Cloudonix Registration-Free Dialing™

Cloudonix supports many deployment scenarios, one is a custom dialing policy in which the SIP subscriber doesn't dial directly using Cloudonix SIP subscriber gateway and built-in external or internal routing, instead a custom application can request a dial-out or a dial-in from a custom application backend that controls routing for incoming or outgoing calls.

Sample use cases:

- The application can't or won't propagate SIP authentication details to the Cloudonix SIP gateway, for example because the application is using third-party and/or non-password based authentication,
- The application cannot maintain an active SIP registration due to battery or connectivity constraints, e.g. mobile device or IoT.

Architecture

Traditional SIP services require each device to be registered at all times. The Cloudonix service has the option of this traditional requirement, or alternatively allowing either pre-authentication or just in time authentication.

Outbound calls performed under the registration-free dialing policy are negotiated between the custom application's backend and the Cloudonix API before the actual SIP session is initiated - this allows the application to negotiate an authentication token on behalf of the SIP client. When the SIP client initiates the SIP session it authenticates with the Cloudonix subscriber gateway using that authentication token.

The process for inbound calls is similar except in such a case the Cloudonix service calls the custom application backend initially to notify it of the incoming call, so the custom backend can signal (using its own custom protocol - e.g. push notifications) the UA application to initiate a SIP session with the Cloudonix subscriber gateway in order to "receive the call".

Workflow

Call Initiation

1. Subscriber's UA initiates call through the customer backend.
2. Customer backend calls Cloudonix API Call Management Service's *Session Initiation* method, to receive a new call management token. The application backend can submit - in the same call - a custom routing scenario for just the current call.
3. Customer backend returns call management token to the subscriber's UA.

4. Subscriber's application initializes the SDK with the subscriber's account details (number and domain) and sends unregistered invite with:
    a. Call management token as the header "`X-Cloudonix-Session`".
    b. Subscriber domain as the header "`X-Cloudonix-Domain`"
5. Cloudonix Subscriber Gateway intercepts the dial and validates the token. If the token is invalid, the call is rejected as if SIP authentication failed.
6. Cloudonix Subscriber Gateway resolve a Cloudonix Voice Application Server address automatically and forwards the call.
7. Cloudonix Voice Application Server receives the call and call token, and routes the call according the destination number and the configured application logic and routing.

Call Reception

1. A call is received in the Cloudonix Voice Application Server, and according to the configured application logic - should be routed to an application subscriber.
2. Cloudonix Voice Application Server runs the Call Routing Application.
3. Call Routing Application logic verifies that the destination number is for a valid subscriber, otherwise it can reject the call.
4. Call Routing Application verifies that the incoming call has a Registration-Free session token, otherwise it calls the Cloudonix API Call Management Service's *Session Initiation* method to register a new call management token.
5. Application backend notifies the subscriber application of the incoming call and sends it the call management token and any relevant details.
6. Call Routing Application returns instructions to the Cloudonix Voice Application Server to park the incoming call in a bridge associated with the call management token.
7. Cloudonix Voice Application Server registers the call token in "incoming calls" list and sends "ringing" to caller (accepts the call).
8. Cloudonix Voice Application Server waits for call completion, rejection or the built-in timeout to expire.
9. Subscriber application starts a long poll on the Cloudonix API Call Management Service's *Session Control - Ringing Notification* endpoint.
10. Subscriber's application simulates an incoming call (ringing, etc) and waits for the user to pick up.
11. Subscriber's application initializes the SDK with the subscriber's account details (number and domain) and the call management token as the header "`X-Cloudonix-Session`", then dials with any text as the call destination.
12. Cloudoix Subscriber Gateway intercepts the dial and validates the token. If the token is invalid the call is rejected.
13. Cloudonix Subscriber Gateway resolves the address of the Cloudonix Voice Application Server holding the incoming call and forwards the call to that server.
14. Cloudonix Voice Application Server receives the call and the call token, and looks up the token in the "incoming calls" list. If the call management token did not match, it rejects the call.

15. Cloudonix Voice Application Server creates a bridge for the incoming call.
16. Cloudonix Voice Application Server connects incoming call to the new bridge.
17. Cloudonix API Call Management Service's *Session Control - Ringing Notification* returns a 200 ("OK") HTTP response, letting the subscriber's application's know the session has been connected.

Incoming Call Cancellation - Callee Side

In the Call Reception process if at stage 10 the callee decides to reject the call or the ringing timed out by the UA (should be a lower timeout than the Cloudonix built-in timeout), the following process continues after stage 10:

1. Subscriber application notifies the application backend about the cancellation, including cancel reason - one of: rejected, timeout.
2. Application backend calls Cloudonix API Call Management Service's *cancel call* to notify about the rejection with the call management token.
3. Cloudonix API Call Management Service call Cloudonix Voice Application Server Session Control service and notifies it of cancellation.
4. Cloudonix Voice Application Server Session Control service looks up the token in the "incoming list". If the call management token matches it will notify the incoming call controller to drop the call.

Incoming Call Cancellation - Caller Side

During a call to a Registration-Free™ subscriber, if the caller decides to cancel the call, they disconnect the call from their side. As a result the Cloudonix Voice Application Server cancels the session In the progress and causes the Cloudonix API Call Management Service's *Session Control - Ringing Notification* to return a 205 ("Reset Content") HTTP response, to let the Callee know that the session was cancelled.

Domain Configuration

The behavior of the Registration-Free flow in Cloudonix is controlled by domain-level configuration stored in the domain profile. The domain profile can be edited using the Cloudonix Dashboard or through the Cloudonix API.Core REST API.

To enable Registration-Free support in a domain, set the field "`registration-free-control-endpoint`" to the URL of the application backend endpoint that should receive incoming call notifications from Cloudonix.

Additionally the following domain profile fields control Registration-Free behavior:

- `call-timeout` - maximum time in seconds for the Cloudonix stack to wait for an incoming call to be picked up, before declaring the call "unanswered". Default: `60`

API Documentation

The Cloudonix Registration-Free Dialing™ relies on both the Cloudonix system providing the session management API to the subscriber application backend, as well as the subscriber application backend providing an API to allow Cloudonix to notify it of incoming calls.

This section details both APIs, the Cloudonix side is called the Call Control and Session Management REST API, while the subscriber application backend side is called the Registration-Free Control Endpoint REST API.

Call Control and Session Management REST API

Pre-Dial Session Initiation - Outgoing

```
POST /calls/<domain-name-or-id>/outgoing/<subscriber-msisdn>
```

This call is used by a subscriber application backend service to authorize a subscriber for Registration-Free Dialing™ outgoing call. The token generated by the response can then used for SIP dialing without the UA needing to register first and without providing SIP credentials.

The API call may include a routing plan, in which case the Cloudonix VoIP stack will act on the provided routing plan. Otherwise Cloudonix will use a different routing plan based on the domain configuration, either a default routing plan or to use the LCR module configured for the domain.

Conditions

This is a privileged API and requires system administrator, tenant administrator, or domain administrator authorization for the specified domain. When the server receives a call with lesser authorization it must return a 401 (“Unauthorized”) HTTP error response and stop processing.

Request

The following data field must be provided in the request URL:

- Domain name or id - the domain name or Cloudonix domain ID in which the specified subscriber is registered and in which to route the call.
- Subscriber MSISDN - the E164 MSISDN number of the subscriber for which to generate the session token.

The following data field must be provided in a JSON document sent in the request body:

- `destination` - The destination number to which the subscriber is going to dial.

The following data field may be provided in a JSON document sent in the request body:

- `routing` - The routing plan for the call in JSON format according to the LCR API.
- `timeLimit` - The maximum time to allow for the call specified, in seconds. After that time has passed in the call, Cloudonix Voice Application Service will disconnect the call automatically.
- `callback` - A URL to be called with the session status changes. Whenever additional session data changes (after the initial creation) the API.Core will send a POST request to that URL with the session object (the same as being returned in this call's response).

Response

If the request is successful, the server will respond with an HTTP 200 ("OK") response with the content type "application/json" containing a JSON document with the generated session token.

If the request is for a subscriber that does not exist, the server will respond with an HTTP error 404 ("Not Found") response.

Example

```
POST /calls/example.com/outgoing/972547340014
Host: api.voice.cloudonix.io
Authorization: bearer XI1234567890
Content-Type: application/json

{
  "destination": "63121233333",
  "timeLimit": 7205,
  "routing": {
    "sellrate": 0.02,
    "sellrate_mimimum": 60,
    "sellrate_increment": 60,
    "route": [
      {
        "provider_id": 1,
        "rate_id": 302,
        "cx_trunk_id": 101,
        "offer_id": 1,
        "termination_ip": "187.33.22.44:5060",
        "termination_number": "2828#63121233333",
        "buyrate": 0.012,
        "buyrate_minimum": 1,
        "buyrate_increment": 1
```

```
      },
      {
        "provider_id": 1,
        "rate_id": 302,
        "cx_trunk_id": 102,
        "offer_id": 1,
        "termination_ip": "187.33.22.45:5060",
        "termination_number": "2828#63121233333",
        "buyrate": 0.012,
        "buyrate_minimum": 1,
        "buyrate_increment": 1
      }
    ]
  }
}

HTTP/1.1 200 OK

{
  "domainId": 3,
  "subscriberId": 372,
  "destination": "63121233333",
  "direction": “outgoing",
  "token": "16a7294c989b11e7b3d32b9edb8660c7",
  "timeLimit": 7205
}
```

Pre-Dial Session Initiation - Incoming

```
POST /calls/<domain-name-or-id>/incoming/<subscriber-msisdn>
```

This call is used by a call routing application (such as the built-in Cloudonix call routing application, or a custom call routing application configured for the domain) to authorize a subscriber for Registration-Free Dialing™ incoming call. The token generated by the response can then used for SIP dialing without the UA needing to register first and without providing SIP credentials, and will automatically connect the SIP session to an existing incoming connection bridge for the same token.

Conditions

This is a privileged API and requires system administrator, tenant administrator, domain administrator or an application authorization for the specified domain. When the server receives

a call with lesser authorization it must return a 401 (“Unauthorized”) HTTP error response and stop processing.

Request

The following data field must be provided in the request URL:

- Domain name or id - the domain name or Cloudonix domain ID in which the specified subscriber is registered and in which to route the call.
- Subscriber MSISDN - the E164 MSISDN number of the subscriber receiving the call, and for which to generate the session token.

The following data field must be provided in a JSON document sent in the request body:

- `origination` - The originating number from which the incoming call was received.
- `callback` - A URL to be called with the session status changes. Whenever additional session data changes (after the initial creation) the API.Core will send a POST request to that URL with the session object (the same as being returned in this call’s response).

Response

If the request is successful, the server will respond with an HTTP 200 (“OK”) response with the content type “application/json” containing a JSON document with the generated session token.

If the request is for a subscriber that does not exist, the server will respond with an HTTP error 404 (“Not Found”) response.

Example

```
POST /calls/example.com/incoming/972547340014
Host: api.voice.cloudonix.io
Authorization: bearer XI1234567890
Content-Type: application/json

{
  "origination": "63121233333"
}

HTTP/1.1 200 OK

{
  "domainId": 3,
  "subscriberId": 372,
  "origination": "63121233333",
  "direction": “incoming",
```

```
  "token": "13d9704298d411e78d1d0f7dca1eed08",
  "timeLimit": null
}
```

Session Control - Update Time Limit

```
PATCH /calls/<domain-name-or-id>/sessions/<token>
PATCH /calls/<domain-name-or-id>/outgoing/<subscriber-msisdn>/<token>
PATCH /calls/<domain-name-or-id>/incoming/<subscriber-msisdn>/<token>
```

This call is used by an application backend to change the parameters of an outgoing call session in progress.

Conditions

This is a privileged API and requires system administrator, tenant administrator, domain administrator or an application authorization for the specified domain. When the server receives a call with lesser authorization it must return a 401 (“Unauthorized”) HTTP error response and stop processing.

Request

The following data field must be provided in the request URL:

- Domain name or id - the domain name or Cloudonix domain ID in which the specified subscriber is registered and in which to route the call.
- Token - the session token for the session that will be updated.

The following data field must be provided in the request URL when using the “outgoing” call:

- Subscriber MSISDN - the E164 MSISDN of the subscriber this session is originating from.

The following data field must be provided in the request URL when using the “incoming” call:

- Subscriber MSISDN - the E164 MSISDN of the subscriber this session is terminating to.

The following data field may be provided in a JSON document sent in the request body:

- `timeLimit` - an updated session time limit, in seconds, to apply to the session.
- `callStartTime` - set the call start timestamp if it wasn’t set already. May be used by the call routing application to update an incoming call session data.

Response

If the request is successful, the server will respond with an HTTP 200 (“OK”) response with the content type “application/json” containing a JSON document with the session details.

If the request is for a session token that doesn't exist, the server will respond with an HTTP error 404 ("Not Found") response.

Example

```
PATCH /calls/example.com/outgoing/972547340014/16a7294c989b11e7b3d…
Host: api.voice.cloudonix.io
Authorization: bearer XI1234567890
Content-Type: application/json

{
  "timeLimit": 60
}

HTTP/1.1 200 OK

{
  "domainId": 3,
  "subscriberId": 372,
  "destination": "63121233333",
  "direction": “outgoing",
  "token": "16a7294c989b11e7b3d32b9edb8660c7",
  "timeLimit": 60
}
```

Session Control - Ringing Notification

This call is used by an MUA receiving a call to notify the API.Core that it started ringing and to wait for confirmation on pickup or disconnect. This API call is intended to be used for long polling and is expected to wait for a pickup event or a cancel event, which may take a long time - thus it is recommended that client set a request timeout of at least 5 minutes.

```
GET /calls/<domain-name-or-id>/ringing/<msisdn>/<token>
```

Conditions

This is an unprivileged API and does not require any authorization. Access control is ensured by forcing the caller to know a valid session token and the destination subscriber's MSISDN for that session.

Request

The following data fields must be provided in the URL of the request:

- `domain-name-or-id` - the domain name or Cloudonix domain ID in which the specified session is registered.
- `msisdn` - the E164 MSISDN of the subscriber this session is terminating to.
- `token` - the session token for the session to be notified.

Response

If the request is successful the server will respond with either a 200 (“OK”) HTTP response if the session was picked up or a 205 (“Reset Content”) HTTP response if the session was disconnected by the caller before it was picked up by calee. In either case the response will have the `application/json` content type and contain a JSON document describing the status of the session.

The response JSON document will contain the following fields:

- `status` - String: The session status description

If the request does not fulfil all of the following conditions, the server will respond with a 403 (“Forbidden”) HTTP error:

- The session token specified in the request matches a session belonging to the domain specified in the request.
- The session specified has a terminating subscriber.
- The MSISDN specified in the request matches the MSISDN of the terminating subscriber.
- The terminating subscriber is active.
- The session status is either “`new`” or “`ringing`”

Example

```
GET /calls/example.com/ringing/972547340014/16a7294c989b11e7 HTTP/1.1
Host: api.cloudonix.io

HTTP/1.1 200 OK
Content-Type: application/json

{
  "status": "ringing"
}
```

Session Control - Retrieve Session

```
GET /calls/<domain-name-or-id>/sessions/<token>
GET /calls/<domain-name-or-id>/outgoing/<msisdn>/<token>
GET /calls/<domain-name-or-id>/incoming/<msisdn>/<token>
```

This call is used by Cloudonix services to lookup session data, but can also be used by application backends to recall session data.

Conditions

This is a privileged API and requires system administrator, tenant administrator, domain administrator or an application authorization for the specified domain. When the server receives a call with lesser authorization it must return a 401 (“Unauthorized”) HTTP error response and stop processing.

Request

The following data fields must be provided in the request URL:

- Domain name or id - the domain name or Cloudonix domain ID in which the specified session is registered.
- Token - the session token for the session to be retrieved.

The following data field must be provided in the request URL when using the “outgoing” call:

- Subscriber MSISDN - the E164 MSISDN of the subscriber this session is originating from.

The following data field must be provided in the request URL when using the “incoming” call:

- Subscriber MSISDN - the E164 MSISDN of the subscriber this session is terminating to.

Response

If the request is successful, the server will respond with an HTTP 200 (“OK”) response with the content type “application/json” containing a JSON document with the session details.

If the request is for a session that does not exist, or is not of the correct type or with the correct MSISDN (for the relevant calls) the server will respond with an HTTP error 404 (“Not Found”) response.

Example

```
GET /calls/example.com/sessions/16a7294c989b11e7b3d32b9edb8660c7
Host: api.voice.cloudonix.io
Authorization: bearer XI1234567890

HTTP/1.1 200 OK

{
  "domainId": 3,
```

```
  "subscriberId": 372,
  "remote": "63121233333",
  "direction": “outgoing",
  "token": "16a7294c989b11e7b3d32b9edb8660c7",
  "timeLimit": 7205,
  "routing": {
    "sellrate": 0.02,
    "sellrate_mimimum": 60,
    "sellrate_increment": 60,
    "routes": [
      {
        "provider_id": 1,
        "rate_id": 302,
        "cx_trunk_id": 101,
        "offer_id": 1,
        "termination_ip": "187.33.22.44:5060",
        "termination_number": "2828#63121233333",
        "buyrate": 0.012,
        "buyrate_minimum": 1,
        "buyrate_increment": 1
      },
      {
        "provider_id": 1,
        "rate_id": 302,
        "cx_trunk_id": 102,
        "offer_id": 1,
        "termination_ip": "187.33.22.45:5060",
        "termination_number": "2828#63121233333",
        "buyrate": 0.012,
        "buyrate_minimum": 1,
        "buyrate_increment": 1
      }
    ]
  }
}
```

Session Control - List Sessions

```
GET /calls/<domain-name-or-id>/sessions
```

This call is used by an application backend to enumerate ongoing sessions.

Conditions

This is a privileged API and requires system administrator, tenant administrator, domain administrator or an application authorization for the specified domain. When the server receives a call with lesser authorization it must return a 401 (“Unauthorized”) HTTP error response and stop processing.

Request

The following data field must be provided in the request URL:

- Domain name or id - the domain name or Cloudonix domain ID in which the specified session is registered.

Response

If the request is successful, the server will respond with an HTTP 200 (“OK”) response with the content type “application/json” containing a JSON document with a list of session records, each with all session details except routing details (if set).

Example

```
GET /calls/example.com/sessions
Host: api.voice.cloudonix.io
Authorization: bearer XI1234567890

HTTP/1.1 200 OK

[
  {
    "domainId": 3,
    "subscriberId": 372,
    "remote": "63121233333",
    "direction": “outgoing",
    "token": "16a7294c989b11e7b3d32b9edb8660c7",
    "timeLimit": 7205
  },
  {
    "domainId": 3,
    "subscriberId": 15,
    "remote": "12124459087",
    "direction": “incoming",
    "token": "09bc786c98e711e7aa5927c0c5bb7cb4",
```

```
    "timeLimit": null
  }
]
```

Session Control - Destroy Session

```
DELETE /calls/<domain-name-or-id>/sessions/<token>[?reason=<reason>]
```

This call can be use by the application backend to disconnect ongoing calls, or by Cloudonix services to remove the session data once the call has ended.

Conditions

This is a privileged API and requires system administrator, tenant administrator, domain administrator or an application authorization for the specified domain. When the server receives a call with lesser authorization it must return a 401 (“Unauthorized”) HTTP error response and stop processing.

Request

The following data fields must be provided in the request URL:

- Domain name or id - the domain name or Cloudonix domain ID in which the specified session is registered.
- Token - the session token for the session to be retrieved.

The following data field may be provided in the request query string:

- `reason` - The reason for cancelling the session. May be one of:
    - `timeout` - the subscriber cannot be reached (either they’re offline or have not responded in time)
    - `denied` - the subscriber has rejected the call
    - `busy` - the subscriber cannot take the call (another call is in progress)
    - `nocredit` - the subscriber has ran out of credit

Response

If the request is successful, the server will respond with an HTTP 204 (“No Content”) response.

If the session being deleted has a `callback` field set to a URL, then the server will send a POST request to that URL with the session object as it looked just before the deletion with the additional field `action` set to `deleted`.

Example

```
DELETE /calls/example.com/sessions/16a7294c989b11e7b3d32b9edb8660c7
```

```
Host: api.voice.cloudonix.io
Authorization: bearer XI1234567890

HTTP/1.1 204 No Content
```

Registration-Free Control Endpoint API

This API must be implemented by the subscriber application backend service, and the endpoint URL must be configured in the Cloudonix system by setting the domain profile attribute `registration-free-control-endpoint` to the URL of the subscriber application backend, using the Cloudonix Dashboard or using API.Core REST API - for example like so:

```
PATCH /tenants/1/domains/12 HTTP/1.1
Host: api.voice.cloudonix.io
Authorization: bearer XI1234567890
Content-Type: application/json

{
  "profile": {
    "registration-free-control-endpoint": "https://app.com/incoming"
  }
}
```

Incoming Call Notification

This API is invoked by Cloudonix to notify the subscriber application backend of an incoming call to a specific subscriber.

```
POST <registration-free-control-endpoint>
```

Request

The following data fields must be provided in the request body, as properties in a JSON object:

- `dnid` - the MSISDN of the subscriber to which the incoming call it being terminated.
- `caller-id` - the number that was reported to Cloudonix as the originating caller.
- `session` - the Registration-Free™ session token that the subscriber should connect to.
- `subscriber` - the Cloudonix subscriber record for the receiving subscriber account.
- `domain-id` - the numeric domain identifier of the Cloudonix domain of the subscriber receiving the call.
- `domain` - the domain name of the Cloudonix domain of the subscriber receiving the call.
- `endpoint` - the URL to the API.Core API.

Response

If the request is successful, the server must respond with any HTTP 200 class response (such as 200 “OK”, 201 “Created” or 204 “No Content”). The body of the response, if any, will be ignored.

If the request was not handled successfully because the subscriber MSISDN (in the `dnid` field) does not exist, the server must respond with an HTTP 404 (“Not Found”) error, to signal Cloudonix to reject the call. The body of the response, if any, will be ignored.

If the request was not handled due a temporary problem and Cloudonix should retry the transaction, the server must respond with an HTTP 500 class error response (such as 500 “Internal Server Error” or 503 “Service Unavailable”). The body of the response, if any, will be ignored.

Any other response will cause Cloudonix to reject the call with a permanent error status.

Example

```
POST /incoming HTTP/1.1
Host: app.com
Content-Type: application/json

{
  "dnid": "972547340014",
  "caller-id": "+15155558484",
  "session": "4b3239e2-ad9d-11e7-b2d0-33c35612ef0a",
  "subscriber": {
    …
  },
  "domain-id": 17,
  "domain": "example.com",
  "endpoint": "https://api.cloudonix.io",
}

HTTP/1.1 204 No Content
```