routing Media Resources Advanced Features Device Application User Management
Related Links: Back To Find/List Go
Save Delete Copy Add New

Translation Pattern Configuration

Status

Status: Ready

Pattern Definition

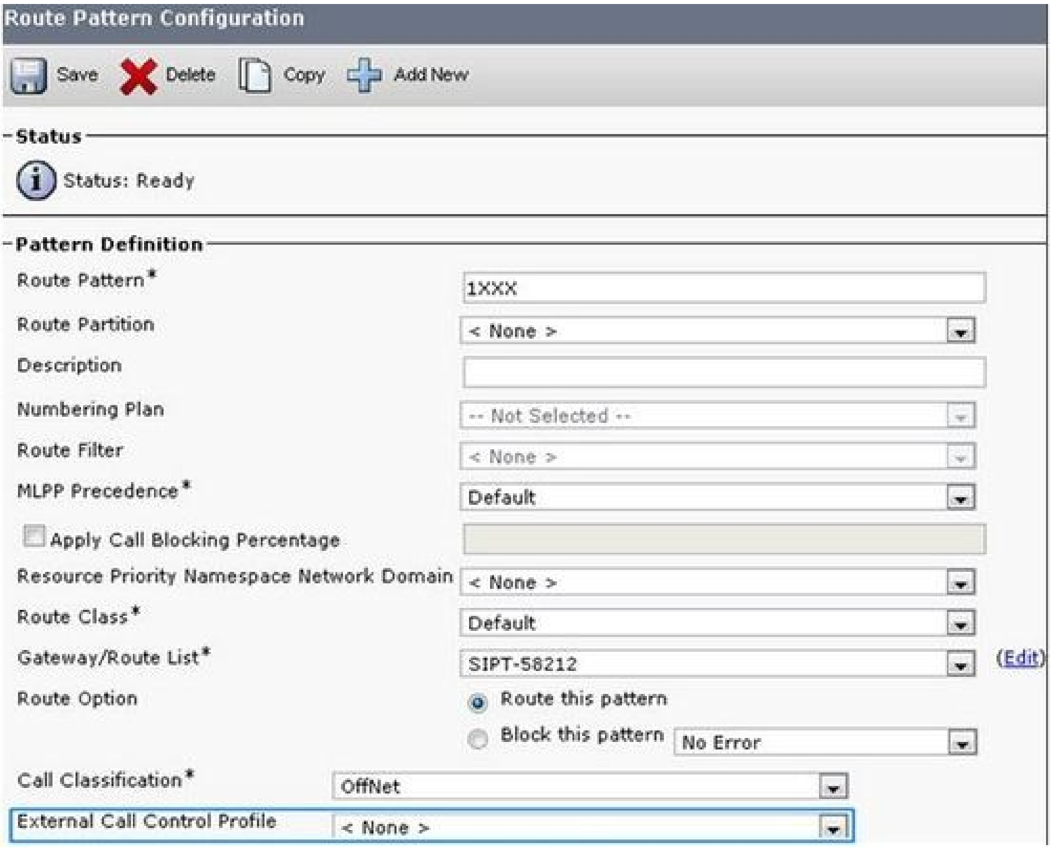
Translation Pattern	0.!
Partition	< None >
Description	OUTGOING
Numbering Plan	< None >
Route Filter	< None >
MLPP Precedence*	Routine
Resource Priority Namespace Network Domain	< None >
Route Class*	Default
Calling Search Space	ALL_IP_PHONES
External Call Control Profile	Imagicle Ecc-curri
Route Option	● Route this pattern ○ Block this pattern No Error

☑ Provide Outside Dial Tone

☑ Urgent Priority

□ Route Next Hop By Calling Party Number

Enable ECCP in Route Pattern Trigger Point (In Unified CM 10.0 and later)



Route Pattern Configuration

Status

Status: Ready

Pattern Definition

Route Pattern* 1XXX

Route Partition < None >

Description

Numbering Plan -- Not Selected --

Route Filter < None >

MLPP Precedence* Default

□ Apply Call Blocking Percentage

Resource Priority Namespace Network Domain < None >

Route Class* Default

Gateway/Route List* SIPT-58212 (Edit)

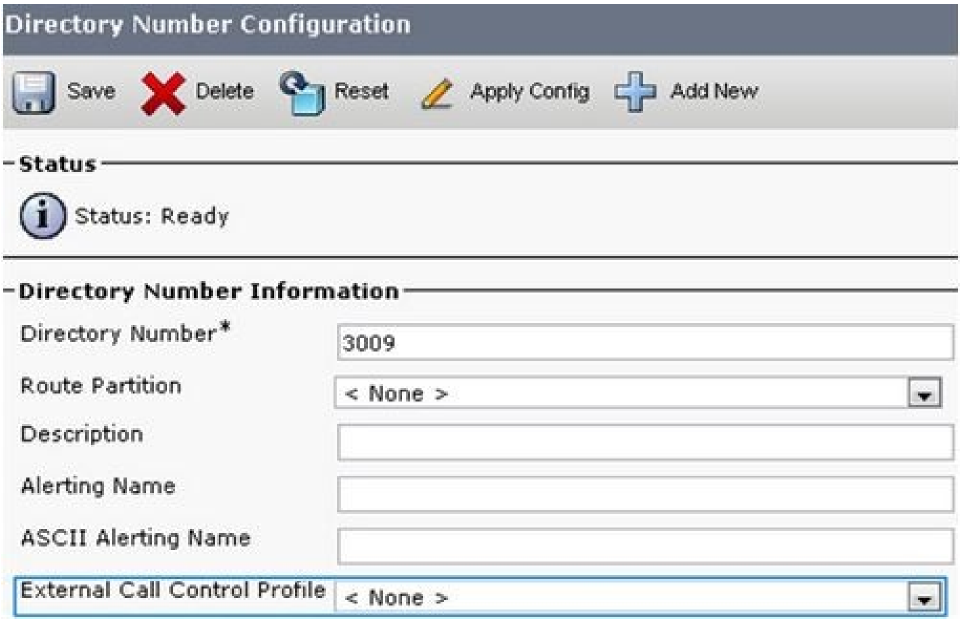
Route Option ● Route this pattern

○ Block this pattern No Error

Call Classification* OffNet

External Call Control Profile < None >

Enable ECCP in Directory Number Trigger Point (In Unified CM 10.0 and later)



Directory Number Configuration

Status

Status: Ready

Directory Number Information

Directory Number* 3009

Route Partition < None >

Description

Alerting Name

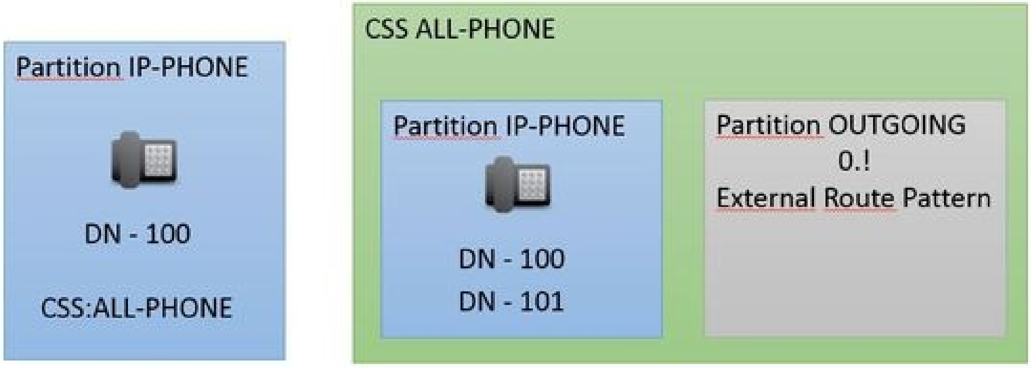
ASCII Alerting Name

External Call Control Profile < None >

CM Configuration Guidelines

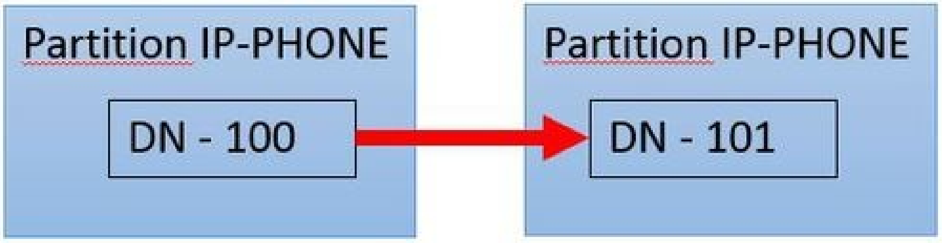
The most used trigger point is Translation Pattern (the only one available until Cisco CallManager version 10.0).

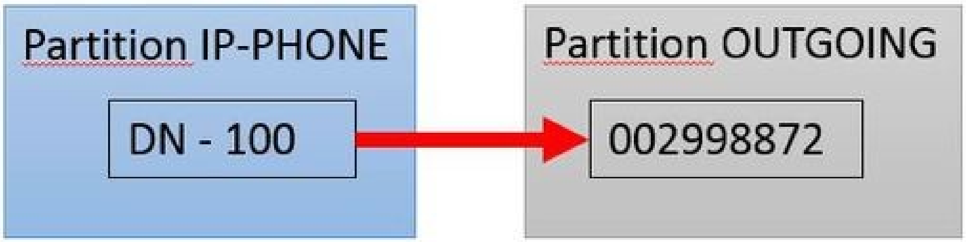
if you want the External Call Control (also known as CURRI) web service to be used in call routing you must be sure to involve the translation pattern in call flow. Following schemas represent a simple standard configuration in a Cisco CallManager environment:



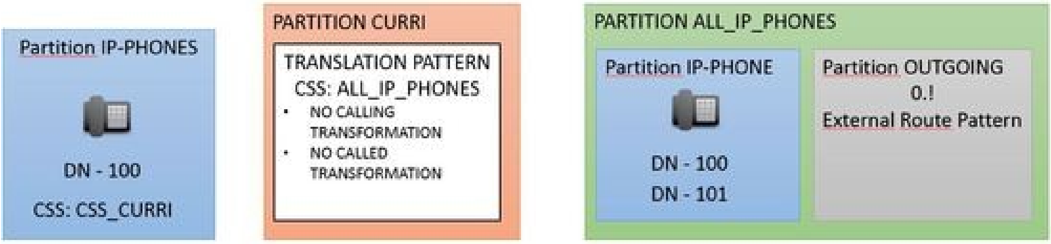
In this example, we have a phone with a Directory Number contained in IP-PHONE partition and with ALL-PHONE Calling Search Space. ALL-PHONE includes IP-PHONE and OUTGOING partitions. In this simple case any Directory Number in partition IP-PHONE could call any phone in IP-PHONE partition or any External number starting with 0.

Call Flow examples:





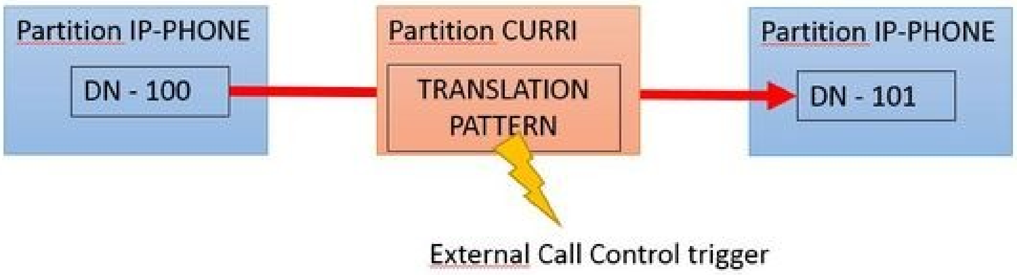
Introducing translation pattern for triggering External Call Control schema should change:

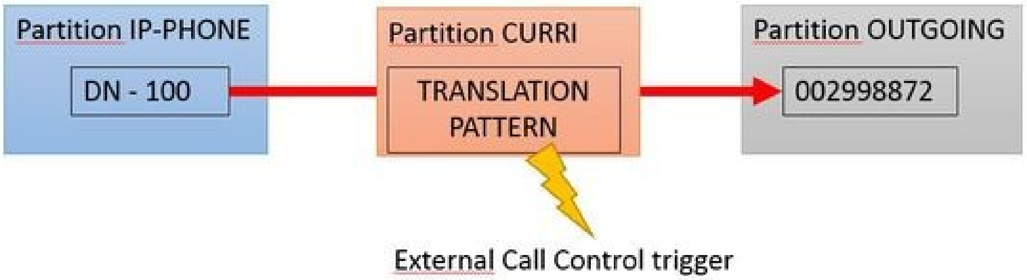


The changes are:

- Create the translation pattern with External Call Control Profile and Calling Search Space ALL-PHONE
- Create a new partition, CURRI, that includes the just created translation pattern
- Create a new Calling search Space, CSS_CURRI, that includes CURRI partition, but no IP-PHONE partition
- Change the Directory Number Calling Search Space to CSS_CURRI

The call flows become:

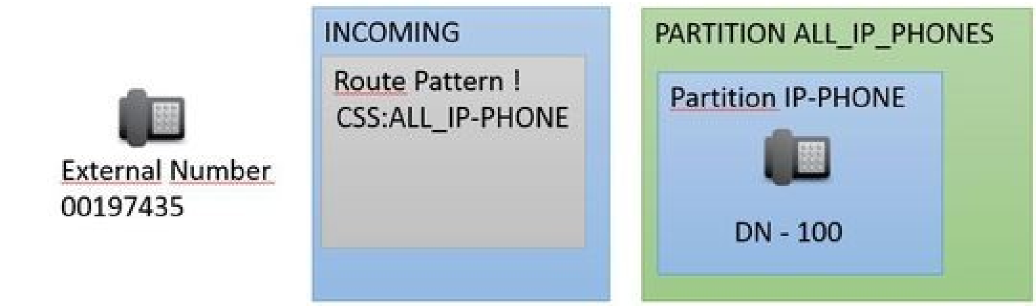




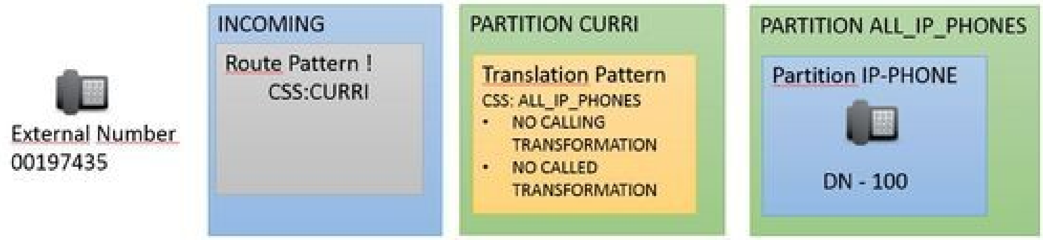
Note: be careful with CSS and Partition configuration, a wrong configuration could lead to call loops that can give telephony inefficiency or deteriorate your PBX and Imagicle Application Suite performances

Blocking incoming calls with ECC - CURRI

To block the incoming calls, the guidelines are similar. Starting with a simple standard configuration, with an incoming route pattern that routes the calls to internal phones as shown below:



If there are Translation Patterns in the flow (E.g. for translation from E164 to internal number) the solutions is easy, just add an External Call Control Profile to the involved translations in order to have a ready to use system.



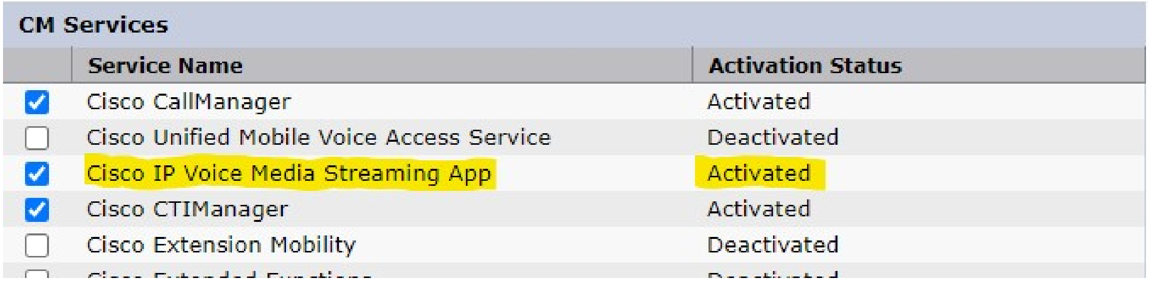
In case no Translation Patterns are involved, it is necessary to insert a new level in Numbering Plan as we did for outgoing calls. You need to:

- Create the translation pattern with External Call Control Profile and Calling Search Space ALL_IP_PHONES
- Create a new partition, CURRI, that includes the just created translation pattern
- Create a new Calling search Space, CSS_CURRI, that includes CURRI partition, but no IP-PHONE partition
- Change the incoming Route Pattern Calling Search Space to CSS_CURRI

Play a message when a call is blocked

In order to play a message to the caller when a call is blocked, you must first enable "IP Voice Media Streaming" service:

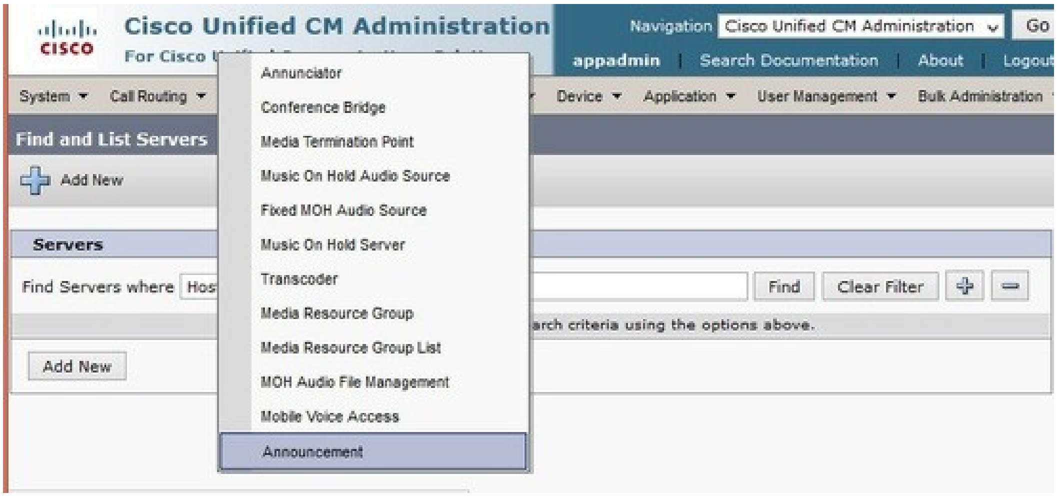
- Access to CUCM "Cisco Unified Serviceability" web portal and select Tools â Service Activation
- Make sure that "Cisco IP Voice Media Streaming App" is **Activated**



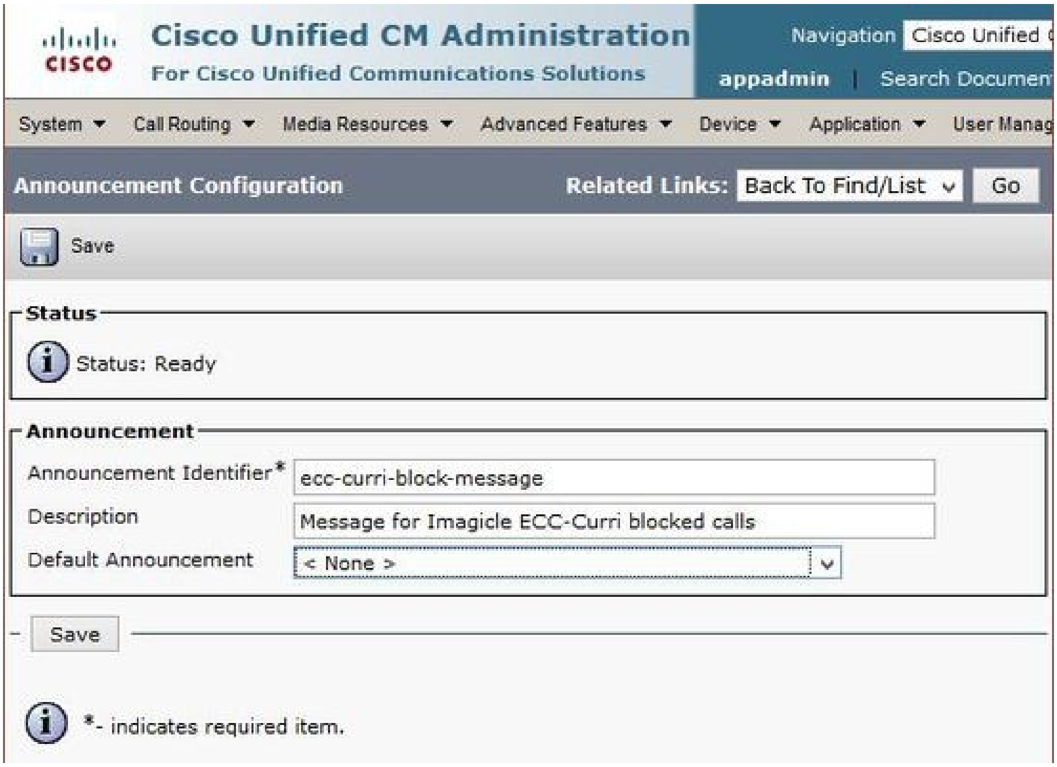
CM Services

	Service Name	Activation Status
☑	Cisco CallManager	Activated
□	Cisco Unified Mobile Voice Access Service	Deactivated
☑	Cisco IP Voice Media Streaming App	Activated
☑	Cisco CTIManager	Activated
□	Cisco Extension Mobility	Deactivated
□	Cisco Extended Functions	Deactivated

Then you should upload a file from Cisco CallManager Administration web portal, in the **Media Resources â Announcement** web page:



Add a new Announcement, filling the required fields as shown below:


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified
appadmin | Search Documen
System
Call Routing
Media Resources
Advanced Features
Device
Application
User Manag
Related Links: Back To Find/List
Go
Save
Save

Announcement Configuration

Status

Status: Ready

Announcement

Announcement Identifier* ecc-curri-block-message

Description Message for Imagicle ECC-Curri blocked calls

Default Announcement < None >

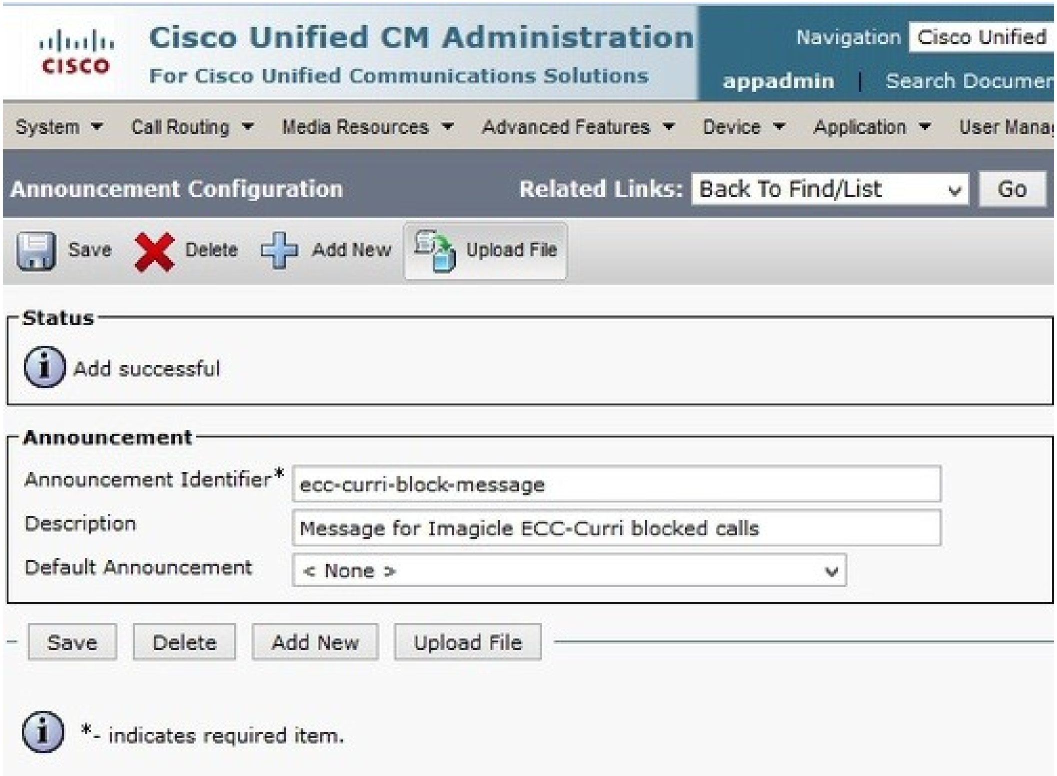
*- indicates required item.

After the Announcement creation, you have to upload a sound file.

Note: Announcements are specific to the locale (language). If your installation is using more than one language locale, each custom announcement must be recorded in each language as a separate **.wav** file and uploaded with the correct locale assignment. This also requires that the correct locale package be installed on each server before uploading custom announcement wav files for languages other than United States English.

The recommended format for announcements includes the following specifications:

- 16-bit PCM wav file
- Stereo or mono
- Sample rates: 48 Khz, 44.1 Khz, 32 Khz, 16 Khz or 8 Khz


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified
appadmin | Search Documen
System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Mana
Related Links: Back To Find/List Go
Save Delete Add New Upload File

Announcement Configuration

Status

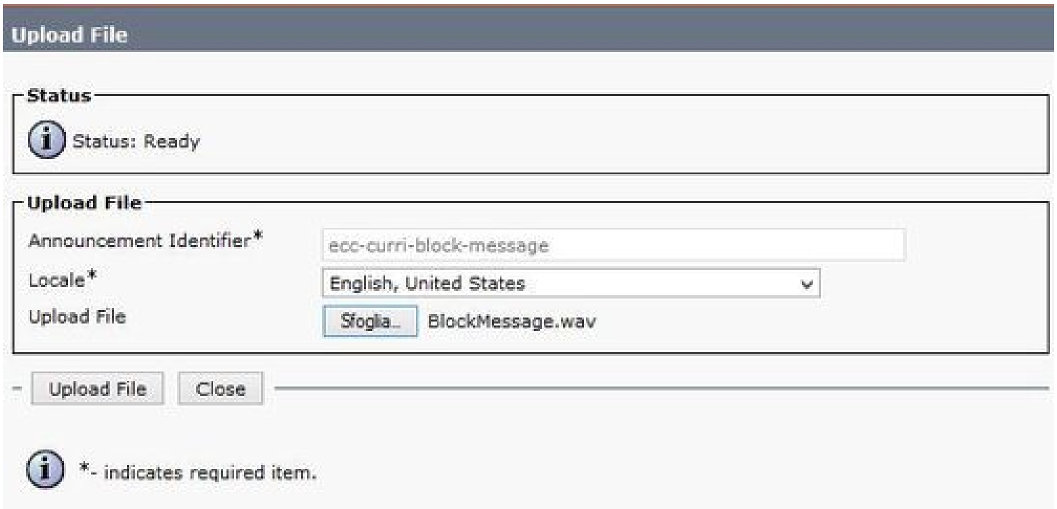
Add successful

Announcement

Announcement Identifier*	ecc-curri-block-message
Description	Message for Imagicle ECC-Curri blocked calls
Default Announcement	< None >

*- indicates required item.

You can upload one different file for each Local installed in your Cisco CallManager



Upload File

Status

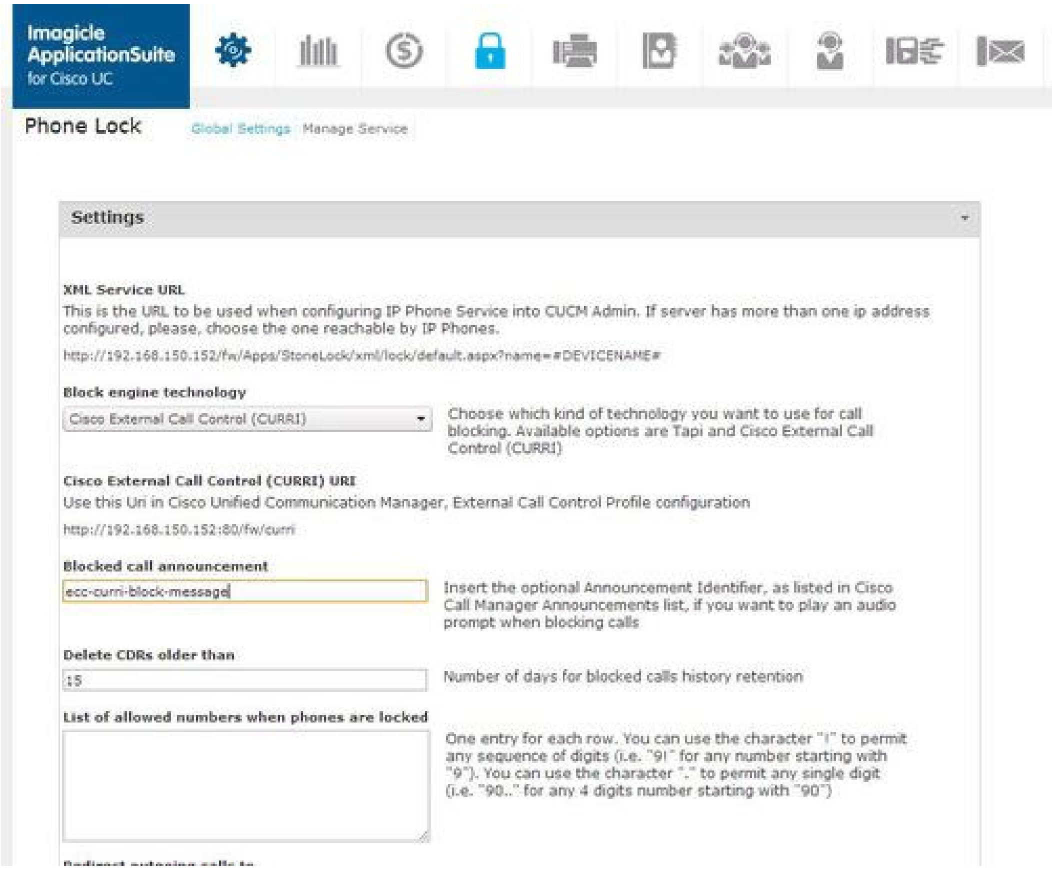
Status: Ready

Upload File

Announcement Identifier*	ecc-curri-block-message
Locale*	English, United States
Upload File	Sfoglia... BlockMessage.wav

*- indicates required item.

After file upload you have to insert the Announcement identifier in the Imagicle Application Suite Web interface, PhoneLock Settings page, as you created in Cisco CallManager (in the example "ecc-curri-block-message")



Settings

XML Service URL
This is the URL to be used when configuring IP Phone Service into CUCM Admin. If server has more than one ip address configured, please, choose the one reachable by IP Phones.
http://192.168.150.152/fw/Apps/StoneLock/xml/lock/default.aspx?name=#DEVICENAME#

Block engine technology
Cisco External Call Control (CURRI)
Choose which kind of technology you want to use for call blocking. Available options are Tapi and Cisco External Call Control (CURRI)

Cisco External Call Control (CURRI) URI
Use this Uri in Cisco Unified Communication Manager, External Call Control Profile configuration
http://192.168.150.152:80/fw/curri

Blocked call announcement
ecc-curri-block-message
Insert the optional Announcement Identifier, as listed in Cisco Call Manager Announcements list, if you want to play an audio prompt when blocking calls

Delete CDRs older than
15
Number of days for blocked calls history retention

List of allowed numbers when phones are locked
One entry for each row. You can use the character "!" to permit any sequence of digits (i.e. "9!" for any number starting with "9"). You can use the character "." to permit any single digit (i.e. "90.." for any 4 digits number starting with "90")

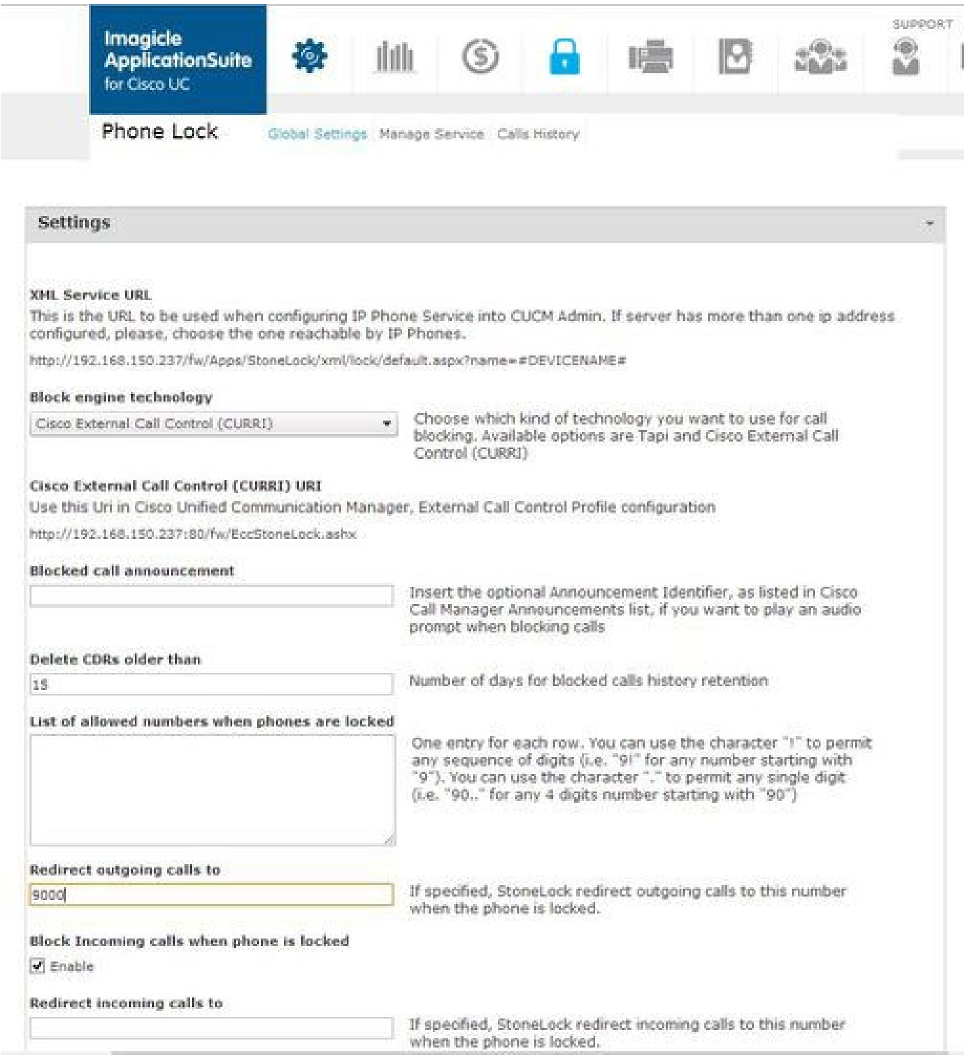
Redirect outgoing calls to

From now on every blocked, the caller will hear the uploaded message.

Warning: *Diversion* is not compatible with *Message playback*, so if you specify both a block message and a diversion number, the External Call Control (Curri) plugin will only redirect the call without playing any message.

Divert blocked calls

You can divert a blocked call to a number (E.g. voicemail), the number is system wide and you can configure it in Imagicle Application Suite Phone Lock **Global Settings** Page.



Settings

XML Service URL

This is the URL to be used when configuring IP Phone Service into CUCM Admin. If server has more than one ip address configured, please, choose the one reachable by IP Phones.

http://192.168.150.237/fw/Apps/StoneLock/xml/lock/default.aspx?name=#DEVICENAME#

Block engine technology

Cisco External Call Control (CURRI) ▾

Choose which kind of technology you want to use for call blocking. Available options are Tapi and Cisco External Call Control (CURRI)

Cisco External Call Control (CURRI) URI

Use this Uri in Cisco Unified Communication Manager, External Call Control Profile configuration

http://192.168.150.237:80/fw/EccStoneLock.ashx

Blocked call announcement

Insert the optional Announcement Identifier, as listed in Cisco Call Manager Announcements list, if you want to play an audio prompt when blocking calls

Delete CDRs older than

15

Number of days for blocked calls history retention

List of allowed numbers when phones are locked

One entry for each row. You can use the character "!" to permit any sequence of digits (i.e. "9!" for any number starting with "9"). You can use the character "." to permit any single digit (i.e. "90.." for any 4 digits number starting with "90")

Redirect outgoing calls to

9000

If specified, StoneLock redirect outgoing calls to this number when the phone is locked.

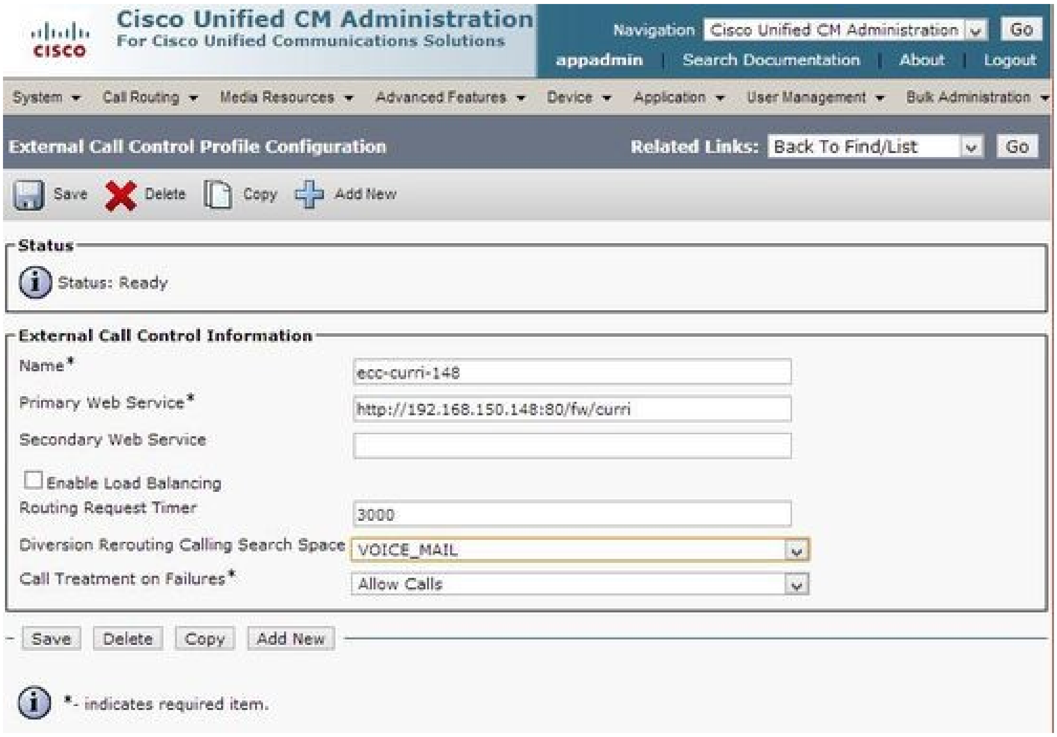
Block Incoming calls when phone is locked

☑ Enable

Redirect incoming calls to

If specified, StoneLock redirect incoming calls to this number when the phone is locked.

It is also necessary to specify a Diversion Rerouting Calling Search Space, used for call diversion of a blocked call


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
appadmin | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration
Related Links: Back To Find/List Go
Save Delete Copy Add New

External Call Control Profile Configuration

Status

Status: Ready

External Call Control Information

Name* ecc-curri-148

Primary Web Service* http://192.168.150.148:80/fw/curri

Secondary Web Service

□ Enable Load Balancing

Routing Request Timer 3000

Diversion Rerouting Calling Search Space VOICE_MAIL

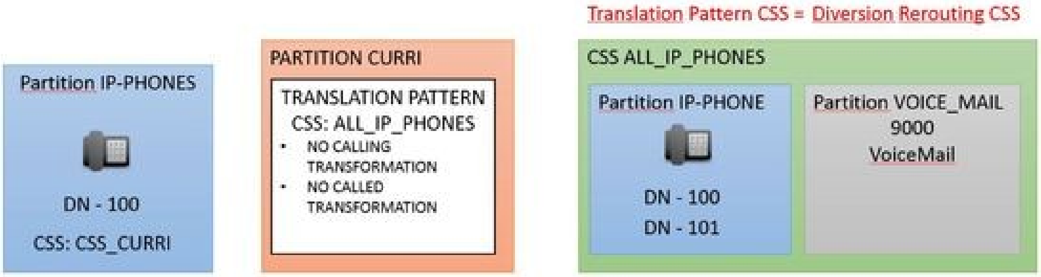
Call Treatment on Failures* Allow Calls

Save Delete Copy Add New

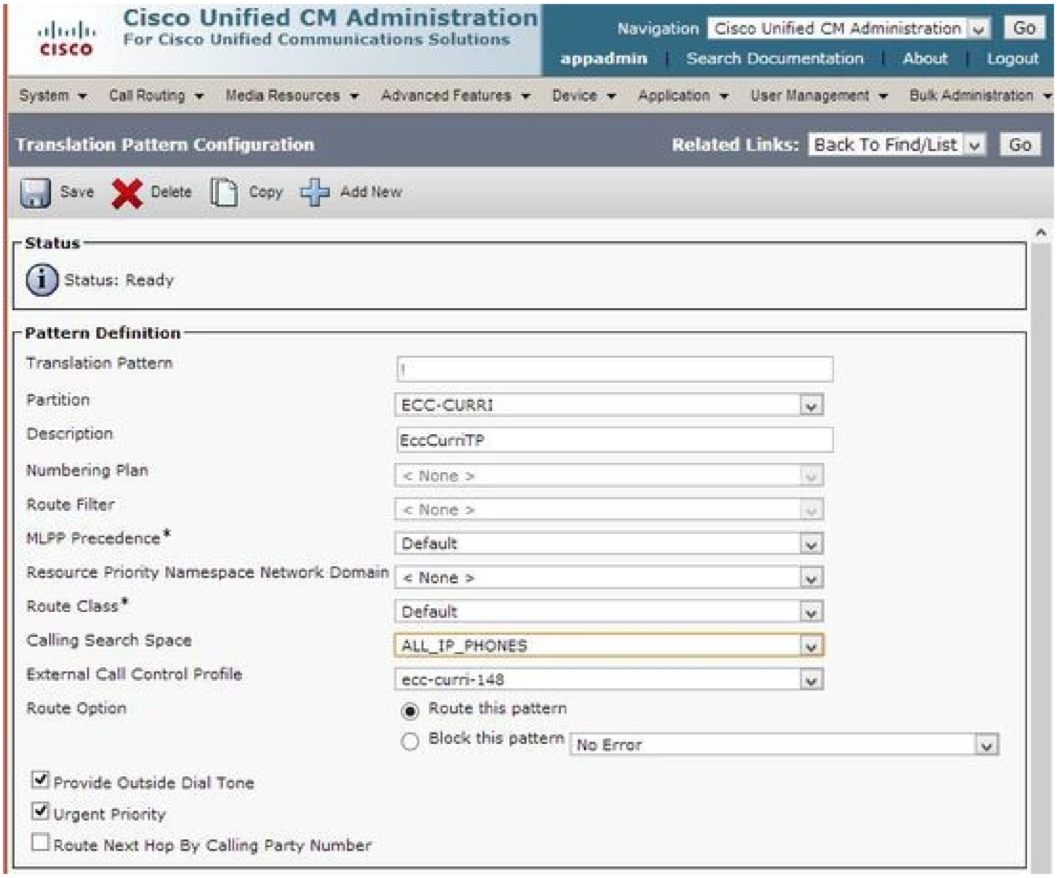
*- indicates required item.

The Diversion Calling Search Space will be used as Calling Search Space for the diverted call, so be sure that the redirection number is contained in that Calling Search Space. In the following images we modified the two standard architectures described above with a Voicemail diversion.

In first image Voicemail number belongs to the same Calling Search Space of the Translation Pattern, so there is no need to specify a new Calling Search Space, it is possible to use the phones one as Diversion rerouting Calling Search Space.



Translation Pattern and External Call Control Profile must be configured this way:


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
appadmin | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration
Related Links: Back To Find/List Go
Save Delete Copy Add New

Translation Pattern Configuration

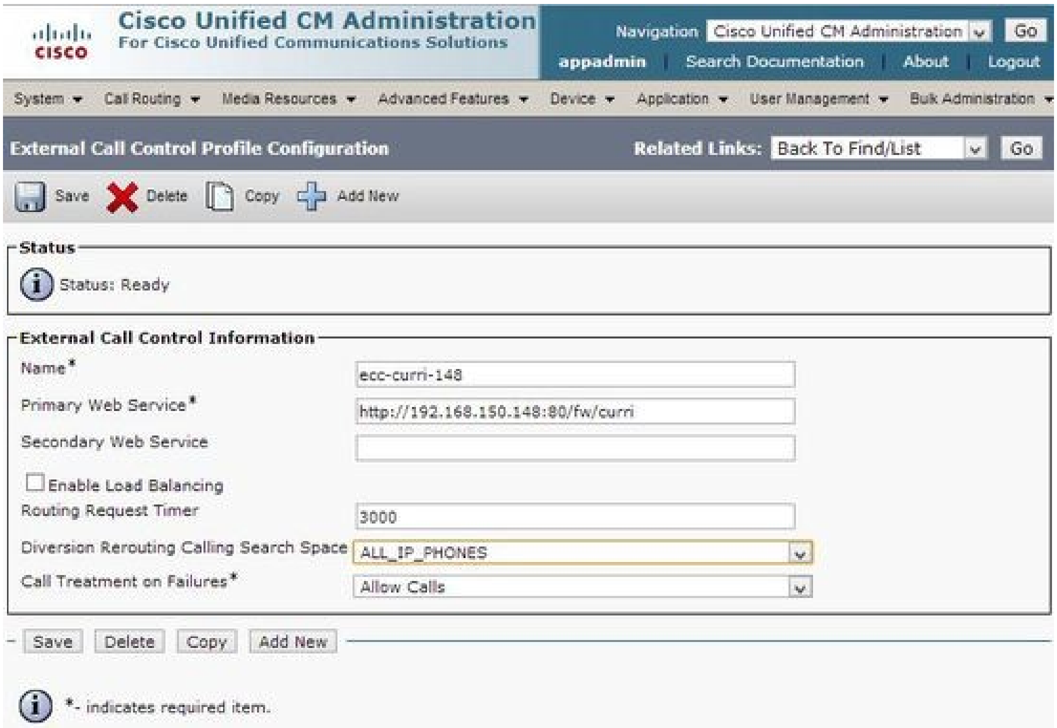
Status

Status: Ready

Pattern Definition

Translation Pattern	!
Partition	ECC-CURRI
Description	EccCurriTP
Numbering Plan	< None >
Route Filter	< None >
MLPP Precedence*	Default
Resource Priority Namespace Network Domain	< None >
Route Class*	Default
Calling Search Space	ALL_IP_PHONES
External Call Control Profile	ecc-curri-148
Route Option	● Route this pattern ○ Block this pattern No Error

☑ Provide Outside Dial Tone
☑ Urgent Priority
☐ Route Next Hop By Calling Party Number


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
appadmin | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration
Related Links: Back To Find/List Go
Save Delete Copy Add New

External Call Control Profile Configuration

Status

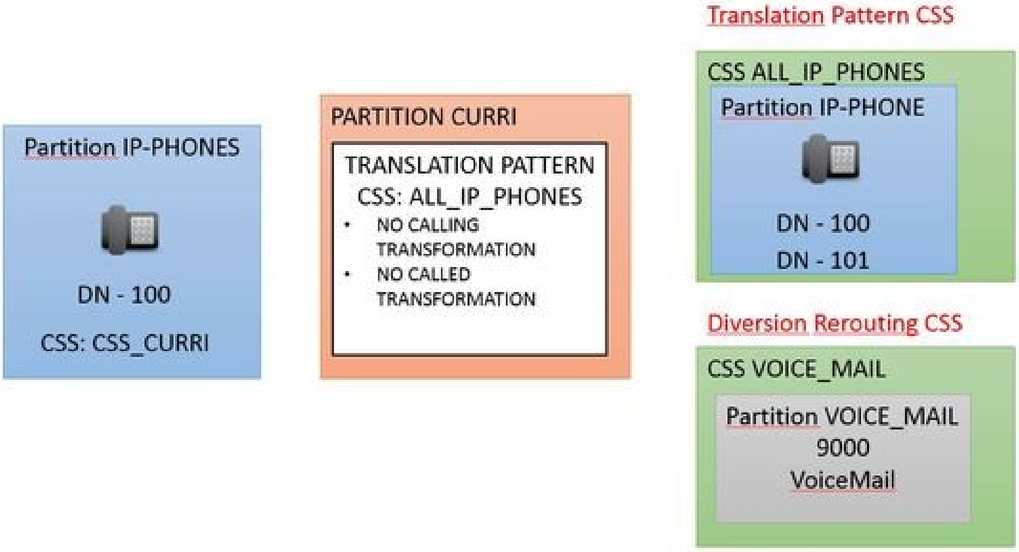
Status: Ready

External Call Control Information

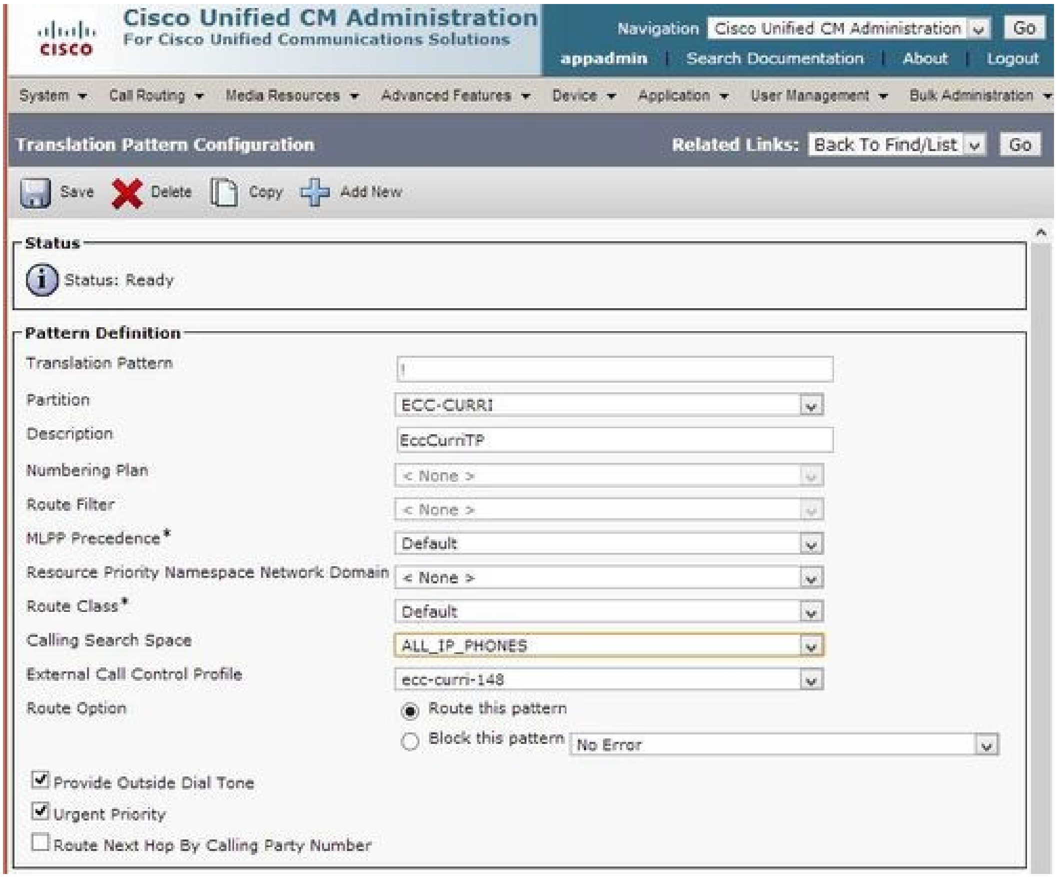
Name*	ecc-curri-148
Primary Web Service*	http://192.168.150.148:80/fw/curri
Secondary Web Service	
☐ Enable Load Balancing	
Routing Request Timer	3000
Diversion Rerouting Calling Search Space	ALL_IP_PHONES
Call Treatment on Failures*	Allow Calls

*- indicates required item.

In second image Voicemail number belongs to a different Calling Search Space, that includes only Voicemail numbers, so there will be the need of specify VOICE_MAIL as Diversion rerouting Calling Search Space.



Translation Pattern and External Call Control Profile must be configured this way:


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
appadmin | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration
Related Links: Back To Find/List Go
Save Delete Copy Add New

Translation Pattern Configuration

Status

Status: Ready

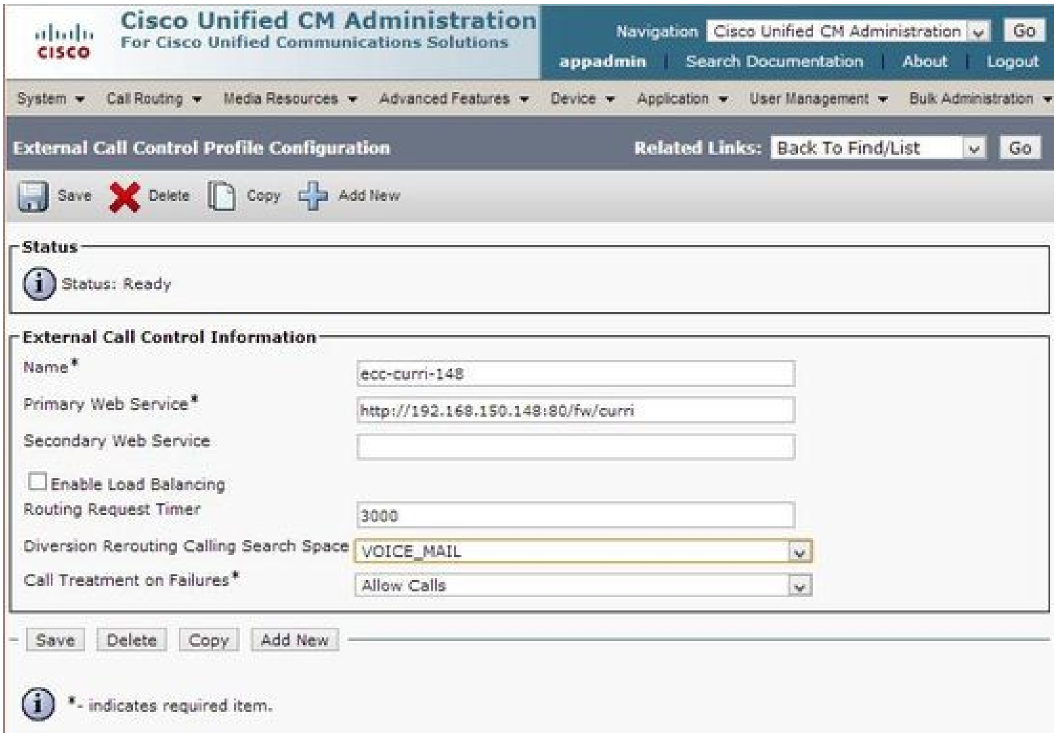
Pattern Definition

Translation Pattern	!
Partition	ECC-CURRI
Description	EccCurriTP
Numbering Plan	< None >
Route Filter	< None >
MLPP Precedence*	Default
Resource Priority Namespace Network Domain	< None >
Route Class*	Default
Calling Search Space	ALL_IP_PHONES
External Call Control Profile	ecc-curri-148
Route Option	● Route this pattern ○ Block this pattern No Error

☑ Provide Outside Dial Tone

☑ Urgent Priority

☐ Route Next Hop By Calling Party Number


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
appadmin | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration
External Call Control Profile Configuration
Related Links: Back To Find/List Go
Save Delete Copy Add New

Status

Status: Ready

External Call Control Information

Name* ecc-curri-148

Primary Web Service* http://192.168.150.148:80/fw/curri

Secondary Web Service

□ Enable Load Balancing

Routing Request Timer 3000

Diversion Rerouting Calling Search Space VOICE_MAIL

Call Treatment on Failures* Allow Calls

*- indicates required item.

NOTE: If you try to divert a blocked call to a number without specifying a Diversion rerouting Calling Search Space, Cisco CallManager will try to reroute the call with **Calling Search Space=NONE**, that will probably let the call run into a service unavailable pattern.

NOTE: Diversion is not compatible with Message playback, so if you specify both a block message and a diversion number, the External Call Control (Curri) plugin will only redirect the call without playing any message.

Notes on CuCM performance

Unified CM experiences some degree of performance degradation if it queries route servers for a majority of incoming calls.

The performance degradation depends on the following factors:

- Response time from route servers
- Network latency for call routing requests and responses

Slow response or network latency adds delay to the post-dial silence for a call. Testing shows that when the response time from the route server is below 50ms (RTT), there is a 15% degradation in the maximum call rate when all calls are subject to a Route Request/Response.

Call Block History & Basic Troubleshooting

A complete list of Calls processed by the Imagicle Application Suite External Call Control (CURRI) web service is accessible at the Phone Lock Calls History Web Page. This web page reports the full list of processed requests. It is possible to filter on a specific date, check the call resume (Time, calling, caller, decision and reason) and go deep in a single request opening the call detail. Here you can check the HttpRequest arrived at the web service, the HttpResponse given back to the Cisco CallManager and the specific Application Decisions taken by the Phone Lock Enterprise Service.
For a full list of call block reasons please refer the table at the end of this article.

Basic functional test

Make a call from an unlocked phone, verify that:

- Call passes
- Call is visible in the Calls History, with decision **Continue**

Lock phone and make a call to an unlocked phone, verify that:

- Call is blocked
- Call is visible in the Calls History, with decision **Deny**

For more Phone Lock troubleshooting tips and information please refer to this section.

Calls History Call Block Reasons Reference

Calling	Called	Description
UserLocked	None	Calling User Locked
UserLocked	UserLocked	Internal Call among locked Users
UserLocked	UserUnlocked	Internal call blocked due to caller block
UserLocked	ExternalNumber	Outgoing external call blocked due to caller block
UserLocked	UserLockedAllowedRemoteParty	Internal call blocked due to caller block
UserLocked	UserLockedAllowedSystemPolicy	Internal call blocked due to caller block (Incoming call block is disable)
UserUnlocked	UserUnlocked	Internal Call among unlocked Users
UserUnlocked	ExternalNumber	Outgoing external call from unlocked User
UserUnlocked	None	Calling User Unlocked
UserUnlocked	UserLocked	Internal Call blocked due to called block
UserUnlocked	UserLockedAllowedRemoteParty	Internal Call, called was locked but caller belongs to white list
UserUnlocked	UserLockedAllowedSystemPolicy	Internal call allowed by system policy (Incoming call block is disable)
ExternalNumber	None	External incoming call
ExternalNumber	UserUnlocked	External incoming call to unlocked User
ExternalNumber	UserLocked	External incoming call to locked User
ExternalNumber	UserLockedAllowedRemoteParty	External incoming call to locked User, from an allowed number
ExternalNumber	ExternalNumber	Call among two external numbers
ExternalNumber	UserLockedAllowedSystemPolicy	Incoming call allowed by system policy (Incoming call block is disable)
UserLockedAllowedRemoteParty	UserLocked	Called User Locked
UserLockedAllowedRemoteParty	UserUnlocked	Called User Unlocked, Called belong to white list
UserLockedAllowedRemoteParty	ExternalNumber	Outgoing Call from locked User to white list external number
UserLockedAllowedRemoteParty	None	Outgoing Call from locked User to white list number
UserLockedAllowedRemoteParty	UserLockedAllowedRemoteParty	Internal Call among locked Users both belonging to white list
UserLockedAllowedRemoteParty	UserLockedAllowedSystemPolicy	Internal call among two locked user, allowed by white list (Called is in white list) and system policy (Incoming call block is disable)
LicenseExpired	LicenseExpired	License expired or not valid

Product Configuration

UC Suite General Configuration

For Phone Lock to be able to run properly, please ensure that the CuCm Ip addresses on which the AXL service runs are configured in UCS System Parameters.

Please provision the **users' database** as explained in the General Configuration section of this guide, including First Extension number and a default PIN. If users are synchronized against CUCM, PIN codes are imported from CUCM End Users.

Note: If VoiceMail is licensed, the PIN must be 4 digits long.

Note: Starting from Imagicle 2020.Spring.1 release, Phone Lock TAPI engine can selectively lock overlapping extensions, if associated to different partitions and different phone devices. To enable this feature please populate relevant "Partition" field in Imagicle Users' list.

Note: If you are leveraging FAC (Forced Authorization Codes) or CMC (Client Matter Codes) to initiate an outbound call, please do not enable Phone Lock feature. Phone Lock operates at phone device or line level, so other phone devices/lines can still initiate outbound calls using FAC/CMC code of a blocked user.

AXL Configuration

To display the padlock or the phone status text message on the IP phones, StoneLock needs to know their IP addresses. It retrieves the IP address through AXL queries. For the AXL queries to be effective, please follow the steps to add an administrative user on the CuCM as described in the "Enabling AXL access".

Note: This configuration must be applied regardless the blocking technology you choose. It is needed both for CURRI and TAPI.

Managing the service

You can start and stop the service from the Manage Service web page.

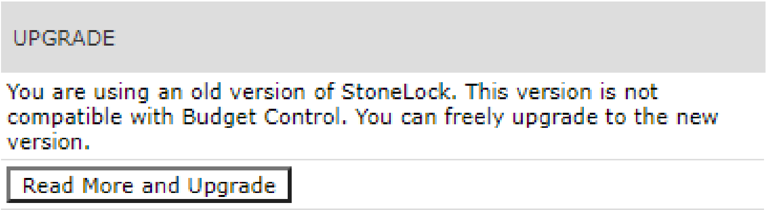
If you hit Stop button, all phone lines are unlocked, but the status message on the IP phone will remain unaffected. They return to existing lock status when you restart service. This is useful if you need to stop the service for a short time.

If you want to stop the service permanently, select the related checkbox. Before shutting down, Phone Lock resets the lock status displayed on the IP phone. The operation can take some minutes to complete.

Restarting the service is usually needed only if you change the license.

Phone Lock legacy service

Imagicle UC Suites prior to 2020.Summer.1 releases offered the option to leverage the legacy Phone Lock service called "Imagicle StoneLock" and, in "Manage Service" menu, you could find a dialog to allow the transition from legacy service to latest "Imagicle StoneLock Enterprise" service. See below:


UPGRADE

You are using an old version of StoneLock. This version is not compatible with Budget Control. You can freely upgrade to the new version.

Starting from 2021.Winter.1 release, above dialog doesn't appear anymore and Phone Lock application leverages the latest service by default.

Configuring emergency numbers

Please login to Imagicle web portal as administrator and select Phone lock **Global settings** menu option.

In "List of allowed numbers when phones are locked" window, please enter a list of allowed numbers/ranges following these rules:

a. Enter single numbers and/or patterns, one for each row
b. Use the character "!" in patterns to permit any sequence of digits. E.g. 9! means "any number starting by 9"
c. Use the character "." in patterns to permit any single digit. E.g. "9.." means 900, 901..

Service parameters

From this page you can also instruct Phone Lock to **Block Incoming calls when phone is locked**. In this case, when relevant DN/Device receives an incoming call, it is dropped.

Phone Lock can also **Clean Call History on locked phones**. If checked, IP Phone's call registry is automatically cleaned-up every time the phone is locked. You can also specify the retention period (days) for blocked calls history records.

Phone Lock Administration

How to reset the users' PIN

When the users access Phone Lock XML service, a personal PIN is requested. This pin is stored in the users' list.

A default PIN can be entered by the UC Suite administrator, when users list is created.

The users may change their PIN directly through the XML service or through the web interface.

Should a user forget his/her pin, he/she can reset it through the web interface. The PIN can also be reset by the administrator.

The maximum PIN length is 50.

Warning: the PIN is shared with other Imagicle applications and services. If VoiceMail is licensed, the user PIN length must be exactly 4.

Administratively locking phone device/line

The administrator can lock the user's phone line through the user's list. This setting overrides user's preference.

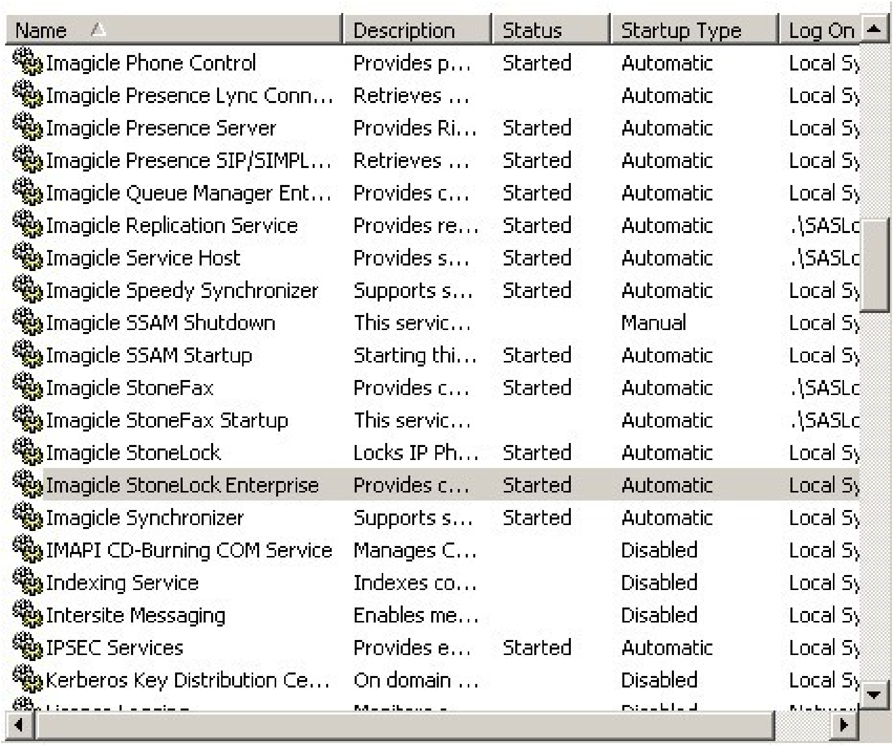
Quick troubleshooting tip: if a device is not associated to ImagicleCTI Application User on CUCM, Phone Lock TAPI engine can't lock the device. If CURRI engine is enabled, TAPI monitoring is not required.

License Activation

Phone Lock is licensed per user.

To activate the license, follow the standard procedure you can find in the General configuration section.

When the license is activated for the first time (and its status changes form "Evaluation" or "Expired" to "Licensed"), you have to stop and restart "Imagicle StoneLock" service in Windows Services Control Panel.



Name	Description	Status	Startup Type	Log On
Imagicle Phone Control	Provides p...	Started	Automatic	Local Sy
Imagicle Presence Lync Conn...	Retrieves ...		Automatic	Local Sy
Imagicle Presence Server	Provides Ri...	Started	Automatic	Local Sy
Imagicle Presence SIP/SIMPL...	Retrieves ...	Started	Automatic	Local Sy
Imagicle Queue Manager Ent...	Provides c...	Started	Automatic	Local Sy
Imagicle Replication Service	Provides re...	Started	Automatic	.\SASLc
Imagicle Service Host	Provides s...	Started	Automatic	.\SASLc
Imagicle Speedy Synchronizer	Supports s...	Started	Automatic	Local Sy
Imagicle SSAM Shutdown	This servic...		Manual	Local Sy
Imagicle SSAM Startup	Starting thi...	Started	Automatic	Local Sy
Imagicle StoneFax	Provides c...	Started	Automatic	.\SASLc
Imagicle StoneFax Startup	This servic...		Automatic	.\SASLc
Imagicle StoneLock	Locks IP Ph...	Started	Automatic	Local Sy
Imagicle StoneLock Enterprise	Provides c...	Started	Automatic	Local Sy
Imagicle Synchronizer	Supports s...	Started	Automatic	Local Sy
IMAPI CD-Burning COM Service	Manages C...		Disabled	Local Sy
Indexing Service	Indexes co...		Disabled	Local Sy
Intersite Messaging	Enables me...		Disabled	Local Sy
IPSEC Services	Provides e...	Started	Automatic	Local Sy
Kerberos Key Distribution Ce...	On domain ...		Disabled	Local Sy

Evaluation

Imagicle Phone Lock runs for 30 days in evaluation mode. During evaluation, Phone Lock can lock up to 250 phone lines. If more than 250 users are configured in the user's list, exceeding users' lines are not affected by Imagicle locking engine.

Old Phone Lock versions

If Phone Lock has been activated on an old UC Suite version, you need to explicitly decide to upgrade the service to the latest one. Upgrading the service results in the lock status of all IP phones to be lost, because the old version stored it in an XML file, while the new one associates it to the users list. The user's personal pin number is reset to VoiceMail pin number (if available). If the user's pin has never been set, it won't be asked the very first time user tries to change the phone lock status from IP Phone XML service.

To activate new service version, go to the "Manage Service" page. A button triggers the update. Then restart the service. Windows IIS is also restarted. Please login again on the web interface.

StoneLock REST APIs

Overview

Starting from 2020.Summer.1 Imagicle AppSuite release, StoneLock enables two REST APIs which allow respectively to lock and unlock phone lines, at global level or department level.

Required permissions

To invoke those APIs, the following permission levels are required:

- IAS Admin â Global users' visibility
- StoneLock "Complete Management" â Global users' visibility
- StoneLock "Manage Department User" â Own department users' visibility

EndPoint

To unlock phone lines:

```
http://{ias-server}/fw/Apps/StoneLock/WebAPI/Phones/Unlock
```

To lock phone lines:

```
http://{ias-server}/fw/Apps/StoneLock/WebAPI/Phones/Lock
```

Filters

You can invoke above APIs by optionally adding `QueryString` filters to further narrow the StoneLock action based on specific IAS users fields:

```
/Lock?filterField=<value>
```

Available fields for filtering are:

- department
- customField1
- customField2
- customField3
- customField4
- customField5
- customField6
- customField7
- customField8
- customField9
- customField10

API Invoke samples

Please find below a couple of samples to invoke StoneLock APIs:

Request URL (client REST, PUT)

```
http://staging.imagicle.local/fw/Apps/StoneLock/WebAPI/Phones/Lock?department=R%26D&customField1=
```

cURL

```
curl -X PUT
"http://staging.imagicle.local/fw/Apps/StoneLock/WebAPI/Phones/Lock?department=R%26D&customField1
-H "accept: */*"
```

Scheduled phone lines lock and unlock using Windows Task Scheduler

Windows Task Scheduler is suitable to schedule automatic phone lines lock and unlock at a certain time of the day. This is accomplished by creating a PowerShell script. See below the procedure to create such a script:

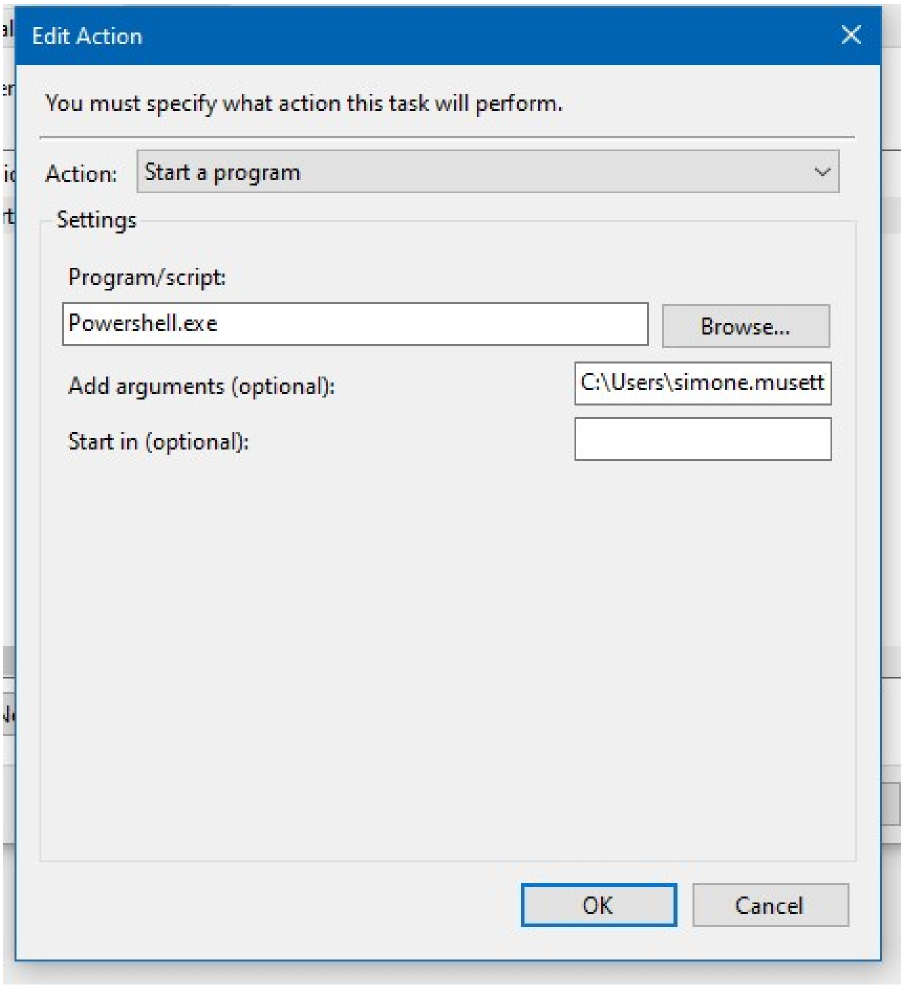
- Create a new PowerShell script using a text editor and call it **script.ps1**
- Copy the following code inside text file:

```
$username='' <# user on behalf of phones will be locked #>
$password='' <# password of the user on behalf of phones will be locked #>

<# set authentication headers for API request #>
$encodedCreds = [System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes("$($username):$($password)")
$Headers = @{
    Authorization = "Basic $encodedCreds"
}

<# set IAS parameters #>
$ias_url = '' <# IAS IP Address/FQDN affected by the API call #>
$action = 'Lock' <# action to be performed by the API (including filters) #>
$url = "http://$($ias_url)/fw/Apps/StoneLock/WebAPI/Phones/$($action)"

<# API request #>
Invoke-WebRequest -Uri $url -Headers $Headers -Method PUT
```

- Now configure above purple-marked field with the appropriate data:
    - **username**: IAS username of the user accessing StoneLock APIs
    - **password**: IAS password of the user accessing StoneLock APIs
    - **ias_url**: IAS FQDN/IP address where APIs are invoked (i.e. 192.168.1.60)
    - **action**: This is the action to be initiated through API call (Lock or Unlock). Here you can optionally add specific filters, with above mentioned syntax.

Windows Task Scheduler usage

- Launch Windows Task Scheduler from Start menu and create a new schedule, specifying a new action including:
    - **Program/script**: Powershell.exe
    - **Add arguments**: path to **script.ps1** text file



You must specify what action this task will perform.

Action: Start a program

Settings

Program/script: Powershell.exe

Add arguments (optional): C:\Users\simone.musett

Start in (optional):

- Please add trigger and conditions, based on desired schedule time.

Troubleshooting

Applies to StoneLock

Troubleshooting related to phone/jabber locking:

Can't access StoneLock service from IP Phone

- Check StoneLock Licenses are active on IAS and involved service is running.
- Check IP Phone user is properly configured on the IAS and the relevant phone device is retrieved by the AXL service running on CUCM.
- Check that XML phone service is subscribed to user's phone device and IAS Server is reachable by the phone via http/https.

Can't access to StoneLock from Jabber Desktop/Mobile Imagicle gadget

- Check StoneLock network configurations, make sure IAS server is reachable from clients on port 80 (http) or port 443 (https).
- Check StoneLock Licenses are active on IAS and that the involved service is running.

While trying to lock/unlock line from IP Phone, I get incorrect PIN message

- To avoid the case a wrong PIN is being inserted, define a new PIN in IAS user database.
- Phone status is not correctly refreshed. Check via Web Portal that phone IP address is available and PUSH test is positive. Check also that phone is visible from AXL.

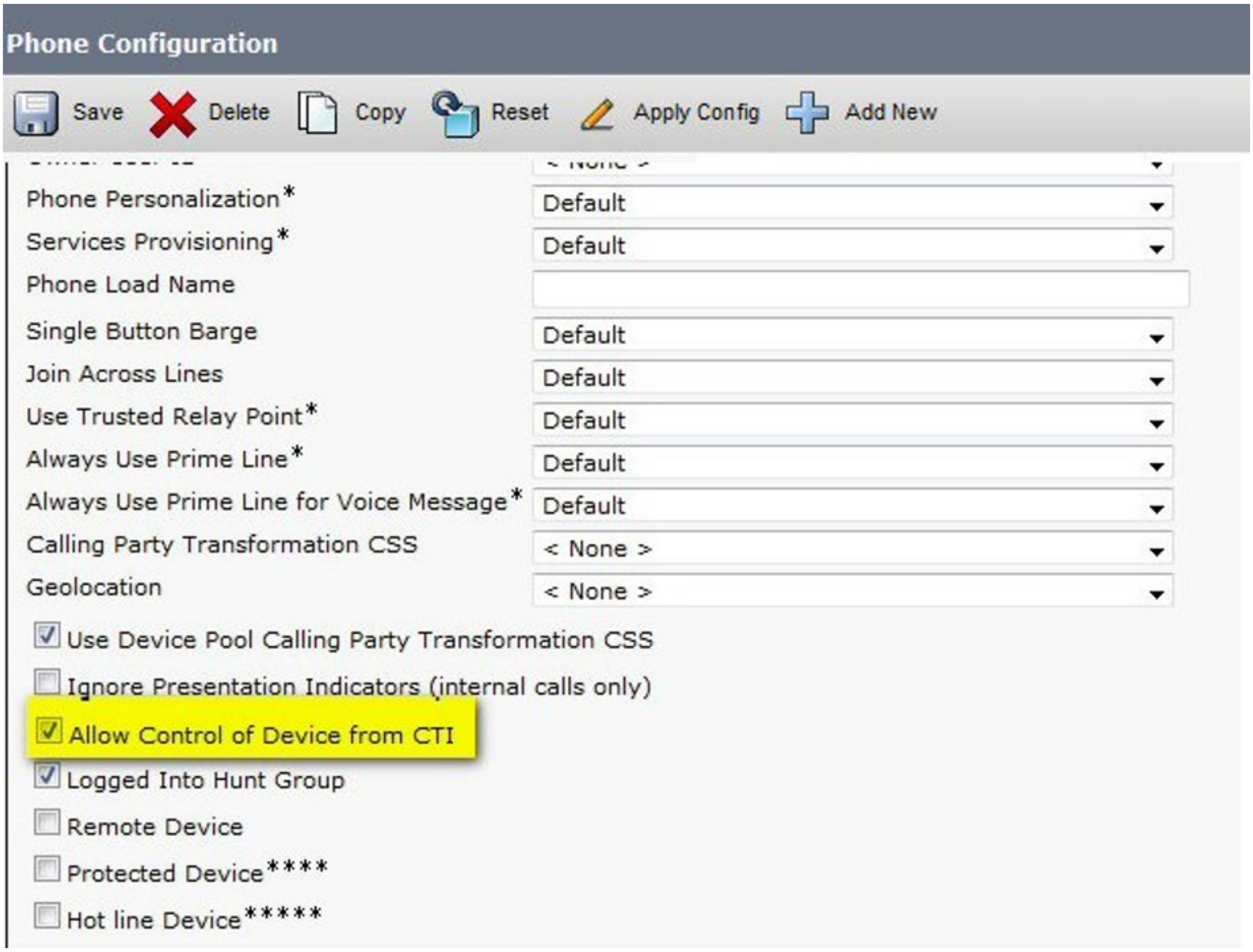
While phone is locked, I have no confirmation about actual lock status

- Please note that some phone devices are not showing lock status. This is why we recommend to configure an audio announcement in CUCM, triggered by StoneLock when phone is locked (CURRI method required). This will work for analog phones, too.

TAPI troubleshooting

1. If an IP Phone does not appear in Admin -> Support -> (details) page, it cannot be monitored by Stonelock. It must have both the "Detected by AXL" and "Detected By TAPI" flags. If not, please double check device association on the CallManager, and AXL configuration on the IAS server.

2. Check that the option "Allow Control of Device from CTI" is enabled in the phone configuration (Device --> Phone)

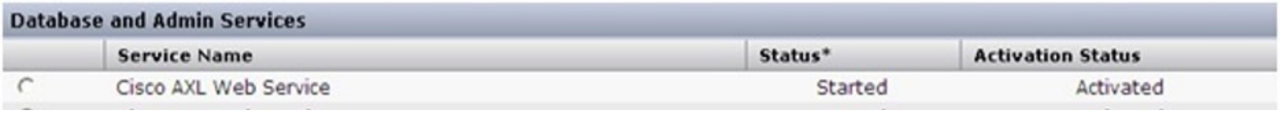


Phone Configuration

Phone Personalization*	Default
Services Provisioning*	Default
Phone Load Name	
Single Button Barge	Default
Join Across Lines	Default
Use Trusted Relay Point*	Default
Always Use Prime Line*	Default
Always Use Prime Line for Voice Message*	Default
Calling Party Transformation CSS	< None >
Geolocation	< None >

☑ Use Device Pool Calling Party Transformation CSS
□ Ignore Presentation Indicators (internal calls only)
☑ Allow Control of Device from CTI
☑ Logged Into Hunt Group
□ Remote Device
□ Protected Device****
□ Hot line Device*****

3. Check that the AXL Service is active. In case of CUCM cluster installations, check that the IP address you entered in the IAS telephony services mask is the one of the node on which the AXL service is activated.



Database and Admin Services

	Service Name	Status*	Activation Status
○	Cisco AXL Web Service	Started	Activated

CURRI troubleshooting

Outgoing call fails

Check Calling Search Space and Partition configuration, there are two common issues in this configuration:

- Loop creation, E.g. with the translation pattern and the called Directory Number in the same partition
- Call Flow is interrupted at some level, E.g. caller Calling Search Space include Translation Pattern, but Translation Pattern Calling Search Space doesn't include the partition containing IP phones

If calls pass but they aren't listed in the Calls History

First of all, we could be in the case that External Call Control hasn't been triggered. Check Calling Search Space and Partition configuration, translation pattern could not be involved in the call flow, use Cisco utility to analyze call flows in order to verify the translation pattern involvement.

If Cisco Call routing do trigger the External Call Control, there are two family of issues, depending on External Call Control Profile Call treatment on failures configuration:

- **Allow calls** option specified: there should be a problem with Imagicle Application Suite External Call Control (CURRI) Web service
    - Check your network configuration
        - Verify that Imagicle Application Server port 80 is reachable from Cisco CallManager.
        - In Imagicle Application Server performance Monitor add SAS:ECC-Curri: Last http HEAD request this counter shows the time elapsed from the last Cisco CallManager connection with IAS, Cisco CallManager tries to connect to IAS Web Service every 20 seconds in order to assure the connectivity and persist a connection for obtain faster routing responses. Check that this performance counter shows compliant information.
        - Verify that in StoneLock Global Settings Cisco External Call Control (CURRI) is chosen as Block Engine Technology.
- **Block calls** option specified: External Call Control hasn't been triggered
    - Check Calling Search Space and Partition configuration, translation pattern could not be involved in the call flow, use Cisco utility for analyse call flows in order to verify the translation pattern involvement

If Outgoing Call isn't blocked but it's listed in the Calls History

In this case you must verify the reason for the application decision, options are:

- License is not valid: check your license
- Called number is included in white list: calls for numbers in white list aren't blocked
- User has been recognized: if user hasn't been recognized, call isn't blocked, check Imagicle Application Suite configuration

If there is no block message specified

If you specified a block audio message in the Imagicle Application Suite StoneLock Settings Web Page but when a call is blocked caller can't hear any message you must verify the Calls History Web Page:

- if the call is displayed, check calls details, ECC Response section
    - if decision is continue, call hasn't been blocked, so caller isn't in block state
    - if decision is deny, but there is no Message field, check StoneLock settings, you could haven't configured the message (E.g. you forgot to save settings)
    - if decision is deny and there is a Message field check the field value:
        - the value and the Cisco CallManager Announcement Identifier must match exactly, if they don't, let them match
        - the Announcement must be available for the locales of all the phones that are using the service
- If the call isn't displayed, check earlier in this section

If the call isn't redirected to the specified number

If you specified a redirection number in the Imagicle Application Suite StoneLock Settings Web Page but calls is only blocked without redirection, you must verify the Calls History Web Page:

- If the call is displayed, check calls details, ECC Response section
    - if decision is continue, call hasn't been blocked, so caller isn't in block state
    - if decision is deny, check StoneLock settings, you could haven't configured the redirection number (E.g. you forgot to save settings)
    - if decision is divert check the divert destination field value:
        - if the number is correct, check Diversion rerouting Calling Search Space in External Call Control Profile configuration, if everything seems to be ok, try to reconstruct the call flow with Cisco Dialled number analyzer in order to determine where the call fails
        - if the number isn't correct, change it in the StoneLock settings
- If the call isn't displayed, check earlier in this section

Cisco Call Manager and Imagicle web service Troubleshooting

Regarding External Call Control - CURRI plugin, Cisco Call Manager could raise some error events to Administrator (You can monitor them also with your Cisco Call Manager Real Time Monitoring Tool). Possible Alarms are:

A web service connection error occurs when Unified CM fails to establish a connection with the web service. The following reasons may cause this failure:

- The web service is not in service.
- Slow responses from the web service that cause Unified CM to time out for two consecutive call routing or Keep-Alive requests.

Unified CM handles this failure with the following actions:

- Issues a ConnectionFailureToPDP error alarm.
- Switches to standby web service for call routing requests, if two URIs are provisioned in the external call control profile to operate in active-standby mode.
- Starts sending all call routing requests to the other web service that Unified CM still has good connections with, if two URIs are provisioned in the external call control profile to operate in load balance mode.
- Retries to establish connections to the web service.
- If no web service is available for call routing request, then follows the Call Treatment on Failure configuration as set on the external call control profile to route the call.

Actions

Check your network configuration

- Verify that Imagicle Application Server port 80 is reachable from Cisco CallManager.
- In Imagicle Application Server performance Monitor add "SAS:ECC-Curri: Last http HEAD request" this counter shows the time elapsed from the last Cisco CallManager connection with IAS, Cisco CallManager tries to connect to IAS Web Service every 20 seconds in order to assure the connectivity and persist a connection for obtain faster routing responses. Check that this performance counter shows compliant information.

Cisco Call Manager routing request timer expires before receiving the call routing response from the Imagicle web service:

The routing request timer is the maximum time in milliseconds that Unified CM waits for the response from the web service for a call routing request. The routing request timer can be provisioned in an external call control profile in the range of 1000 to 5000 milliseconds. If the timer is not set in the external call control profile, the cluster wide service parameter "External Call Control Routing Request Timer" takes effect. The default value for the timer is 2000 milliseconds.

Unified CM takes the following actions when the routing request timer expires before receiving the call routing response:

- Issues an AwaitingResponseFromPDPTimeout error alarm.

Routes the call following the Call Treatment on Failure configuration set on the external call control profile.

Actions

Check your network configuration

The Imagicle web service can return a 4XX or 5XX error response to Unified CM to indicate invalid call routing requests or internal errors when processing a request from Unified CM.

Unified CM takes the following actions for a 4XX or 5XX error response from the Imagicle web service:

- Issues a FailureResponseFromPDP error alarm.
- Routes the call following the Call Treatment on Failure configuration on the external call control profile.

Unified CM takes the following actions when the response from the web service contains the status indicating request errors:

- Issues an ErrorParsingResponseFromPDP warning alarm.
- Routes the call by following the call routing directive in the response.

Actions

Imagicle Application Suite Application Server is answering to Cisco Call Manager requests, but it's encountering some problems.

- Check configured External Call Control Profile link.
- Check StoneLock Enterprise service status, try to restart it.

Cisco CallManager encountered a problem parsing Imagicle Application Suite Application Server requests.

Unified CM takes the following actions when it fails parsing the response:

- Issues an ErrorParsingDirectiveFromPDP error alarm.
- Routes the call following the "Call Treatment on Failure" configuration on the external call control profile.

Actions

- Check StoneLock Enterprise service status and Internet Information Service on Imagicle Application Suite, try to restart it.