A MITEL
PRODUCT
GUIDE

CloudLink Gateway

CloudLink Gateway User Guide

July 2025

Mitel
Powering connections

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by **Mitel Networks Corporation (MITEL®).**The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC), its affiliates, parents, or subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website:http://www.mitel.com/trademarks.

Contents

Overview 1

This chapter contains the following sections:

Welcome to CloudLink! Before you onboard your first customer, see the topics listed below, which will provide answers to the following questions:

What are the components of the CloudLink platform?

What are the processes required to deploy CloudLink applications for a customer?

What is the Partner Dashboard?

1.1 What is CloudLink?

Mitel CloudLink is a platform that enables communication between the on-premise PBX (such as MiVoice Office 400) and cloud-based applications such as Mitel One.

CloudLink includes:

- **CloudLink Platform**- The technology platform that provides services for CloudLink apps.
- **CloudLink Gateway**-Technology that connects premise-based PBXs to the CloudLink platform and CloudLink applications.
- **CloudLink Apps**-The applications that use the CloudLink Application Programming Interfaces (APIs) and micro-services to provide hybrid communications services to our customers. For example, Mitel One application.

1.2 Deployment Workflow

The following topics document the most important processes for deploying Mitel CloudLink applications for your customers:

- **Configure the PBX**
  - Configure MiVoice Office 400 PBX
    - Configure MiVoice Office 400 on Standalone Platform
    - Configure MiVoice Office 400 on SMBC Platform
    - Configure MiVoice Office 400 on Virtual Appliance on page 100
  - Configure a MiVoice Business PBX
  - Configure a MiVoice MX-ONE PBX on page 109
  - Configure a MiVoice Office 5000 PBX on page 110
- Deploy the CloudLink Gateway
- Access the CloudLink Gateway
- Onboard Users and Configure integration

Within the above topics you will find different instructions for the different supported MiVoice Office PBX models.

Customers will be able to utilize a CloudLink application by doing the following:

- Downloading and installing the CloudLink app
- Registering the CloudLink app

1.3 Managing Customer Accounts

The home page of Mitel Administration can be used to do the following:

- Create customers in the CloudLink platform. For more details, see Create Accounts.
- Associate a CloudLink Gateway with a customer. For more details, see Gateway Integration.
- View and manage previously created CloudLink customers. For more details, see Managing Accounts.

After you create a customer in Mitel Administration, that customer is listed in the https://accounts.mitel.io/.

1.4 Best Practices for Site Deployments

The following is a list of best practices recommended for CloudLink site deployments:

- If there is no DHCP server on site, configure a MiVoice Office PBX or use another DHCP server.
- For standalone platforms, the CloudLink Gateway appliance and MiVoice Office PBX should be installed on the same LAN subnet. If this is not done, disable all SIP ALG functions in the firewall to enable communication between these two components. Additionally, ensure that port blocking is disabled.
- When you configure a firewall, ensure that the path to the Internet is open before you set the site rules.
- For remote access management, separate the data networks from the voice networks.
- Ensure that your end-user mobile carrier supports propagation of incoming caller ID.
- To ensure that the Welcome/Deployment emails do not get rejected by the mailbox, you must include the * .mitel.io alias in the user's e-mail whitelist.

- Ensure that the user database in the MiVoice Office PBX is updated accurately and User Groups are labeled with informative names to enable importing contacts into CloudLink applications such as Mitel One.
- CloudLink solution supports the following emergency numbers: 000, 110, 111, 112, 118 119, 911, and 999, which are specific to each supported country. To ensure that there are no dialing conflicts, the administrator must configure these emergency numbers in MiVoice Office 400.
- To ensure optimal network efficiency with free flow of data using minimum network bandwidth, you must enable Bandwidth Optimization. For more information about how to enable Bandwidth Optimization, see *Account Information* in Mitel Administration documentation. To learn more about Bandwidth Optimization, see *System Requirements* in CloudLink Platform documentation.
- Ensure that you enter the IP Address or FQDN value that is displayed in the Network Element form. For more information about entering PBX information see, Enter PBX Information.
- It is strongly recommended not to deploy CloudLink directly on the Wide Area Network to ensure that the CloudLink solution is properly secured. See the following Mitel KMS articles related to Network Security and Toll Fraud prevention for the Mitel Office PBX installations:

  - Preventing Toll Fraud
  - Toll Fraud prevention on SIP trunks
  - General Guidelines to Secure SIP trunks for Toll Fraud prevention

For more information about configuring the firewall for CloudLink deployments, see Configuration Prerequisites on page 4.

Configuration Prerequisites 2

This chapter contains the following sections:

This chapter is intended to inform customer Administrators about the performance profile and network requirement prerequisites that must be ensured for the proper functioning of CloudLink enabled applications, services, and devices.

The information provided helps customer Administrators in choosing the level of restrictions to impose on the network equipment that they manage, based on the risk management capability they need to achieve.

Note:
Any use of third-party links is subject to the terms of service, terms of usage, and permission notices of the third-party content provider and is in no way intended to circumvent the site owner's navigational structure or attempt to obtain materials or information through means not purposely made available through the site(s).

2.1 Performance Profiles

Performance profiles are designed to allow the correct resource to best fit a solution for a customer's requirements.

Profiles are selected by the gateway platform based on the platform type, the number of CPUs/cores, and the amount of physical memory allocated. The call manager connected to the gateway has no influence on the selection of the performance profile.

Performance profiles have been defined by reflect the results of Mitel performance testing. Specific characteristics of the gateway depend on the connected call manager and other environmental factors.

All Platforms

For more information about the network requirements of performance profiles, see *CloudLink Gateway Performance Profile* section in CloudLink Gateway.

Rank	Profile	CPU/RAM	Sim. Calls (Mitel One)	Memory Cloud Link/FreeSWI TCH
25	Small	1 Core / 1 GiB	25	256 MiB / 512 MiB

Virtual Appliance

Note:
CloudLink Gateway VMware release v2.4.0-1821 and later requires a VMware environment with version 7.0 or later.

Rank	Profile	CPU/RAM	Sim. Calls (Mitel One)	Memory Cloud Link/FreeSWI TCH
28	Small Plus	2 cores / 2GiB	40	256MiB / 1 GiB
30	Medium	4 cores / 2GiB	30	256MiB / 512MiB
125	Large	8 cores / 4GiB	125	512MiB / 2GiB

Note:
The profile Small Plus is created based on performance tests with MiVoice Office 5000 in a KVM environment.

MSL (on SMBC MiVoice Business only)

Note:
The CloudLink gateway must have MSL 11.0 or later.

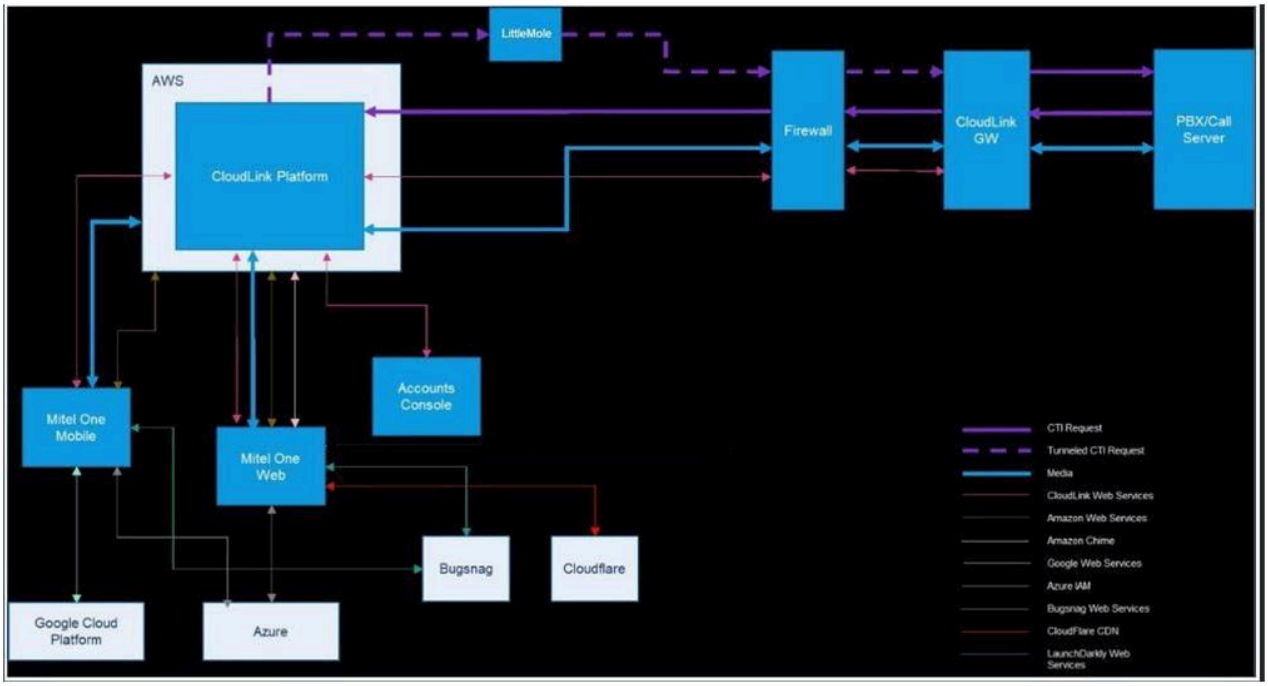
Rank	Profile	CPU/RAM	Sim.Calls (Mitel One)	Memory Cloud Link/FreeSWITCH
30	Medium	4 cores / 5GiB	30	1GiB / 512GiB
125	Large	8 cores / 5GiB	125	512MiB / 2GiB

Note:
FreeSWITCH on MSL is only available if a MiVoice Office 400 is installed on the same system.

2.2 Network View

The following diagram illustrates a top-level network view of the various network connections.

Note:
Mitel One and the Accounts Console might also reside in the corporate network behind the corporate firewall.



2.3 CloudLink Platform IP Address Ranges

The CloudLink Platform and many of the sub-service providers leverage the Amazon Web Services Platform for their infrastructure, Software as a Service, and Platform as a Service needs.

The IP address range required by the CloudLink Platform can be determined by using the IP address range of the AWS region with which your CloudLink account is registered along with the global IP range defined by AWS.

The following provides a list of AWS regions used by North America (NA), Europe, Middle East, Africa (EMEA) and Asia Pacific (APAC).

- **North America**
  - US East N. Virginia (us-east-1), and
  - US West Oregon (us-west-2)

- **Europe, Middle East, Africa**
  - Europe Frankfurt (eu-central-1), and
  - Europe Ireland (eu-west-1)
- **Asia Pacific**
  - Asia Pacific Sydney (ap-southeast-2)

For details, see AWS General Reference and select an IP address range that matches the AWS regions mentioned with the service name **AMAZON**. The AWS global range is defined by a service name **GLOBAL**.

For a global company with CloudLink accounts in multiple regions, Mitel recommends including all regions in your firewall rules to ensure proper communication between regional offices.

The CloudLink Platform relies on a Content Delivery Network (CDN) called Amazon CloudFront. Ensure that your IT infrastructure is enabled to support the CDN.

Examples of the IP address ranges which are expected can be found here.

2.4 Mitel Administration

The following table lists network connections for the Mitel Administration.

Note:

Examples of the IP address ranges which are expected can be found here.

Purpose	Direction	Protocol	Destination FQDN	Destination IP	Port
Managed Services provided by the CloudLink Platform including APIs, and portals.	App to Internet	TCP	*.mitel.io	See the CloudLink Platform IP Address Ranges section in this document.	443
Launch Darkly feature flag management	App to Internet	TCP	See Domain List.	See the Public IP List.	443

2.5 CloudLink Gateway

The following table lists the network connections from CloudLink Gateway to the external destination unless specified.The rules used for establishing the connections assume a firewall that permits return traffic on these established connections. This is referred to as pin hole punching. If pin hole punching is not available or has been disabled on the firewall, then you must exercise your own due diligence in configuring and testing the connections with the ports listed.

Note:

- ICMP must be enabled on the firewall.
- The CloudLink Gateway onboarding portal network configuration is different when embedded with an MBG.

  Examples of the IP address ranges which are expected can be found here.

Purpose	Direction	Protocol	Domain Name	IP Address Range	Ports
NTP Service	GW to Internet	UDP	*.mitel.pool.ntp.org	The public service assigns a random set of servers on an hourly basis. It is not possible to set an effective IP address range.	123
DNS Service	GW to Internet	UDP	N/A	DNS configured by the customer	53
Managed Services provided by the CloudLink Platform including LittleMole, APIs, and portals	GW to Internet	TCP	*.mitel.io mitel.io	See the CloudLink Platform IP Address Ranges section in this document.	443
STUN Service	GW to Internet	UDP	*.mitel.io	See the CloudLink Platform IP Address Ranges section in this document.	3478 and 3479

Purpose	Direction	Protocol	Domain Name	IP Address Range	Ports
SIP Connectivity	GW to Internet	TCP	*.mitel.io	See the CloudLink Platform IP Address Ranges section in this document.	5061
RTP/SRTP Connectivity for CloudLink Gateway Appliance and SMBC **Note**: See performance profile considerations in the following section for virtual and embedded variants.	GW to Internet	UDP	*.mitel.io	See the CloudLink Platform IP Address Ranges section in this document.	16384 to 49152 and 65336 to 65534
Required for CloudLink Single Sign-On deployment using Azure AD federation	User Browser to Internet	TCP	*.microsoftonline.com *.microsoft.com	The IP address range published by Microsoft is shown here: Office 365 URLs and IP address ranges - Microsoft 365 Enterprise See "ID 56" in the table of the given link.	443

Purpose	Direction	Protocol	Domain Name	IP Address Range	Ports
Gateway onboarding portal **Note**: This row is not applicable to an MBG scenario. See the MBG Considerations Section below for the necessary configuration.	User Browser to Gateway	TCP	Cloudlink.local	Local IP address of the gateway as configured on site.	80

Testing Network Connections

To help identify a network connection issues a test tool is included in the CloudLink Gateway

After the completion of onboarding process, if the CloudLink Gateway fails to connect to the required CloudLink services the installer is notified through the following channels:

- An email is sent to the **Support Contact(s)** listed in the account.
- An entry is created in the **Support Logs** page of the Mitel Administration portal.
- The local web page of the CloudLink Gateway.

The gateway type determines how those tests are run and where the results are displayed.

The following table can be used to identify how to run the test and see the results.

Gateway Type	Initiate Test	Output Displayed
MSL	Click the **Run Diagnostics** button located in the CloudLink Gateway page in MSL.	Issues displayed in the diagnostics section located in the CloudLink Gateway page in MSL.

Gateway Type	Initiate Test	Output Displayed
Appliance and Virtual	Diagnostic test runs during the startup of the CloudLink Gateway.	Issues displayed in the system monitor (Physical CloudLink Gateway Appliance requires a Monitor, Virtual CloudLink Gateway displays via the hosts Virtual Console).
SMBC	Diagnostic test runs during the startup of the CloudLink Gateway.	Issues displayed as a system alarm.

Note:
The failed test cases are written in the CloudLink Gateway logs, see file **clgw.log file**. This can be located in CloudLink Gateway log file **<File name.tar.gz> \log\hostlog\log\clgw\clgw.log**.

2.5.1 MBG Considerations

Mitel Administration is accessed differently when embedded within an MBG server.

The following table provides the required details:

Purpose	Direction	Protocol	Domain Name	IP Address Range	Ports
Gateway onboarding portal	User Browser to Gateway	TCP	Domain Name of MBG Server	Local IP address of the gateway as configured on site	80
Gateway onboarding portal from MBG	User Browser to Gateway	TCP	GW IP address	Local IP address of the gateway as configured on site	8287

2.5.2 CloudLink Gateway Performance Profiles

The following tables provide information about the performance profiles of CloudLink Gateway.

For information about hardware requirements related to performance profiles, see Performance Profiles.

Profile	Platform	Purpose	Direction	Protocol	Domain Name	IP Address Range	Ports
Small	CloudLink Gateway Appliance, SMBC, Virtual, MiVoice 5000, and MSL	RTP/SRTP	GW to Internet	UDP	*.mitel.io	See the CloudLink Platform IP Address Ranges section in this document.	16384 to 49152 and 65336 to 65534
Small-Plus	Virtual, MiVoice 5000	RTP/SRTP	GW to Internet	UDP	*.mitel.io	See the CloudLink Platform IP Address Ranges section in this document.	16384 to 49152 and 65198 to 65534
Medium	Virtual, MSL	RTP/SRTP	GW to Internet	UDP	*.mitel.io	See the CloudLink Platform IP Address Ranges section in this document.	16384 to 49152 and 65296 to 65534
Large	Virtual, MSL	RTP/SRTP	GW to Internet	UDP	*.mitel.io	See the CloudLink Platform IP Address Ranges section in this document.	16384 to 49152 and 61536 to 65534

2.6 Connections Between the CloudLink GW and PBX/Call Server

This section provides details of network connections required between CloudLink Gateway and the respective PBXs.

You must ensure that the ports on the Call Server or PBX are reserved for operational use for the CloudLink Gateway and that the connections are routed properly through the corporate network.

When deploying the CloudLink Gateway the hosts IP Address(s) must be added to the trusted network of each PBX node if they are deployed using MSL.

Note:
Examples of the IP address ranges which are expected can be found here.

2.6.1 MiVoice Business Considerations

The following table summarizes the connection details of CloudLink Gateway with MiVoice Business.

Purpose	Direction	Protocol	Domain Name	IP Address Range	Ports
SIP (Trunk from PBX to GW)	PBX to GW	TCP/UDP	cloudlink.local	Local IP address of the gateway as configured on site	5060
SIP (TLS Trunk from PBX to GW)	PBX to GW	TCP	cloudlink.local	Local IP address of the gateway as configured on site.	5061
SIP (Subscriber Side)	GW to PBX	TCP/UDP	Local domain name of the PBX as configured on site.	Local IP address of the PBX as configured on site.	5070
SIP (Subscriber Side TLS)	PBX to GW	TCP	cloudlink.local	Local IP address of the gateway as configured on site.	5071

Purpose	Direction	Protocol	Domain Name	IP Address Range	Ports
MiVB GDS for user config	GW to PBX	TCP	Local domain name of the PBX as configured on site.	Local IP address of the PBX as configured on site.	7011
SIPS (GW to Cloud TLS Trunk)	GW to Cloud	TCP	*.mitel.io	See the CloudLink Platform IP Address Ranges section in this document.	5061
SIP (Trunk from PBX to GW for SMBC only)	PBX to GW	TCP/UDP	cloudlink.local	Local IP address of the gateway as configured on site.	19060
SIP (LS Trunk using TLS to GW for SMBC only)	PBX to GW	TCP	cloudlink.local	Local IP address of the gateway as configured on site.	19061
CTI Q2K Driver	GW to PBX	TCP	Local domain name of the PBX as configured on site.	Local IP address of the PBX as configured on site.	5320

Note:

Ensure that all the required servers (such as MBG, MiCollab, etc.) are added as trusted networks in MSL.

2.6.2 MiVoice Office 400 Considerations

The following table summarizes the connection details of CloudLink Gateway with MiVoice Office 400.

Purpose	Direction	Protocol	Domain Name	IP Address Range	Ports
SIP (Trunk from PBX to GW)	PBX to GW	TCP/UDP	cloudlink.local	Local IP address of the gateway as configured on site.	5060
SIP (TLS Trunk from PBX to GW)	PBX to GW	TCP	cloudlink.local	Local IP address of the gateway as configured on site.	5061
SIP (Subscriber Side)	GW to PBX	TCP/UDP	Local domain name of the PBX as configured on site	Local IP address of the gateway as configured on site.	5060
SIP (Subscriber Side)	GW to PBX	TCP	Local domain name of the PBX as configured on site	Local IP address of the gateway as configured on site.	5061
SIP (Subscriber Side)	PBX to GW	TCP/UDP	Local domain name of the PBX as configured on site.	Local IP address of the PBX as configured on site.	5070
SIP (Subscriber Side TLS)	PBX to GW	TCP	cloudlink.local	Local IP address of the gateway as configured on site.	5071
CTI Port	GW to PBX	TCP	Local domain name of the PBX as configured on site.	Local IP address of the PBX as configured on site.	7001 (default)
SIPS (GW to Cloud TLS Trunk)	GW to Cloud	TCP	*.mitel.io	See the CloudLink Platform IP Address Ranges section in this document.	5061
SIP (Trunk from PBX to GW for SMBC only)	PBX to GW	TCP/UDP	cloudlink.local	Local IP address of the gateway as configured on site.	19060

Purpose	Direction	Protocol	Domain Name	IP Address Range	Ports
SIP (LS Trunk using TLS to GW for SMBC only)	PBX to GW	TCP	cloudlink.local	Local IP address of the gateway as configured on site.	19061
Webhook for MiVO400 user config	PBX to GW	TCP	cloudlink.local	Local IP address of the gateway as configured on site.	8086

2.6.3 MiVoice MX-ONE Considerations

The following table summarizes the connection details of CloudLink Gateway with MiVoice MX-ONE.

Purpose	Direction	Protocol	Domain Name	IP Address Range	Ports
SIP (Trunk from PBX to GW)	PBX to GW	TCP/UDP	cloudlink.local	Local IP address of the gateway as configured on site.	5060
SIP (TLS Trunk from PBX to GW)	PBX to GW	TCP	cloudlink.local	Local IP address of the gateway as configured on site.	5061
SIP (Subscriber Side)	GW to PBX	TCP/UDP	Local domain name of the PBX as configured on site.	Local IP address of the PBX as configured on site.	5070
SIP (Subscriber Side TLS)	PBX to GW	TCP	cloudlink.local	Local IP address of the gateway as configured on site.	5071
CTI Port	GW to PBX	TCP	Local domain name of the PBX as configured on site.	Local IP address of the PBX as configured on site.	8882

Purpose	Direction	Protocol	Domain Name	IP Address Range	Ports
SIPS (GW to Cloud TLS Trunk)	GW to Cloud	TCP	*.mitel.io	See the CloudLink Platform IP Address Ranges section in this document.	5061
SIP (Trunk from PBX to GW for SMBC only)	PBX to GW	TCP/UDP	cloudlink.local	Local IP address of the gateway as configured on site.	19060
SIP (LS Trunk using TLS to GW for SMBC only)	PBX to GW	TCP	cloudlink.local	Local IP address of the gateway as configured on site.	19061
PBX user config	PBX to GW	TCP	cloudlink.local	Local IP address of the gateway as configured in site .	8086

2.6.4 MiVoice 5000 Considerations

The following table summarizes the connection details of CloudLink Gateway with MiVoice 5000.

Purpose	Direction	Protocol	Domain Name	IP Address Range	Ports
SIP (Trunk from PBX to GW)	PBX to GW	TCP/UDP	cloudlink.local	Local IP address of the gateway as configured on site.	5060
SIP (TLS Trunk from PBX to GW)	PBX to GW	TCP	cloudlink.local	Local IP address of the gateway as configured on site.	5061
SIP (Subscriber Side)	GW to PBX	TCP/UDP	Local domain name of the PBX as configured on site.	Local IP address of the PBX as configured on site.	5070

Purpose	Direction	Protocol	Domain Name	IP Address Range	Ports
SIP (Subscriber Side TLS)	PBX to GW	TCP	cloudlink.local	Local IP address of the gateway as configured on site.	5071
CTI Port	GW to PBX	TCP	Local domain name of the PBX as configured on site	Local IP address of the PBX as configured on site.	3211
SIPS (GW to Cloud TLS Trunk)	GW to Cloud	TCP	*.mitel.io	See the CloudLink Platform IP Address Ranges section in this document.	5061
SIP (Trunk from PBX to GW for SMBC only)	PBX to GW	TCP/UDP	cloudlink.local	Local IP address of the gateway as configured on site.	19060
SIP (LS Trunk using TLS to GW for SMBC only)	PBX to GW	TCP	cloudlink.local	Local IP address of the gateway as configured on site.	19061
PBX user config	PBX to GW	TCP	cloudlink.local	Local IP address of the gateway as configured on site.	8086

2.7 Mitel One Web

The following table lists the connections from Mitel One to the external destination unless specified.
The rules used for establishing the connections assume a firewall that permits return traffic on these established connections. This is referred to as pin hole punching. If pin hole punching is not available or has been disabled on the firewall, then you must exercise your own due diligence in configuring and testing the connections with the ports listed.

Note:

- The port requirements for WebSockets are given here: Device communication protocols - AWS IoT Core.
- If you are using a proxy server, ensure that it proxies WebSockets and HTTPS.
- The Mitel One web application uses WebRTC. By default, the CS0 value is set to the same as the DSCO value.
- Check using Amazon Chime Readiness Checker whether your firewall rules require updating for AWS Chime support.
- For more information about VPN recommendations and network requirements, see Network Handling and Requirements.
- For AWS Chime rules, see Hosts, Ports and Protocols needed for Amazon Chime services - Amazon Chime Help Center. The CloudLink Platform IP address ranges in AWS will cover the AWS IP address ranges mentioned in the document link. For details, see the **CloudLink Platform IP Ranges** section in this document. In addition, the **highlighted feature** used is **Amazon Chime Meetings, Chat, and Business Calling**.
- ICMP must be enabled on the firewall.
- Source port numbers are typically managed by the network stack.
- For more details about the media flow, see CloudLink Platform.
- * The RTP/RTCP source port range for the softphone is automatically selected by WebRTC or the OS, respectively. There are no restrictions on the port range.

  Examples of the IP address ranges which are expected can be found here.

Purpose	Direction	Protocol	Domain Name	IP Address Range	Ports
Managed Services provided by the CloudLink Platform including APIs and portals	App to Internet	TCP	*.mitel.io	See the CloudLink Platform IP Address Ranges section in this document.	443
STUN Service	App to Internet	UDP	*.mitel.io	See the CloudLink Platform IP Address Ranges section in this document.	3478 and 3479
DNS Service	GW to Internet	UDP	N/A	Customer's configured DNS	53

Purpose	Direction	Protocol	Domain Name	IP Address Range	Ports
WebRTC Connectivity *	App to Internet	TCP	*.mitel.io	See the CloudLink Platform IP Address Ranges section in this document.	7443
RTP/SRTP Connectivity	App to Internet	UDP	*.mitel.io	See the CloudLink Platform IP Address Ranges section in this document.	16384 to 49152
WebSocket Connectivity	App to Internet	TCP	*.amazonaws.com	See the CloudLink Platform IP Address Ranges section in this document.	See note on **WebSocket** above
Meet Capability	App to Internet	TCP and UDP	See note on AWS Chime above	See note on **AWS Chime** above	See note on **AWS Chime** above
Google Cloud Resources	App to Internet	TCP	*.gstatic.com *.googleapis.com	Google IP address ranges can be found here: Obtain Google IP address ranges - Google Workspace Admin Help (See "IP ranges that Google makes available to users on the internet" in the given link.)	443

Purpose	Direction	Protocol	Domain Name	IP Address Range	Ports
cdnjs open-source content delivery network hosed on Cloudflare	App to Internet	TCP	cdnjs.cloudflare.com	See IP Ranges Cloudflare	443
Required for CloudLink Single Sign-On deployment using Azure AD federation	App to Internet	TCP	*.microsoftonline.com *.microsoft.com	The IP address range published by Microsoft is shown here: Office 365 URLs and IP address ranges - Microsoft 365 Enterprise . See "ID 56" in the table of the given link.	443
Bugsnag Troubleshooting service	App to Internet	TCP	See BugSnag firewall rules	See BugSnag firewall rules	443

2.8 Mitel One Mobile

The following table lists the connections from Mitel One to the external destination unless specified. The rules used for establishing the connections assume the firewall that permits return traffic on these established connections. This is referred to as pin hole punching. If pin hole punching is not available or has been disabled on the firewall, then you must exercise your own due diligence in configuring and testing the connections with the ports listed.

Note:

- The port requirements for WebSockets are given here: Device communication protocols - AWS IoT Core.
- If you are using a proxy server, ensure that it proxies WebSockets and HTTPS.
- For more information about the ports and hosts used for Apple Push Notification service (APNs), see Apple documentation (If your Apple devices aren't getting Apple push notifications).
- For more information about configuring your firewall to connect a device with Firebase Cloud Messaging (FCM), see Firebase Cloud Messaging.
- For more information about VPN recommendations and network requirements, see Mitel One Mobile Application User Guide.
- ICMP must be enabled on the firewall.
- Source port numbers are typically managed by the network stack.
- For details about the media flow, see CloudLink Platform.
- * The RTP/RTCP source port range for the softphone is automatically selected by WebRTC or the OS, respectively. There are no restrictions on the port range.

  Examples of the IP address ranges which are expected can be found here.

Purpose	Direction	Protocol	Destination FQDN	Destination IP	Port
Managed Services provided by the CloudLink Platform including APIs, and portals	App to Internet	TCP	*.mitel.io	See the CloudLink Platform IP Address Ranges section in this document.	443
STUN Service	App to Internet	UDP	*.mitel.io	See the CloudLink Platform IP Address Ranges section in this document.	3478 and 3479
DNS Service	GW to Internet	UDP	N/A	Customer's configured DNS	53
SIP Connectivity	App to Internet	TCP	*.mitel.io	See the CloudLink Platform IP Address Ranges section in this document.	5061

Purpose	Direction	Protocol	Destination FQDN	Destination IP	Port
WebRTC Connectivity*	App to Internet	TCP	*.mitel.io	See the CloudLink Platform IP Address Ranges section in this document.	7443
RTP/SRTP Connectivity	App to Internet	UDP	*.mitel.io	See the CloudLink Platform IP Address Ranges section in this document.	16384 to 49152
WebSocket Connectivity	App to Internet	TCP	*.amazonaws.com	See the CloudLink Platform IP Address Ranges section in this document.	See note on **WebSocket** above
Google Cloud Resources	App to Internet	TCP	*.gstatic.com *.googleapis.com	Google IP address ranges can be found here: Obtain Google IP address ranges - Google Workspace Admin Help (See "IP ranges that Google makes available to users on the internet" in the given link.)	443

Purpose	Direction	Protocol	Destination FQDN	Destination IP	Port
Required for CloudLink Single Sign-On deployment using Azure AD federation	App to Internet	TCP	*.microsoftonline.com *.microsoft.com	The IP address range published by Microsoft is shown here: Office 365 URLs and IP address ranges - Microsoft 365 Enterprise See "ID 56" in the table of the given link.	443
Bugsnag Troubleshooting service	App to Internet	TCP	See BugSnag firewall rules	See BugSnag firewall rules	443

2.9 CloudLink Chat Integration

This section provides details on firewall requirements for Mitel products that integrate CloudLink Chat into their solution. The details include conversations, notifications, presence, and SSO.

The following table lists the connections from the Mitel product to the external destination unless specified. The rules used for establishing the connections assume a firewall that permits return traffic on these established connections. This is referred to as pin hole punching. If pin hole punching is not available or has been disabled on the firewall, then you must exercise your own due diligence in configuring and testing the connections with the ports listed.

Note:

- The port requirements for WebSockets are given here: Device communication protocols - AWS IoT Core.
- For Mobile deployments, the Chat Service leverages push notifications:
  - For more information about the ports and hosts used for Apple Push Notification service (APNs), see Apple documentation (If your Apple devices aren't getting Apple push notifications).
  - For more information about configuring your firewall to connect a device with Firebase Cloud Messaging (FCM), see Firebase Cloud Messaging.

    Examples of the IP address ranges which are expected can be found here.

Purpose	Direction	Protocol	Destination FQDN	Destination IP	Destination Port
Managed Services provided by the CloudLink Platform including APIs, and portals	Server to Internet	TCP	*.mitel.io	See the CloudLink Platform IP Address Ranges section in this document.	443
DNS Service	GW to Internet	UDP	N/A	Customer's configured DNS	53
WebSocket Connectivity	Server to Internet	TCP	*.amazonaws.com	See the CloudLink Platform IP Address Ranges section in this document.	See note on **WebSocket** above
Required for CloudLink Single Sign-On deployment using Azure AD federation	Server to Internet	TCP	*.microsoftonline.com *.microsoft.com	The IP address range published by Microsoft is shown here: Office 365 URLs and IP address ranges - Microsoft 365 Enterprise See "ID 56" in the table of the given link.	443

2.10 Mitel Assistant

For Call History Subscription, Mitel Assistant, like the Mitel One web application, uses a WebSocket.

Note:

- The port requirements for WebSockets are given here: Device communication protocols - AWS IoT Core.
- If you are using a proxy server, ensure that it proxies WebSockets and HTTPS.

  Examples of the IP address ranges which are expected can be found here.

Purpose	Direction	Protocol	Domain Name	IP Address Range	Ports
Managed Services provided by the CloudLink Platform including APIs, and portals	App to Internet	TCP	*.mitel.io	See the CloudLink Platform IP Address Ranges section in this document.	443
DNS Service	GW to Internet	UDP	N/A	Customer's configured DNS	53
WebSocket Connectivity	App to Internet	TCP	*.amazonaws.com	See the CloudLink Platform IP Address Ranges section in this document.	See note on **WebSocket** above
Microsoft Azure AD APIs	App to Internet	TCP	graph.microsoft.com	The IP address range published by Microsoft is shown here: Office 365 URLs and IP address ranges - Microsoft 365 Enterprise The entry of interest the row with ID 56 in the table.	443

2.11 MiTeam Meetings

The following table lists the connections from MiTeam Meetings to the external destination unless specified. The rules used for establishing the connections assume a firewall that permits return traffic on these established connections. This is referred to as pin hole punching. If pin hole punching is not available or has been disabled on the firewall, then you must exercise your own due diligence in configuring and testing the connections with the ports listed.

Note:

- The port requirements for WebSockets are given here: Device communication protocols - AWS IoT Core.
- If you are using a proxy server, ensure that it proxies WebSockets and HTTPS.
- Check using Amazon Chime Readiness Checker whether your firewall rules require updating for AWS Chime support.
- For more information about VPN recommendations and network requirements, see Network Handling and Requirements.
- For AWS Chime rules, see Hosts, Ports and Protocols needed for Amazon Chime services - Amazon Chime Help Center. The CloudLink Platform IP address ranges in AWS will cover the AWS IP address ranges mentioned in the document link. For details, see the **CloudLink Platform IP Ranges** section in this document. In addition, the **highlighted feature** used is **Amazon Chime Meetings, Chat, and Business Calling**.
- ICMP must be enabled on the firewall.

Purpose	Direction	Protocol	Domain Name	IP Address Range	Ports
Managed Services provided by the CloudLink Platform including APIs and portals	App to Internet	TCP	*.mitel.io	See the CloudLink Platform IP Address Ranges section in this document.	443
DNS Service	GW to Internet	UDP	N/A	Customer's configured DNS	53

Purpose	Direction	Protocol	Domain Name	IP Address Range	Ports
WebSocket Connectivity	App to Internet	TCP	*.amazonaws.com	See the CloudLink Platform IP Address Ranges section in this document.	See note on **WebSocket** above
Meet Capability	App to Internet	TCP and UDP	See note on **AWS Chime** above	See note on **AWS Chime** above	See note on **AWS Chime** above
Google Cloud Resources	App to Internet	TCP	*.gstatic.com *.googleapis.com	Google IP address ranges can be found here: Obtain Google IP address ranges - Google Workspace Admin Help (See "IP ranges that Google makes available to users on the internet" in the given link.)	443
Required for CloudLink Single Sign-On deployment using Azure AD federation	App to Internet	TCP	*.microsoftonline.com *.microsoft.com	The IP address range published by Microsoft is shown here: Office 365 URLs and IP address ranges - Microsoft 365 Enterprise . See "ID 56" in the table of the given link.	443

Purpose	Direction	Protocol	Domain Name	IP Address Range	Ports
Bugsnag Troubleshooting service	App to Internet	TCP	See BugSnag firewall rules	See BugSnag firewall rules	443

Install and Access the CloudLink Gateway

3

This chapter contains the following sections:

The CloudLink Gateway appliance has the following characteristics:

- For standalone platforms, the CloudLink Gateway can be deployed as:
  - an external device installed on premise to provide a connection from the PBX to the CloudLink platform.
  - a virtual instance of CloudLink Gateway installed in the VMware vCenter server. For more information see, Install the CloudLink Gateway in a VMware Virtual Environment on page 39.
  - a blade on the virtual instance of MSL in VMware or Hyper-V environments with MiVoice Office 400 already installed. For more information see, Configure MiVoice Office 400 on Virtual Appliance on page 100.
- For SMBC platforms, it is installed as a software package on the same SMBC hardware.
- CloudLink Platform is integrated as a virtual instance using a KVM image on both EX Controller and Compact Server (for MiVoice Office 5000).

See the topics listed below to learn how to install and access the CloudLink Gateway.

- Install the CloudLink Gateway Appliance on page 31
- Gateway Appliance Software Update on page 33
- Access the CloudLink Gateway on page 35
- Install the CloudLink Gateway in a VMware Virtual Environment on page 39

3.1 Install the CloudLink Gateway Appliance

The CloudLink Gateway appliance, which connects your PBX to the Mitel CloudLink platform, should be connected to a DHCP-enabled LAN.

Prerequisites

This CloudLink Gateway requires the following:

- An

  connection that provides sufficient bandwidth.
- A DNS server that the Gateway uses to resolve domain names.
- A DHCP server to assign an IP address to the Gateway (not mandatory in VMware environments).
- An Ethernet connection to the LAN.
- For more information about specific network configuration see, CloudLink Gateway.

Assigning an IP Address

When the Gateway is powered up, it will acquire an IP Address from a DHCP Server on the LAN

The PBX needs to be programmed with the IP address of the CloudLink Gateway. This means a fixed IP address must be allocated to the Gateway.

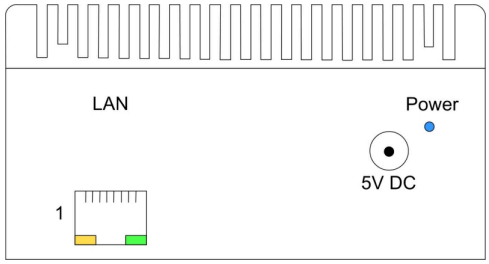
There are several different ways you can do this:

- Configure a static IP address (recommended). See Configure the Customer Site for related information.
- Configure your DHCP server to reserve an IP address for the CloudLink Gateway appliance.
- Your DHCP server may automatically reallocate the same IP address to the CloudLink Gateway appliance.

Consult your DHCP server documentation to learn more about the server's IP address allocation scheme

Connecting the Appliance

1. Connect the CloudLink Gateway to the LAN using port 1.



2. Apply power.
3. The CloudLink Gateway automatically accesses the Internet to download and install any Software Updates. To learn more, see the Gateway Appliance Software Update topic.

Warning:

If you have a Check Point "Security Gateway" firewall, unless special configuration steps are taken, the CloudLink Gateway and client cannot register SIP TLS (Transport Layer Security) through the firewall. To resolve this, the person in your organization who manages the Check Point firewall should review the following two Check Point issues:

- sip_tls_authentication Service does not traverse the Security Gateway
- Unable to connect to Skype application using port 5061 with pre-defined TCP service

3.2 Gateway Appliance Software Update

Mitel recommends that you enable and schedule automatic updates for the Gateway appliance in the CloudLink Gateway Portal. To learn more, see Configure Advanced Settings and Options.

If you access the Gateway appliance while it is performing a software update, the progress status is displayed. If the software update fails, you will be provided with recovery options.

The Gateway appliance checks for, downloads, and installs software updates from Mitel whenever it is powered on or an automatic update is scheduled. Software updates vary in size and can be as large as 500-700 MB.

Downloading and installing software updates typically takes about 10 to 15 minutes. The actual time that it takes to download the updates depends on your Internet connection speed.

Note:
CloudLink Gateway is built on the CentOS operating system. The OS level updates come from CentOS community update servers.

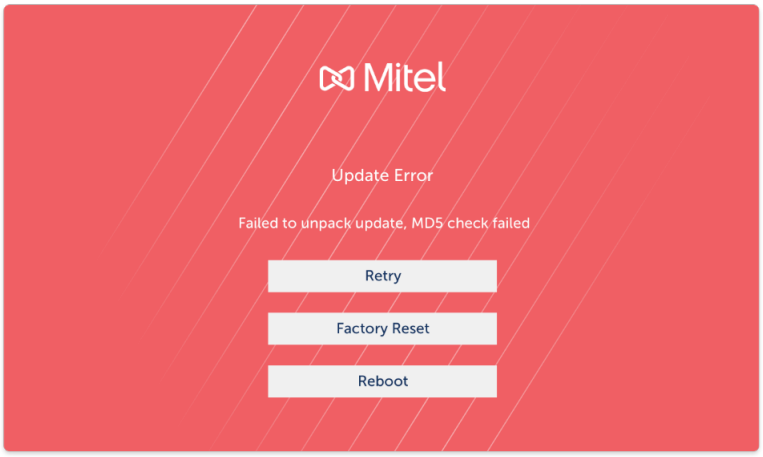
Warning:
If you have a standalone platform with external Gateway, do NOT disconnect power or the LAN cable until the update process has completed or within 15 minutes of powering up the Gateway. Powering down or disconnecting the Gateway from the network in the middle of an update can cause the update to fail and the Gateway to not boot up properly.

Whenever the Gateway appliance is rebooted or restarted, you may see a brief display of a **Lost trunk connection to PBX** message. This temporary issue should resolve itself.

When you connect your browser to the Gateway appliance, if the Gateway is still downloading updates, you may see the **System update in progress** screen as shown below.

If your browser loses connection to the Gateway during the update, you may see the **Lost Connection to Gateway** screen as shown below:

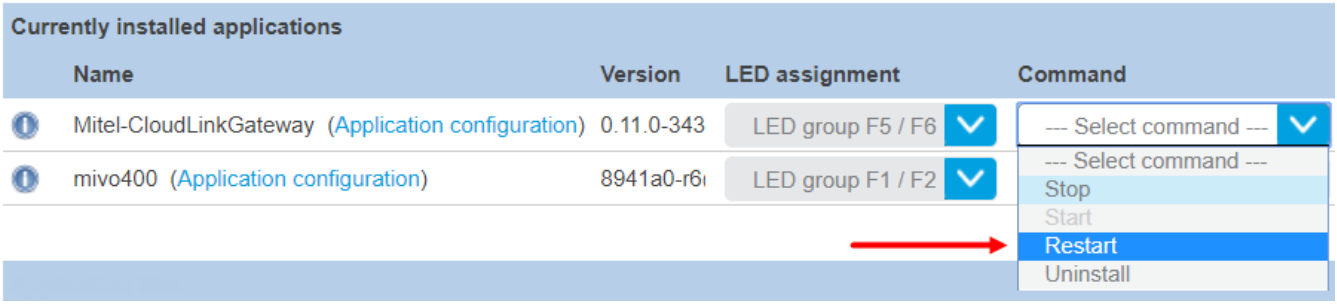
If there is an error while downloading the update, you may see an **Update Error** screen as shown below.



If you have a **standalone** platform with external Gateway and there are downloading errors, you can take appropriate action as explained below:

- **Retry** should be attempted if the error message indicates a connection failure or a problem that you have the ability to resolve. For example, if there is a firewall configuration error, you should use the Retry option after resolving the error.
- **Reboot** should be attempted if retry fails to resolve the problem.
- **Factory Reset** can be attempted if you suspect the Gateway received a bad update from Mitel or you received guidance from Mitel Support to do a Factory Reset.

If you have an **SMBC** platform with embedded Gateway and there are downloading errors, an administrator can apply the **Restart** command to the Mitel-CloudLink Gateway in the **Software** > **Applications** screen of the SMB Controller Manager admin console as shown below.



If these errors persist, contact Mitel Partner Technical Support via a login at https://www.mitel.com/en-ca/login.

3.3 Access the CloudLink Gateway

To properly associate a Gateway with a new customer account on the CloudLink platform, the CloudLink Gateway Portal must be accessed the first time as indicated below.

- For **standalone** platforms, which have an external Gateway, the Portal must be accessed the first time by connecting to the Gateway from the same LAN subnet.
  - Details are in the Portal Access for Standalone Platforms section of this topic.
- For **SMBC** platforms, which have an embedded Gateway, the Portal must be accessed the first time from the SMB Controller Manager.
  - Details are in the Portal Access for SMBC Platforms section of this topic.

After a customer has been associated with a Gateway, you can access the CloudLink Gateway Portal to manage customers in the following different ways:

- By connecting from the same LAN subnet to the Gateway at http://cloudlink.local/ (for standalone platforms only)
- By accessing the Application configuration link in the SMB Controller Manager (for SMBC platforms only)
- By accessing Mitel MiAccess at https://connect.mitel.com/

- By accessing the Gateway Portal directly at https://mitel.io/cloudlink/gateway

Note: Internet Explorer (IE) does not properly display pages in the CloudLink Gateway Portal.

3.3.1 Update Progress

When you connect your browser to the Gateway appliance, if the Gateway is still downloading updates, a 'system update in progress' message is displayed.

If your browser loses connection to the Gateway during an update, a 'Lost Connection to Gateway' message is displayed.

If there is an error while downloading the update, an 'Update Error' message is displayed.

If your Gateway is rebooted, you may see a brief display of a 'Lost trunk connection to PBX' message.

For more detailed information, see the Gateway Appliance Software Update topic.

3.3.2 CloudLink Policy

To enable personnel to log into the CloudLink Gateway Portal via Mitel MiAccess, the CloudLink policy must be assigned to individual users (or as part of a bundle) by a Partner Administrator through the Mitel MiAccess user management portal. Please refer to the MiAccess Admin manual for additional information.

3.3.3 Portal Access for Standalone Platforms

3.3.3.1 Associate Gateway with a Customer by Connecting to Gateway

To associate an external Gateway with a customer account in the CloudLink platform, the CloudLink Gateway Portal should be accessed by connecting a supported browser to the Gateway at http://cloudlink.local/ or by entering the IP address of the gateway appliance in the browser. This needs to be done from a computing device located on the same LAN subnet as the CloudLink Gateway Portal. Unless the Gateway is currently being updated, the browser redirects to the CloudLink Gateway Portal login page. In the login page, click the **MiAccess** button. In the Mitel MiAccess login page that appears, enter your MiAccess credentials and click the **Login** button. After a successful login, your name and avatar are displayed in the upper-right corner of the interface.

Note:

The first time you connect to the Gateway (from the same LAN subnet), type the http:// prefix explicitly in the browser's address bar as shown below:

http://cloudlink.local or http://ip.address.of.gateway

This is an important step that only needs to be done once. A browser normally stores this information to make future connections to the Gateway.

You can use Apple Bonjour software to locate the Gateway when you connect from the LAN. Apple Bonjour software, which is compatible with the CloudLink Gateway, is a zero-configuration networking technology that locates devices such as printers and other computers, and the services that those devices provide on a local network subnet. You can download and install Apple Bonjour Print Services for Windows at https://support.apple.com/kb/dl999?locale=en_US.

3.3.4 Portal Access for SMBC Platforms

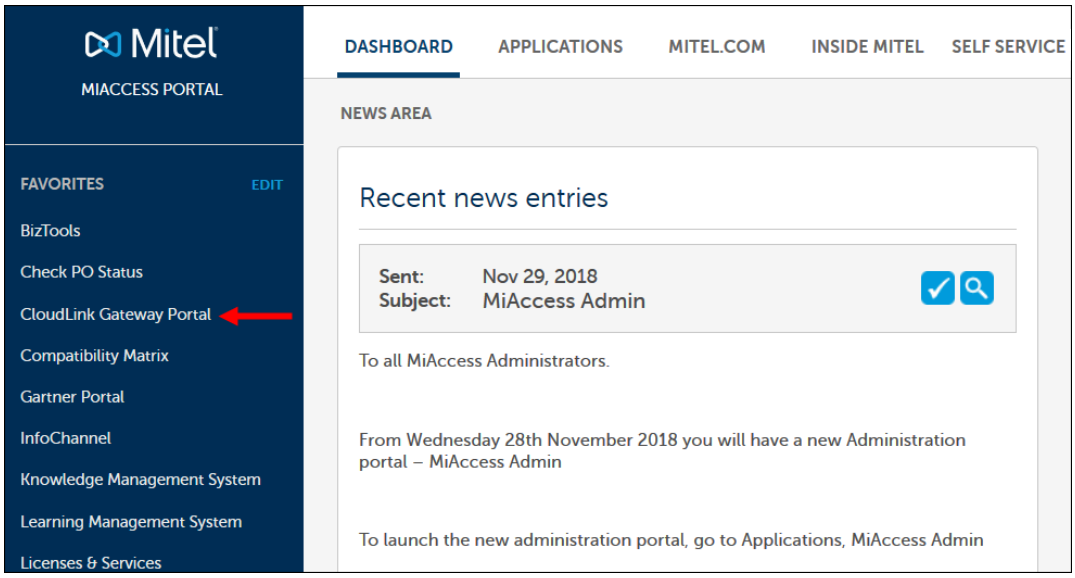
Associating an embedded Gateway with a new customer account on the CloudLink platform must be done via the SMB Controller Manager. For instructions, see the Access Application Configuration Link section of the Configure MiVO400 on SMBC Platform topic.

3.3.5 Portal Access for All Platforms

The following two additional ways to access the CloudLink Gateway Portal apply to both standalone platforms (with external Gateway) and SMBC platforms (with embedded Gateway).

3.3.5.1 Access the CloudLink Gateway Portal via Mitel MiAccess Portal

To perform maintenance on a customer account already associated with a Gateway, access the CloudLink Gateway Portal by logging in to the Mitel MiAccess Portal using your MiAccess credentials. In the **MiAccess Portal** home page, **CloudLink Gateway Portal** will be listed on the left side of the site, if the CloudLink policy has been assigned to you. Click **CloudLink Gateway Portal**. The Gateway Portal opens and the Partner Dashboard is displayed.



3.3.5.2 Access the CloudLink Gateway Portal via Direct Access

A Mitel Partner or an administrative user of a customer account can access the CloudLink Gateway Portal directly at http://gateway.mitel.io/.

For information about logging in to the Gateway portal directly, see Log in to CloudLink Gateway Portal.

3.4 Install the CloudLink Gateway in a VMware Virtual Environment

This topic describes the equipment, network, and configuration considerations that apply when setting up CloudLink Gateway on servers enabled with VMware® vSphere™ virtualization.

.

3.4.1 System Requirements

For information about VMware requirements see, Performance Profiles.

Note:

- You must have VMware vCenter server installed in your machine to change the network configuration of the gateway during the deployment.
- The CloudLink appliance and the MiVoice Office PBX must be installed on the same virtual environment / LAN subnet. If this is not done, disable all SIP ALG functions in the firewall to enable communication between these two components. Additionally, ensure that port blocking is disabled.
- CloudLink Gateway does not support virtualization features related to application migrations, for example vMotion.

3.4.2 Assigning IP Address

During the virtual deployment of CloudLink Gateway, the system assigns the initial IP address through Dynamic Host Configuration Protocol (DHCP). Alternately, the user can configure the initial IP address during the Open Virtualization Application (OVA) deployment using the portal. The console displays the network address after the deployment.

3.4.3 Deployment

You can deploy CloudLink Gateway in a VMware environment in any of the following ways:

3.4.3.1 Deploy using VMware vSphere/vCenter

The following are the high-level steps to deploy CloudLink Gateway OVA using the VMware vSphere Client to an ESXi host via vCenter Manager.

1. Log in to the VMware vSphere Client with your username and password.
2. From the vSphere Client Menu Bar, choose **File** > **Deploy OVF Template**.

3. In the OVA Wizard, select the Source of the OVF template file (OVA file extension)

    a. URL

        i. If the OVF template file is on the Internet or accessible through a web browser; enter the URL of the location of the file.

    b. Local File

        i. If the OVF template file was downloaded to the local computer or to a network share drive, click **Browse** to locate the file.

4. Click **Next**.
5. Under **Name** and **Inventory Location**, specify the name for the virtual machine and click **Next**.
6. Under **Deployment Configuration**, select the desired hardware configuration profile from the drop-down menu.
7. Click **Next**.
8. Under **Storage**, select the **Datastore** to use for the virtual machine. Click **Next**.
9. Set the virtual disk format to **Thick Provisioned**.
10. Under Network Mapping, allocate one virtual network interface card (vNIC) on the destination network using the drop-down list. The options for mapping the vNICs differ depending on the release version.
11. Configure the properties for the virtual machine.
12. Select **Power** on after deployment to automatically power on the virtual machine.
13. Click **Finish** to deploy the OVA.

3.4.3.2 Deploy using VMware Open Virtualization Format Tool

Alternately, use the command ovftoolto deploy CloudLink Gateway in a VMware environment through the VMware Open Virtualization Format Tool. The configuration parameters such as static IP address, user name, and password can be specified when deploying the OVA package to an ESXi host.

The following is an example of how to deploy CloudLink Gateway in a VMware environment using the command.

```
# target host
# (replace values as needed for your environment)
ESXI_DATASTORE=datastore1
ESXI_USERNAME=root
ESXI_PASSWORD=password
ESXI_HOST=198.51.100.10
# network settings for virtual CloudLink Gateway
# (replace values as needed for your environment)
DEPLOYMENT_IP=198.51.100.20
DEPLOYMENT_NETMASK=24
DEPLOYMENT_GATEWAY=198.51.100.1
DEPLOYMENT_DNS=198.51.100.1
DEPLOYMENT_HOST_NAME=cloudlink.domain.com

ovftool \
    --acceptAllEulas \
    --disableVerification \
```

```
    --noSSLVerify \
    --skipManifestCheck \
    --X:injectOvfEnv \
    --powerOn \
    --prop:cl.hostname=${DEPLOYMENT_HOST_NAME} \
    --prop:cl.ip0=${DEPLOYMENT_IP} \
    --prop:cl.netmask0=${DEPLOYMENT_NETMASK} \
    --prop:cl.gateway0=${DEPLOYMENT_GATEWAY} \
    --prop:cl.dns0=${DEPLOYMENT_DNS} \
    --datastore=${ESXI_DATASTORE} \
    Mitel-CloudLink-Gateway-1.0.0.ova \
    "vi://${ESXI_USERNAME}:${ESXI_PASSWORD}@${ESXI_HOST}/"
```

3.5 Upgrading the CloudLink Gateway

This section describes the steps to upgrade a CloudLink Gateway. The requirements differ based on the type of gateway .

To confirm the latest version, refer to https://download.mitel.io/

Note:
Containers refer to Tunnel, MiCloud and FreeSWITCH (where applicable) Gateway refers to the underlying CloudLink Gateway software.

Table 1: SMBC, Physical Gateway Appliance, Stand-Alone Virtual Appliance and KVM (5000 Only) and MSL from V2.3+:

Containers	
On start-up	**Yes**
Manual upgrade via Accounts Portal	**Yes**
Scheduled upgrade enabled	**Yes**
Gateway	
On start-up	**Yes**
Manual upgrade via Accounts Portal	**Yes**

Containers	
Scheduled upgrade enabled	**Yes**

Note:
Once the CloudLink Gateway software is on version 2.3.0 or higher the manual steps described blow are no longer required as the software will upgrade automatically as described in Table 1.

Table 2: CloudLink Virtual Gateway (MSL) Version 2.2.x or below:

Containers	
On start-up	**Yes**
Manual upgrade via Accounts Portal	**Yes**
Scheduled upgrade enabled	**Yes**
Gateway[1]	
On start-up	**No**
Manual upgrade via Accounts Portal	**No**
Scheduled upgrade enabled	**No**

[1]For upgrade procedure see *Upgrading CloudLink Virtual Gateway (MSL)*

Table 3: CloudLink Virtual Gateway (MSL) for MiVoice Office 400 Version 2.2.x or below:

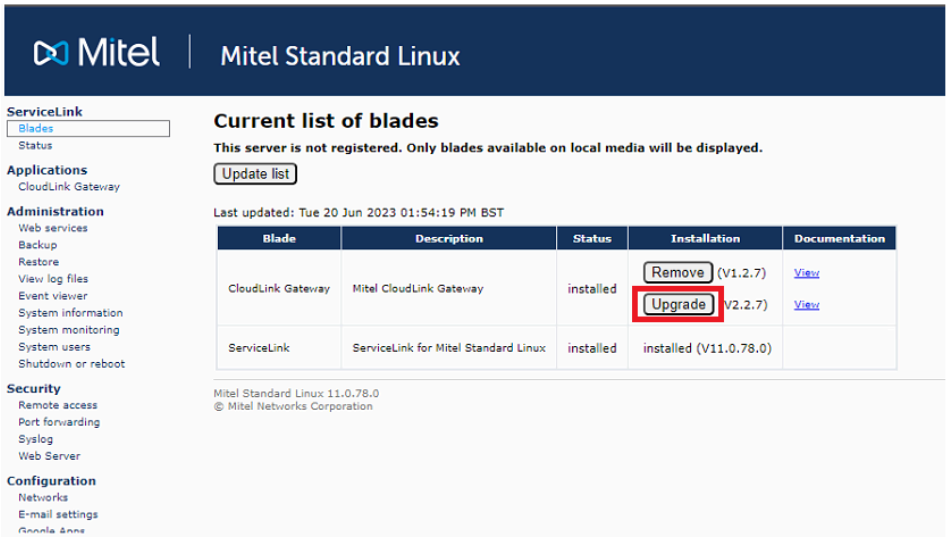
Containers	
On start-up	**Yes**
Manual upgrade via Accounts Portal	**Yes**

Containers	
Scheduled upgrade enabled	**Yes**
Gateway[2]	
On start-up	**No**
Manual upgrade via Accounts Portal	**No**
Scheduled upgrade enabled	**No**

[2]For upgrade procedure see *Upgrading CloudLink Virtual Gateway (MSL) for MiVoice Office 400*

Upgrading CloudLink Virtual Gateway (MSL)

1. Login to Mitel Standard Linux (MSL).
2. Navigate to the **Blades** panel
3. Identify the **Mitel CloudLink Gateway Blade** and if new version is available select the upgrade button.

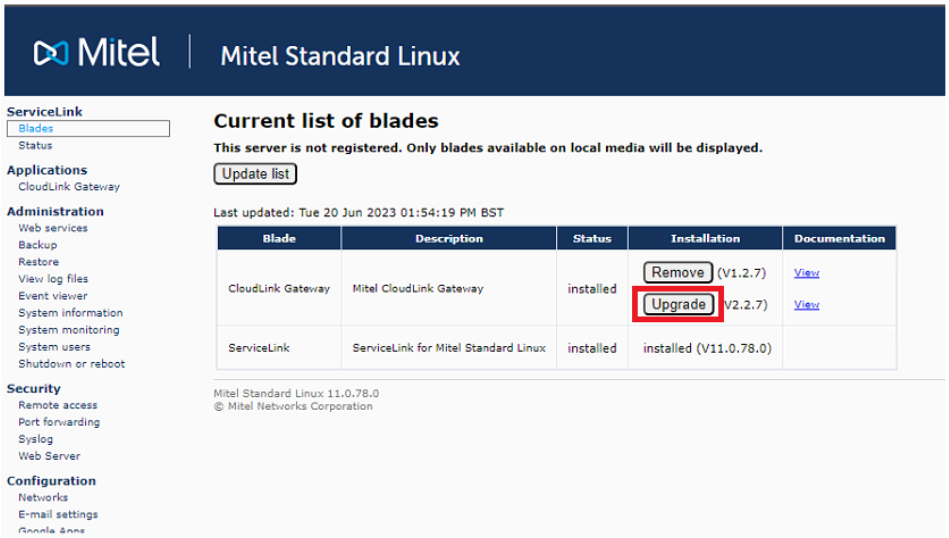


4. Once you click the upgrade button follow the on-screen prompts to complete the upgrade.

Upgrading CloudLink Virtual Gateway (MSL) for MiVoice Office 400.

1. To upgrade the CloudLink Gateway Blade, download the latest ISO image (CloudLink Virtual Gateway (MSL) Rx.x.x for MiVoice Office 400) from the Software Downloads Center.
2. Upload the ISO image to the Virtual Machines data store as described in the install section.
3. Login to MSL.

4. Navigate to the **Blades** panel
5. Identify the **Mitel CloudLink Gateway Blade** and if a new version is available, click the **Upgrade** button.



6. Once you click the upgrade button, follow the on-screen prompts to complete the upgrade.

3.6 Replacing a CloudLink Gateway

If the CloudLink Gateway appliance linked with a CloudLink customer account was factory reset or replaced, you must re-link the new Gateway appliance with the CloudLink customer account to re-establish the account's connection to the PBX.

The following table lists the platforms that are supported for re-linking after the platform type is changed.

Origin / Destination	Hardware Appliance	Virtual Appliance	SMBC	Embedded on MiVoice Office 400 MSL	KVM (MiVoice 5000)
Hardware Appliance	Supported	Supported	Not supported	Not supported	Not supported
Virtual Appliance	Supported	Supported	Not supported	Not supported	Not supported
SMBC	Not supported	Not supported	Supported	Not supported	Not supported

Origin / Destination	Hardware Appliance	Virtual Appliance	SMBC	Embedded on MiVoice Office 400 MSL	KVM (MiVoice 5000)
Embedded on MiVoice Office 400 MSL	Not supported	Not supported	Not supported	Supported	Not supported
KVM (MiVoice 5000)	Not supported	Not supported	Not supported	Not supported	Supported

Note:

- If you are replacing a Gateway type that is not supported, you must first remove the CloudLink Gateway integration then add CloudLink Gateway integration. After adding the CloudLink Gateway integration, perform the gateway deployment, following the standard installation process for the gateway type being deployed.

.

Perform the following steps to replace and re-link a Gateway appliance.

1. Install the new Gateway appliance.
2. Access Mitel Administration to onboard the new gateway appliance as indicated below:
   - For **standalone** platforms, which have an external gateway, access Mitel Administration by doing either of the following:
     - enter the IP address of the gateway appliance in a supported browser.
     - connect a supported browser to the gateway at http://cloudlink.local/.

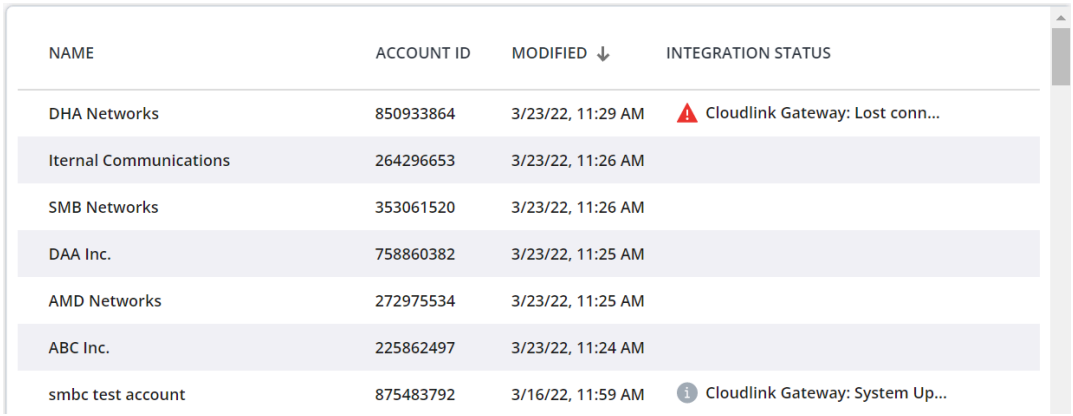
Note:
To access the gateway using http://cloudlink.local/ your system must support **mDNS.** For Windows, this support can be downloaded and installed with Bonjour Print Services. You must do this from a computing device located on the same LAN subnet as the CloudLink Gateway. For more information, see Access the CloudLink Gateway.

After successful login, the gateway will redirect you to Mitel Administration.

- For **SMBC** platforms, which have an embedded gateway, access Mitel Administration from the SMB Controller Manager. For more information, see Access the CloudLink Gateway on page 35.

  After successful login, the gateway will redirect you to Mitel Administration.

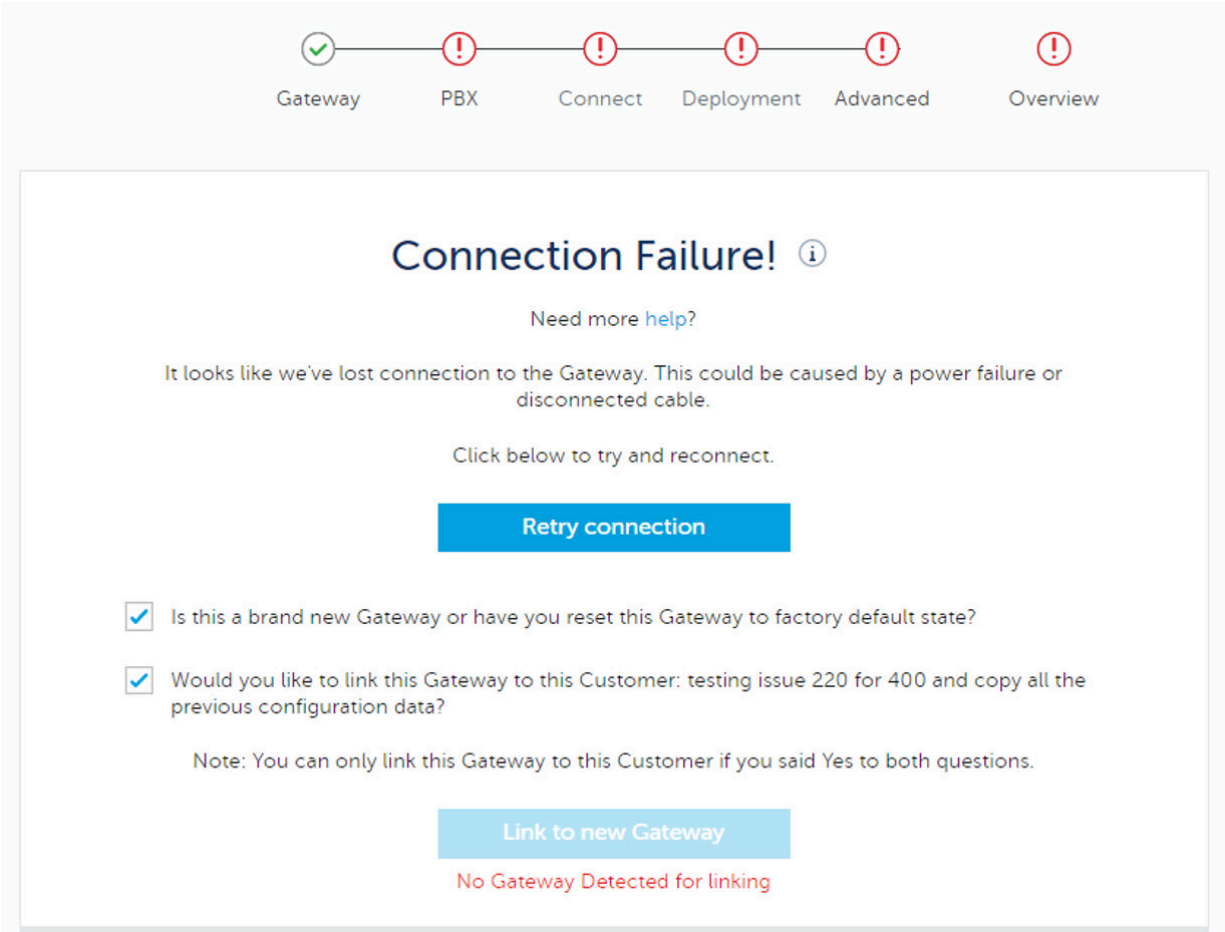
3. In the accounts list, click the CloudLink customer account associated with the old CloudLink Gateway appliance, which will show the status as **Lost Connection to gateway**.



NAME	ACCOUNT ID	MODIFIED ↓	INTEGRATION STATUS
DHA Networks	850933864	3/23/22, 11:29 AM	Cloudlink Gateway: Lost conn...
Iternal Communications	264296653	3/23/22, 11:26 AM	
SMB Networks	353061520	3/23/22, 11:26 AM	
DAA Inc.	758860382	3/23/22, 11:25 AM	
AMD Networks	272975534	3/23/22, 11:25 AM	
ABC Inc.	225862497	3/23/22, 11:24 AM	
smbc test account	875483792	3/16/22, 11:59 AM	Cloudlink Gateway: System Up...

4. In the **Integrations** panel, click the ⚙ icon associated with CloudLink Gateway integration. After you have entered the CloudLink Gateway integration page, the CloudLink Gateway portal tries to establish a connection with the old CloudLink Gateway appliance. Because the connection will not be successful, a page opens displaying a **Connection Failure** error.

5. In the **Connection Failure** error page, select the check boxes against the two confirmation questions and click **Link to new Gateway**.



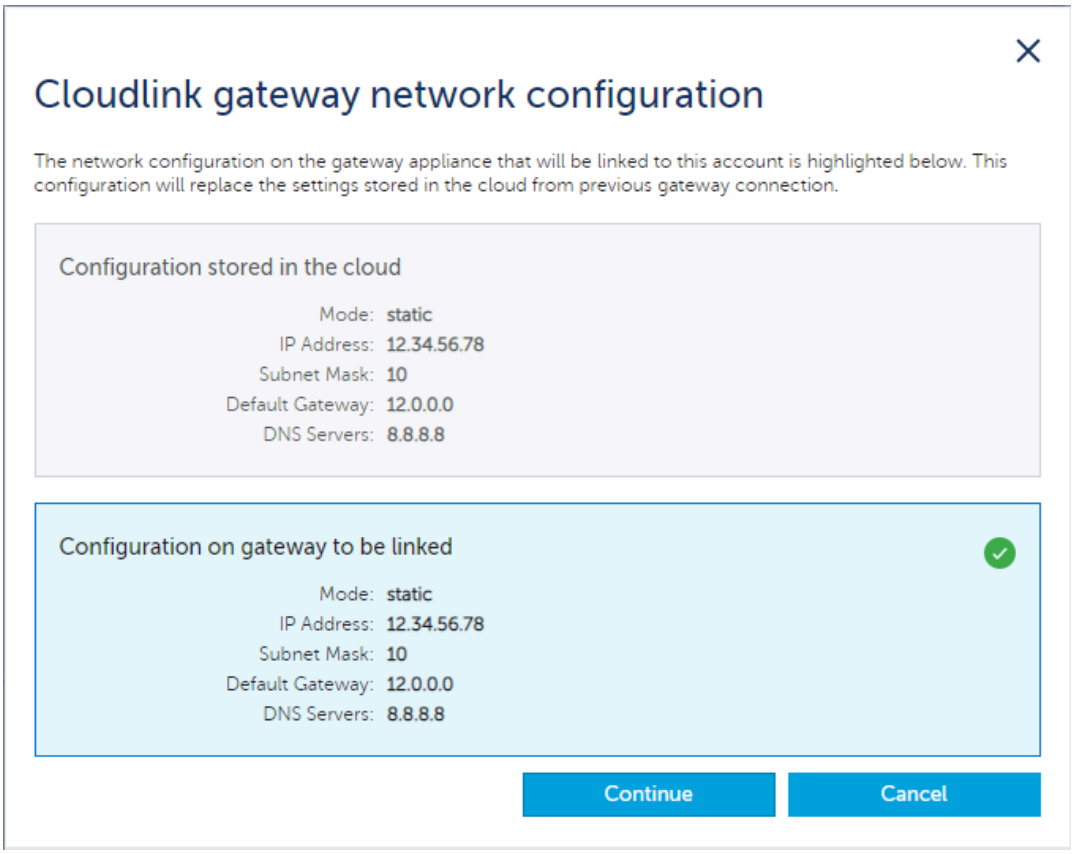
Note:

- If you do not select both check boxes, the new CloudLink Gateway appliance will not be linked to the CloudLink customer account.
- If the **Link to new Gateway** option is disabled and the error message **No Gateway detected for linking** is displayed, you must first access Mitel Administration by following the instructions described in Step 2.

6. One of the following pages will be displayed:

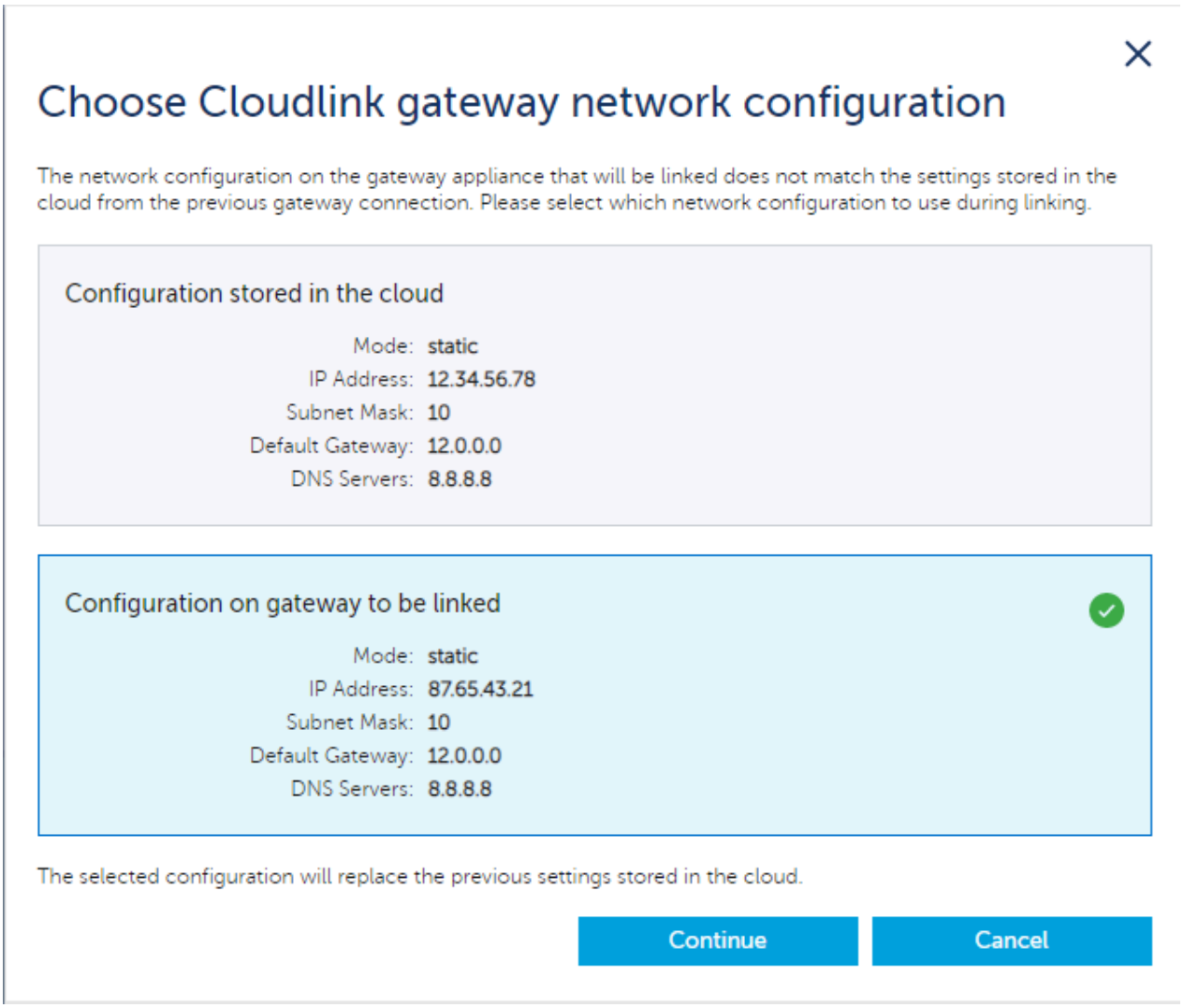
- The **CloudLink gateway network configuration** page is displayed if you are connecting a gateway appliance that has a similar network configuration to the appliance previously connected to this account. The **Configuration on gateway to be linked** option is selected by default. Review the information and click **Continue**. The **CloudLink gateway network configuration** page is displayed if you are connecting a gateway appliance that has similar network configuration to the appliance

connected to this account. The **Configuration on gateway to be linked** option is selected by default. Review the information and click **Continue**.



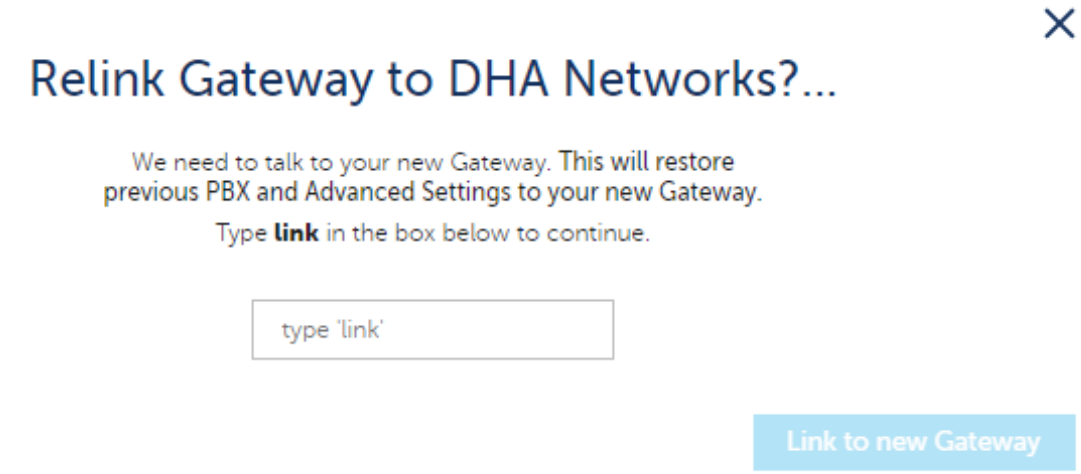
- The **Choose CloudLink gateway network configuration** page is displayed if you are connecting a gateway appliance with a network configuration that is not similar to the appliance previously connected to this account. Select **Configuration stored in the cloud** to continue with previous

network configuration or select **Configuration on gateway to be linked** to continue with the new the network configuration on the gateway appliance. Click **Continue**.

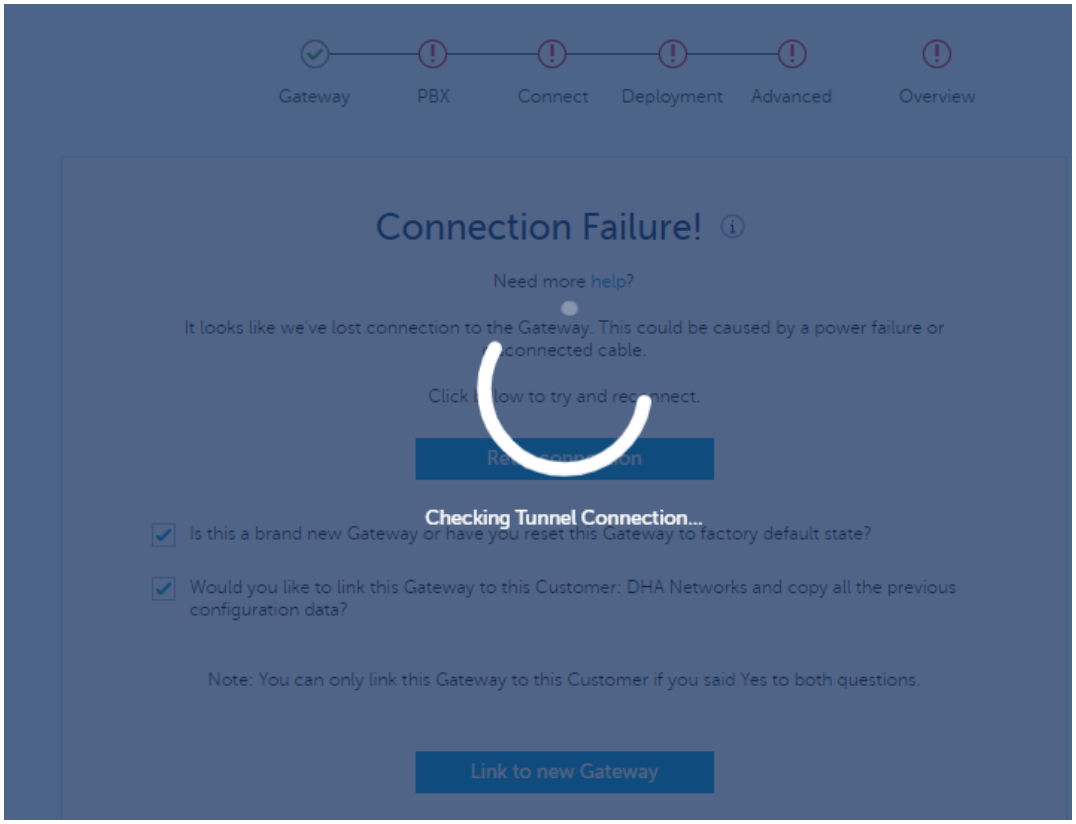


A re-link confirmation panel opens.

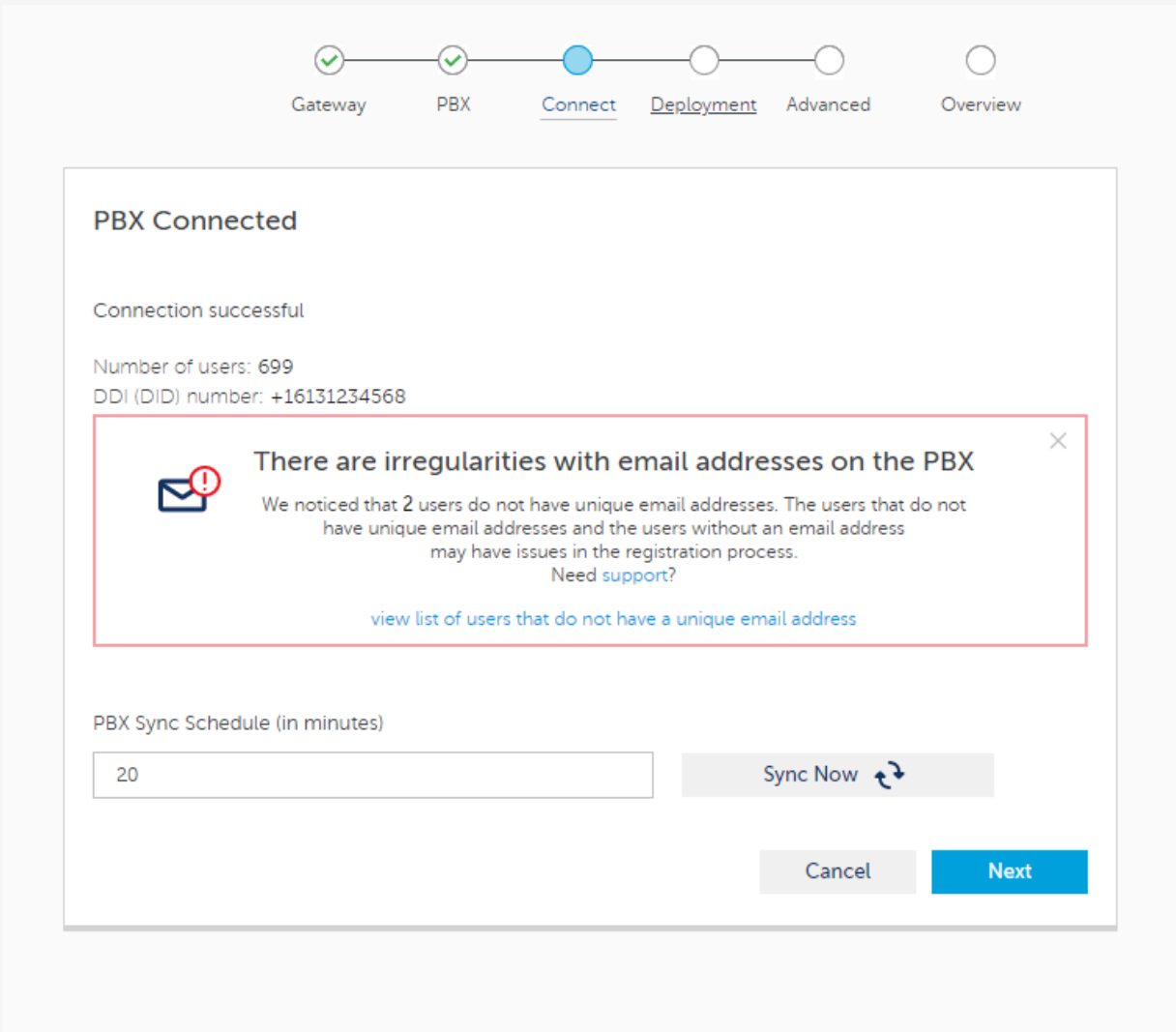
7. Type the word “link” in the text box that appears within the panel, and click **Link to new Gateway**.



The CloudLink Gateway integration attempts to establish a connection to the new CloudLink Gateway appliance. If the account previously had a PBX connected, that connection will also be re-established.



Depending on the platform (standalone or SMBC), either the **Connect** page or the **Sync** page is displayed when the new CloudLink gateway appliance is linked to the Cloudlink customer account and the PBX connection is re-established.



8. After successful configuration of the gateway, the status message associated with **CloudLink Gateway** in the **Integrations** panel changes to **Onboarding Complete** as shown below.

Restoring an MSL/MBG backup with a CloudLink Gateway

When upgrading or installing a replacement MBG OVA where the administrator will be using a backup from MSL/MBG, CloudLink Gateway data is not provided. The CloudLink Gateway data is not included in the MBG backup. If a new OVA file is installed to upgrade MBG, it is necessary to install and reconfigure the CloudLink Gateway blade from the MSL blades panel.

Perform the following steps to restore MSL/MBG backup on CloudLink Gateway Data:

1. Deploy vMBG OVA file on the host system and power on the new VM.
2. Complete the MBG upgrade/install (restoring MBG database, etc.)

Note:
Under Applications, CloudLink Gateway does not appear in MSL.

3. Install the CloudLink Gateway Blade from the MSL Blades panel.
4. From the CloudLink Gateway application (under Applications), select the **CloudLink Portal** button and log into the CloudLink Accounts Console.
5. In the Configure PBX, enter the required fields and click **Next**.

   "Successfully created PBX link" is displayed.
6. Click **retry** to try another sync.

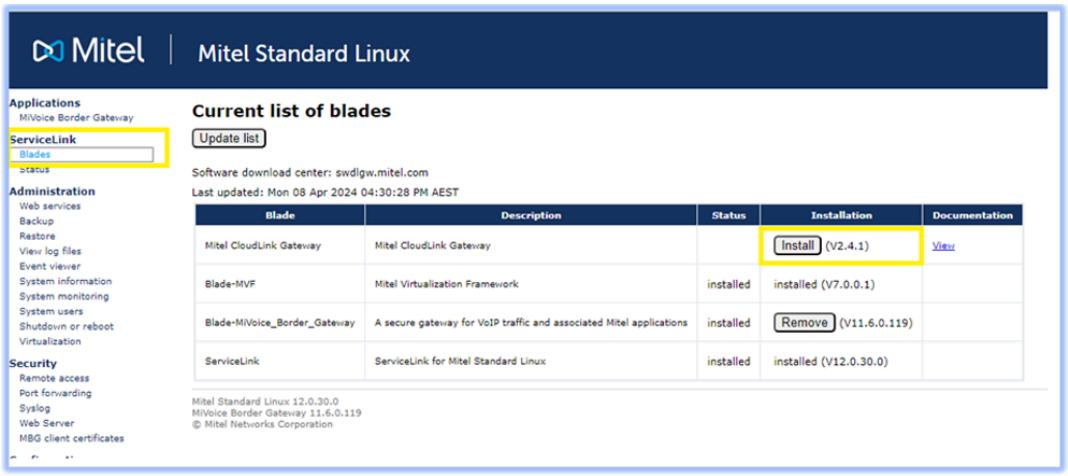
   "Successfully completed customer sync" and "Sync Successful" including number of users are displayed.
7. Click **Next**.

   "Onboarding complete" with the customer's Account ID is displayed.

3.7 Replace a Gateway in MSL

When upgrading or replacing a Mitel Border Gateway (MBG) OVA and using a backup from MSL/MBG, the backup does not include CloudLink Gateway data. Therefore, after installing a new OVA for the MBG upgrade, you must manually install and reconfigure the CloudLink Gateway blade from the MSL blades panel.

1. Login to MSL Server-Manager, navigate to **ServiceLink** > **Blades**.
2. Identify the **Mitel CloudLink Gateway Blade** and click **Install**. Once the installation process is complete, proceed to step 3.



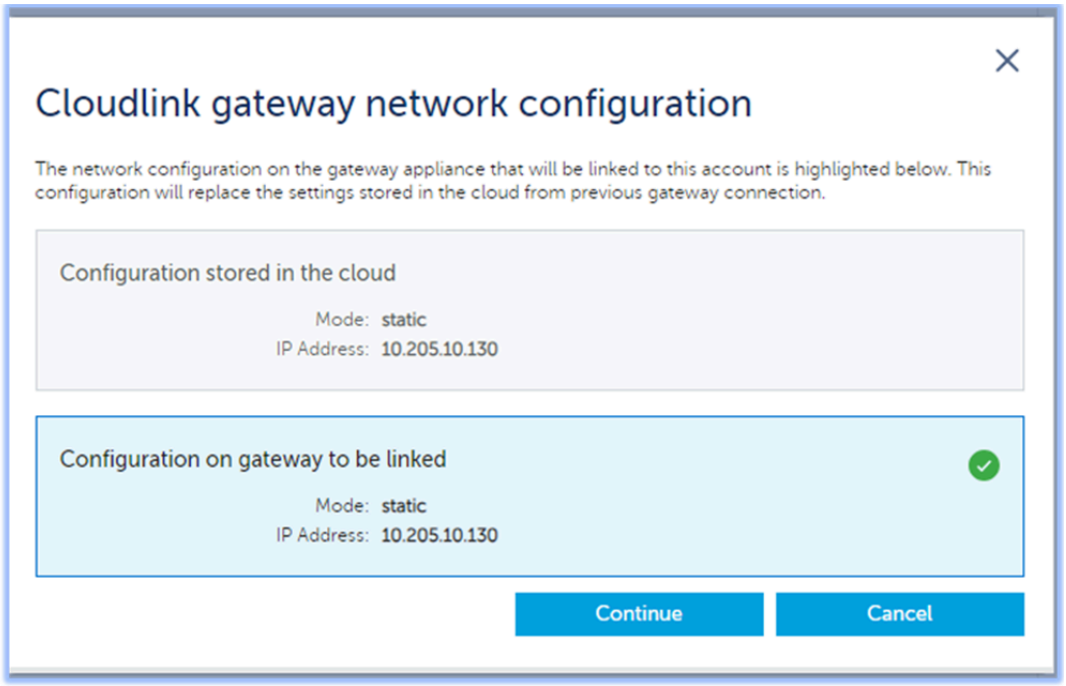
3. Navigate to **Applications** > **CloudLink Gateway**.

4. In the **CloudLink Gateway** panel, click **CloudLink portal**. You are re-directed to the Mitel Administration portal to complete the onboarding and configuration process.
5. Login to Mitel Administration console using your credentials.
6. Navigate to **Integrations and Apps**. In the **CloudLink Gateway integration** panel, an error message is displayed: **Failed to get status**.
7. Click the gear icon beside CloudLink Gateway. Since the CloudLink Gateway portal tries to establish a connection with the old CloudLink Gateway appliance, a **Connection Failure** error message page is displayed.
8. Select the check boxes and click **Link to new Gateway**.

   The CloudLink gateway network configuration page is displayed

   .

9. The **Configuration on gateway to be linked** option is selected by default. Click **Continue**.



10. In the **Relink Gateway to <Customer_Name>?** page, type the word link in the text box and click **Link to new Gateway**. This creates a connection to the MBG.
11. Enter the required details, click **Next** to complete the configuration.

Note:
The MBG and MiCollab IP address are populated with the internal IP addresses of the appliances.

3.8 Console Menu for CloudLink Gateway

The **Console** menu in CloudLink Gateway allows commands to be run locally for the physical and the virtual gateway. Functions such as Data Reset, Factory Reset, Enable/Disable SSH access for Mitel support, Ethernet configuration, Hostname, and Download logs can be performed using these commands.

To access the Console menu, press ALT+F2 for Windows and FN+F2 for MAC.

To exit the Console menu and return to home screen, press ALT+F1 for Windows and FN+F1 for MAC.

Data Reset

Data Reset allows you to reset the data that is stored on the gateway during onboarding.

Factory Reset

Factory Reset allows you to reset the boot and root partitions to factory default. During a factory reset process, the application reboots, starts the recovery system, and then restores the boot and root partition. This process may take 15-20 minutes.

For virtual gateways, **Factory Reset** option is not available. To do a factory reset, redeploy and follow the deployment guide.

Enable/Disable SSH access

By default, SSH access is disabled. SSH will be requested only by Mitel support to investigate customer issues. Selecting the SSH option enables SSH on the physical gateway for 24 hours unless it is disabled manually within this time. When SSH is enabled, a line of text is displayed above the **Menu** option indicating that SSH is enabled.

Ethernet configuration and Hostname

Ethernet configuration and Hostname allows you to configure local IPv4 settings and hostname of the gateway.

Download logs

The **Download logs** option can be used to download logs in cases where the gateway does not connect to the CloudLink Platform. When you click **Download logs**, a confirmation box is displayed with the message "**Create an unreproducible and temporary log archive URL**". Click **Yes** to continue (the download takes up to couple of minutes). A temporary URL is created, which expires after few minutes. To download the logs, type the URL into the browser of a machine that has access to CloudLink Gateway. The log files will be downloaded automatically. You can investigate the issue using plain text logs. For further assistance, share the logs as per your standard support process.

3.9 Collecting CloudLink Gateway Logs from SMBC

By default, CloudLink Gateway logs are collected through Mitel Administration. In cases where the CloudLink Gateway becomes inaccessible from Mitel Administration, you may be require to collect logs locally.

Perform the following steps to collect the logs locally:

1. Log in to the SMB Controller Manager and enable SSH access.
2. Connect through SSH connector to the SMBC (port 22) using your MiVoice Office 400 credential.

> **Note**:
> The network cable must be connected to Eth0 of the SMBC and the CloudLink container must be running.

3. Run the command `clgw-log-download`.
4. Once the logs are collected, an URL is generated. Copy the URL into a browser. The logs will start to download.

Note:
The logs expiry time is displayed in the SSH window once the log file is ready to download.

5. Disable the SSH access in the SMB Controller Manager.

Onboard Customers 4

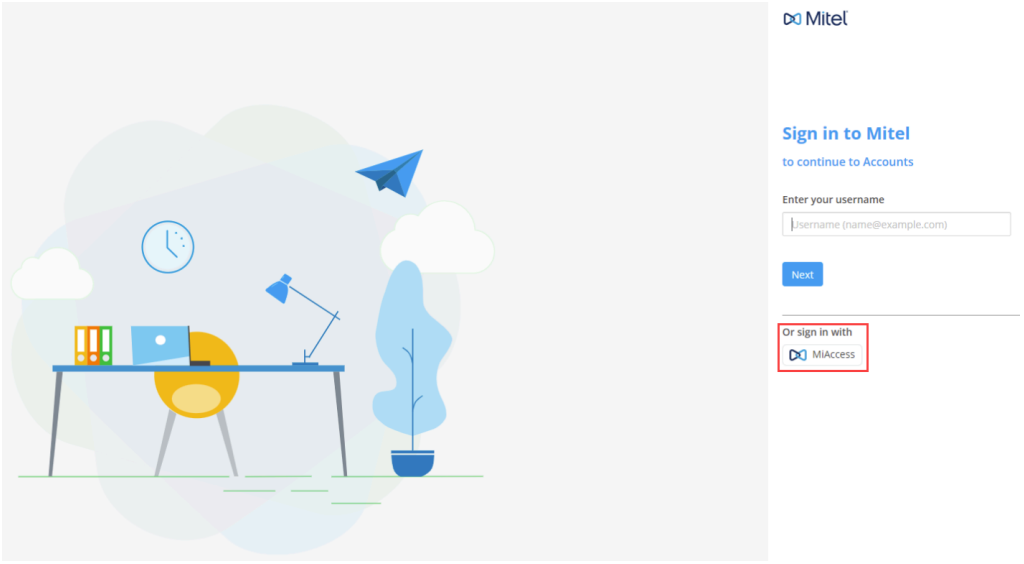
This chapter contains the following sections:

The topics listed below provide instructions for onboarding your customers, which is required to enable customers to access CloudLink applications.

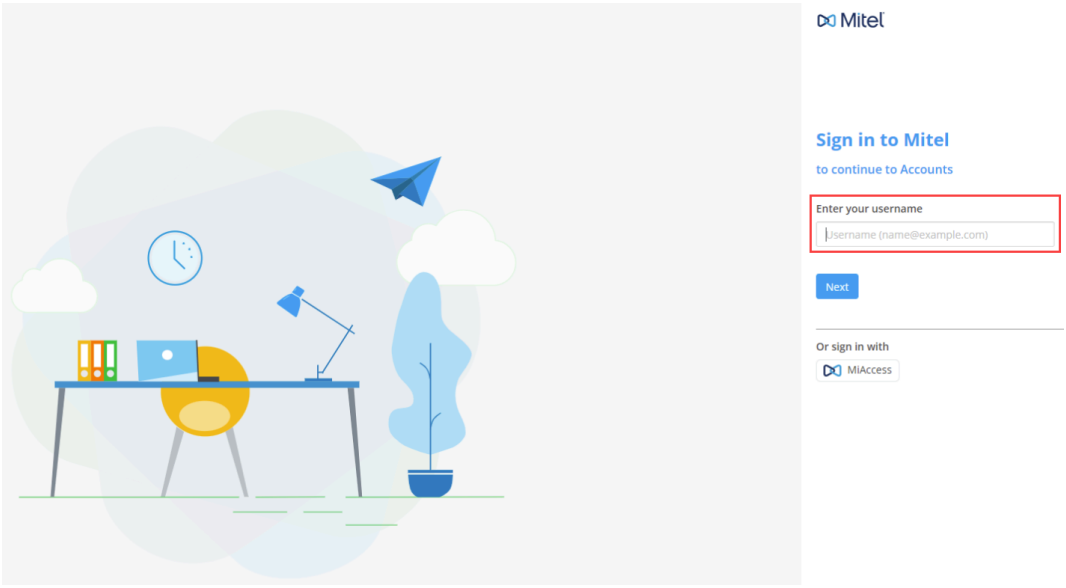
4.1 Log in to Mitel Administration

A Mitel Administrator or a user who has administrative rights over a user account can log in to the Mitel Administration directly through the URL https://accounts.mitel.io/.

To log in, a Mitel Partner must click the **MiAccess** button on the Mitel Administration login screen. In the Mitel MiAccess login page, enter your MiAccess credentials and click **LOGIN** to log in to the Mitel Administration.

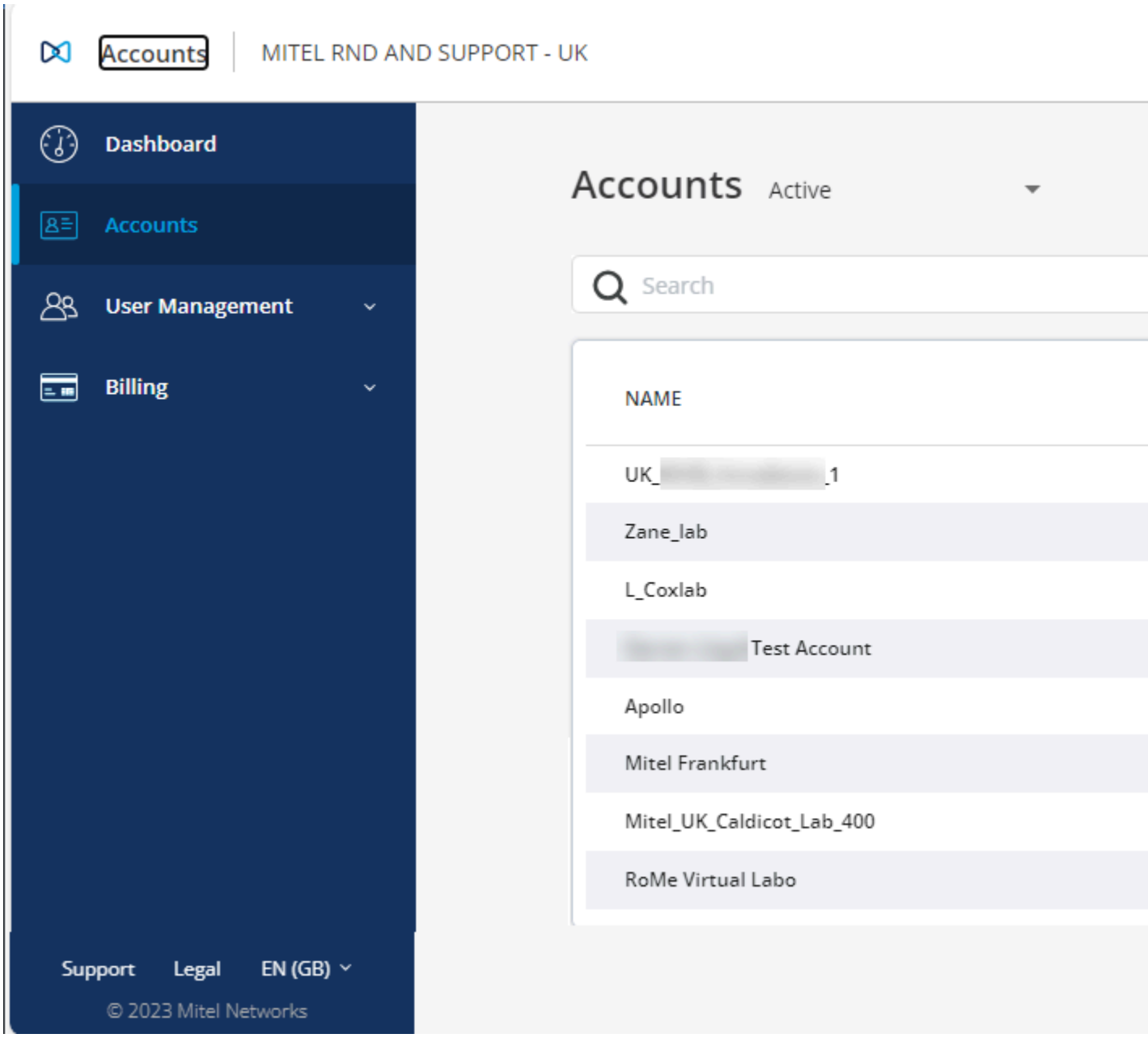


To log in, an administrative user must enter the email id (specified in the account for the user) as the user name and the password (specified by the user while registering the account) as the password, and click **Next** to log in to Mitel Administration.



Note:
If a user's email address is registered with multiple accounts, the system will identify this (while you to log in) and prompt you to enter the **Account ID** of the account (associated with the CloudLink application you want to log in to).

The Mitel Administration opens and the Partner Dashboard is displayed. The following image shows an example of the Managing Customer Accounts on page 2 when a Partner or an administrative user logs in to the Mitel Administration for the first time.



4.2 Onboard Customers Using Navigation Bar or a Single Page

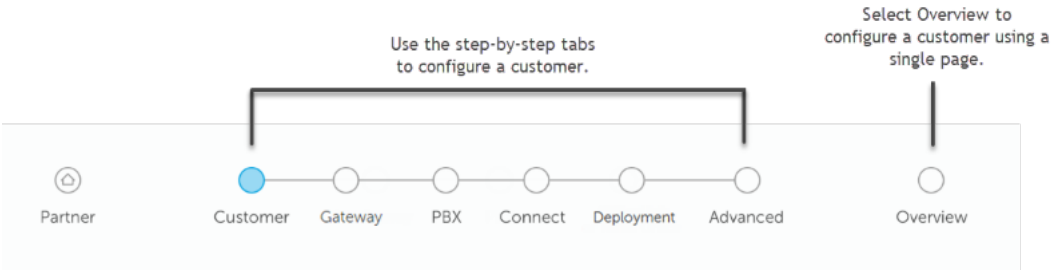
You can onboard a customer in a step-by-step manner by clicking links in the navigation bar or you can perform all steps from a single page by selecting the Overview option. Some of the onboarding steps are different for the two supported platform types listed below:

Standalone Platform with External Gateway on page 60

SMBC/VA Platform with Embedded Gateway on page 60

Standalone Platform with External Gateway

The image below shows the onboarding steps for a standalone platform, which connects an external Gateway to a MiVO400 PBX:



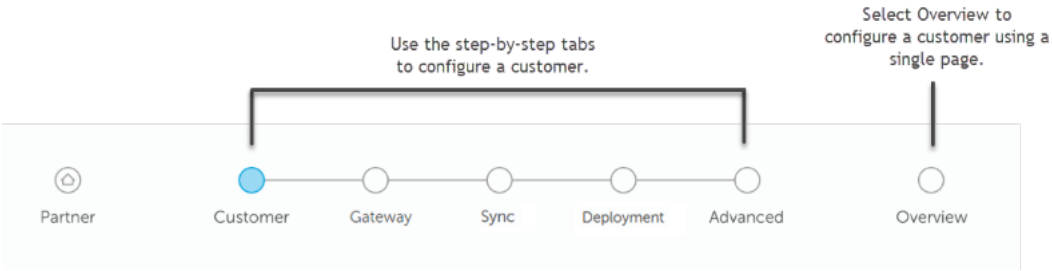
Onboarding a customer includes the following required and optional steps:

- **Required**
  - Customer - Enter information about the customer including the mailing address and admin contacts.
  - Gateway-Enter information about the physical Gateway site or the virtual machine and configure IP addresses to associate the Gateway with the CloudLink Platform.
  - PBX - Enter information to configure the MiVoice Office PBX including the IP address, CloudLink credentials, port number, and SIP trunk group credentials and extension.
  - Connect - Connect the PBX to the CloudLink Gateway and set the sync schedule.
- **Optional**
  - Deployment - Deploy the CloudLink application associated with your PBX (for example, Mitel One).
  - Advanced - Configure advanced settings that can be used for troubleshooting issues, usually while working with Mitel Support.

For standalone platforms, see Enter Customer Information for details about the next step of the onboarding process (Customer).

SMBC/VA Platform with Embedded Gateway

The image below shows the onboarding steps for an SMBC/VA platform, which syncs an embedded Gateway to a MiVO400 PBX:



Onboarding a customer includes the following required and optional steps:

- **Required**
  - Customer - Enter information about the customer including the mailing address and admin contacts.
  - Gateway-Enter information about the physical Gateway site.
  - Sync- Sync the CloudLink Gateway to the PBX.
- **Optional**
  - Deployment - Deploy the CloudLink application associated with your PBX (for example, Mitel One).
  - Advanced - Configure advanced settings that can be used for troubleshooting issues, usually while working with Mitel Support.

For SMBC/VA platforms, see Enter Customer Information for details about the next step of the onboarding process (Customer).

4.3 Enter Customer Information

Note:

For SMBC/VA platforms, the Sync step is used instead of the PBX and Connect steps shown above.

The Customer step of the onboarding process requires entering information about the customer including defining domains and adding site administrators.

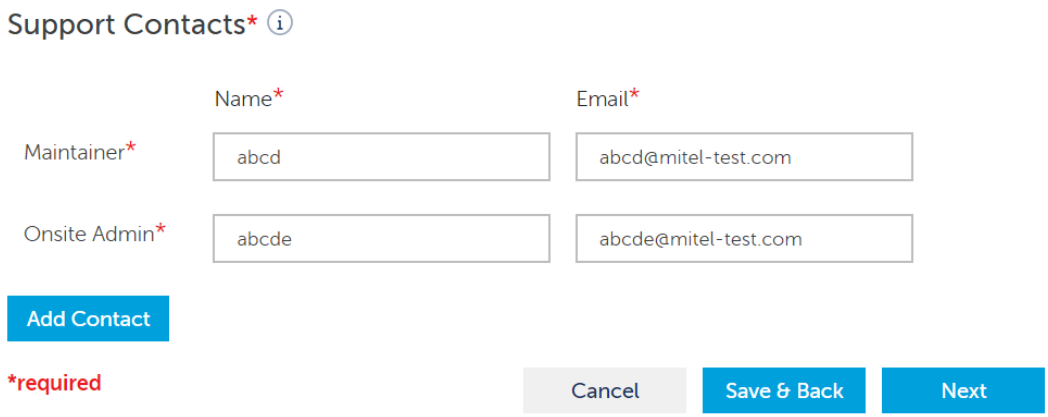
1. Enter the following information:

   - **Customer Information** - Enter the customer's name and complete mailing address (not necessarily the PBX location). Also be sure to select the most closely associated value from the Business Type menu, which is used only as statistical information to help Mitel better serve customers.
   - **Admin Contacts** - Enter any number of contacts as site administrators to provide these contacts with advanced privileges for managing CloudLink applications. For example, in the Mitel One application, an administrator can add, change, or delete other users from the account.
   - **Support Contacts** - The **Support Contacts** for a customer account comprises a **Maintainer**, **Onsite Admin**, or any **Other** contact added by the Partner user or an administrative user of that account to whom all issue reports pertaining to that account are sent.

     - **Maintainer**: Maintains the system for the customer.
     - **Onsite Admin**: Administrates the system from the site.
     - **Other**: Any other user assigned to be a support contact for the customer account.

     When a customer reports an issue with a CloudLink application, an email is sent to the **Support Contacts**. The **Support Contacts** are responsible for addressing the issues reported by their customers and when needed, contact Mitel Partner Technical Support via appropriate channels. To add a Support Contact, enter the name and email address of the **Maintainer**, **Onsite Admin**, or any **Other** user as shown in the following figure.

> **Note**:
> It is mandatory to add at least one **Maintainer** and **Onsite Admin** while onboarding a new customer. You can add as many **Support Contacts** as you want.



2. Click **Next** to continue to configure the Gateway. Click **Cancel** to discard the changes and return to the Partner dashboard. If you are a Partner, you can click **Save and Back** to save the changes and return to the Partner dashboard.

See Configure the Customer Site for information about the next step of the onboarding process (Gateway).

4.4 Configure the Customer Site

Note:
For SMBC/VA platforms, the Sync step is used instead of the PBX and Connect steps shown above.

The Gateway step of the customer onboarding process requires the following:

For **standalone**, **SMBC**, and **VA** platforms, configure the customer's CloudLink Gateway site by doing the following:

- In the Gateway Information area, enter the site name and complete address for the physical location of the PBX if different from your business address (populated by default).

Note:
The **(preview)** label associated with a country indicates that the country is recently added to the list of countries that support complete deployment of the CloudLink solution. If there are any issues, contact Mitel Partner Technical Support via appropriate channels.

For **standalone** platforms, configure the Ethernet ports on the external Gateway appliance or on the virtual machine by doing the following:

- In the Appliance Ethernet Configuration area, choose one of the following options. You can configure your DHCP server to assign a fixed IP address to the CloudLink Gateway or you can provide a static IP configuration. For more information about these options, see the Assigning an IP Address section of the Install the CloudLink Gateway Appliance topic.
  - Select **DHCP** to enable your DHCP server to set the necessary IP addresses.
  - Select **Static** to manually set the following IP addresses:
    - IP Address (static IP address assigned to Port 1)
    - Subnet Mask (subnet mask of the LAN to which Port 1 is connected)
    - Default Gateway (IP address of the router that the CloudLink Gateway will use to route IP traffic to the Internet)
    - DNS Servers (IP addresses separated by commas with the primary DNS server listed first)

For all platforms, click **Save** or **Next**.

For information about network view of various network connections see, Network View.

*For **standalone** platforms, see Enter PBX Information for details about the next step of the onboarding process (PBX).*

*For **SMBC/VA** platforms, see Connect or Sync the PBX for information about the next step of the onboarding process (Sync).*

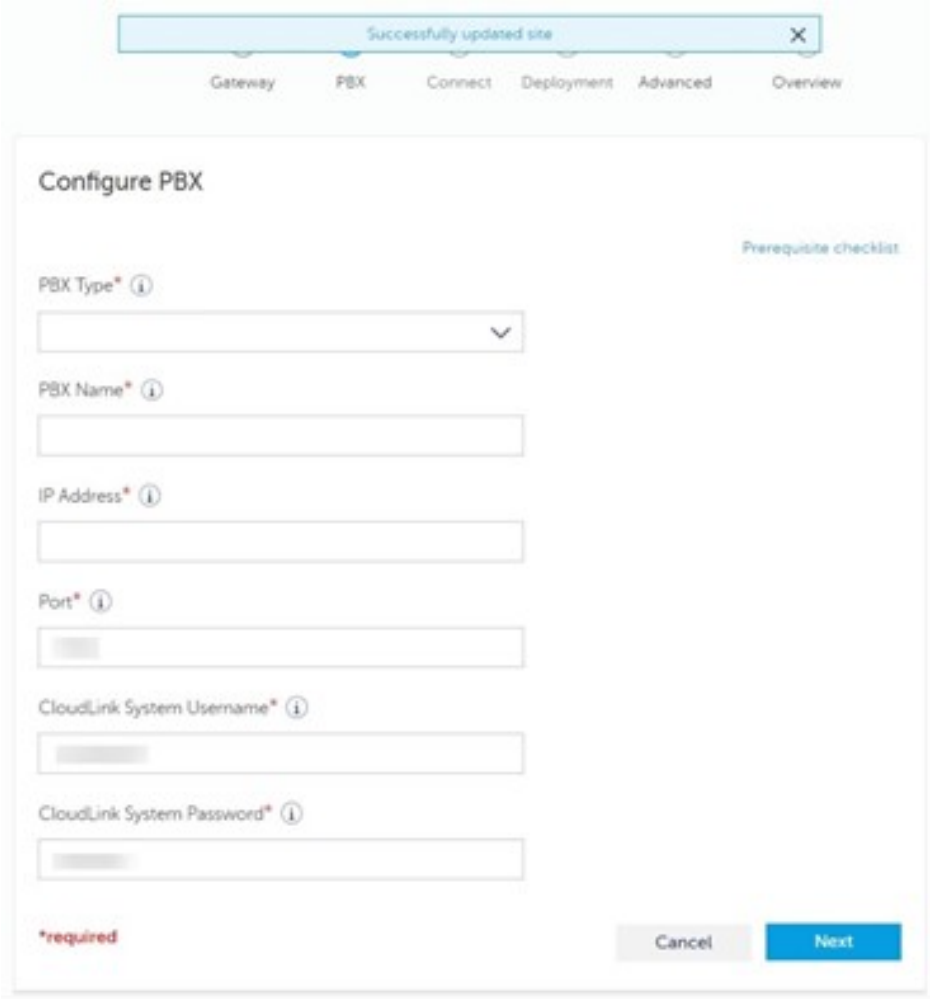
4.5 Enter PBX Information

The PBX steps of the customer onboarding process requires entering information about the PBX to begin establishing a connection between the PBX and the CloudLink platform.

Note:
The PBX step is required for standalone platforms only. For SMBC/VA platforms, perform the steps described in Connect or Sync the PBX (used instead of the PBX and Connect steps shown above).

1. Select the **PBX Type**. Depending on the type of PBX selected, enter information as follows:

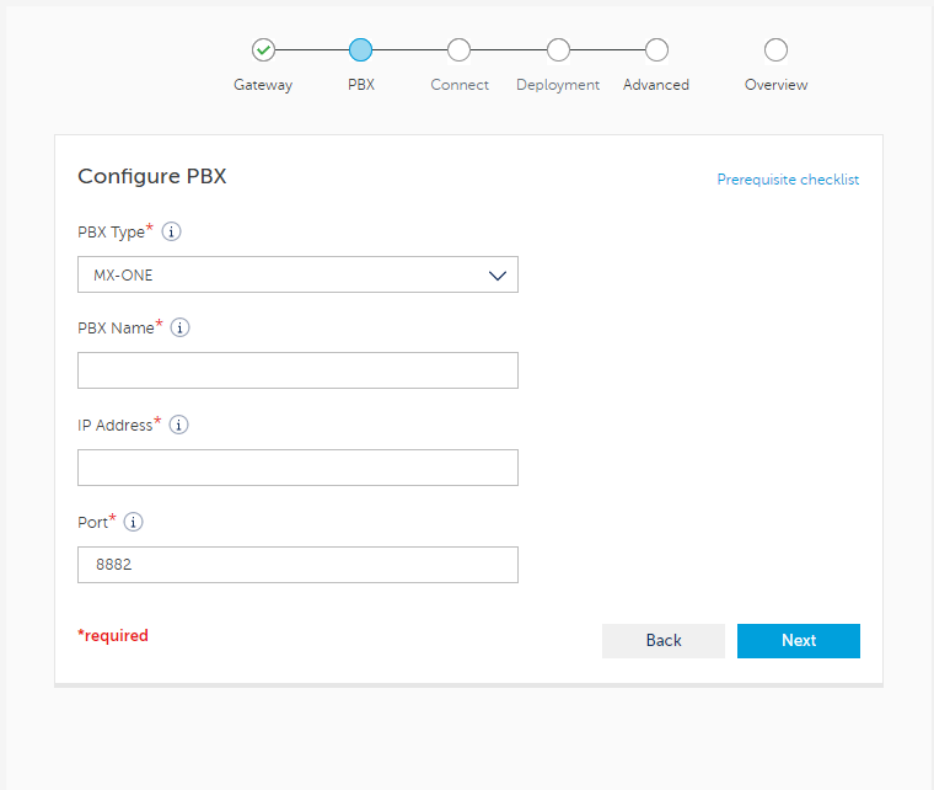
   - For MiVoice Office 400:



     a. **PBX Name**: Enter PBX name.
     b. **IP Address**: Enter the IP address of the selected PBX.
     c. **Port**: By default, the port is displayed. Enter the port number if it is different from the default port number selected for the CSTA service during Configure a MiVoice Office 400 PBX on page 78.
     d. **CloudLink System Username**: Enter the same user name entered during Configure MiVoice Office 400 on Standalone Platform on page 83.
     e. **CloudLink System Password**: Enter the same password entered during Configure MiVoice Office 400 on Standalone Platform on page 83.

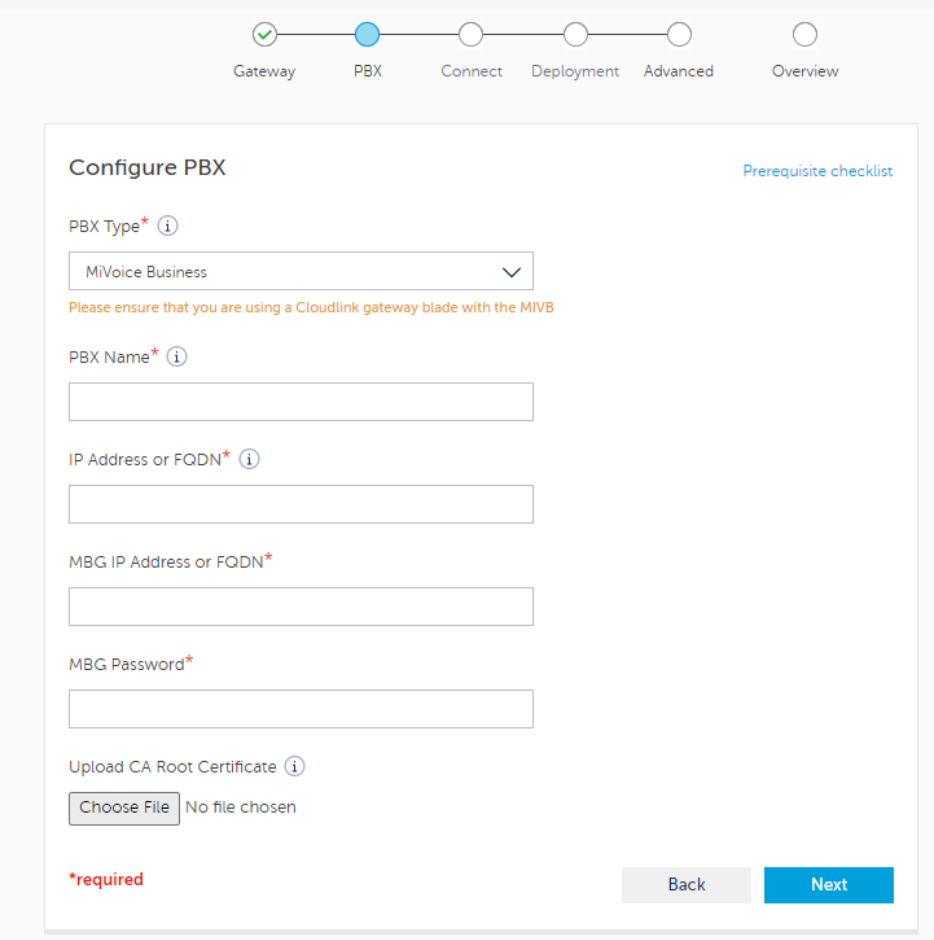
     For both standalone and SMBC platforms, see Connect or Sync the PBX on page 70 for details about the next steps of the onboarding process (Connect or Sync).

   - For MX-ONE:



a. **PBX Name**: Enter PBX name.
b. **IP Address**: Enter the IP address of the selected PBX.
c. **Port**: Enter the port number if it is different from the default port number selected for the CSTA service.

- For MiVoice Business:



a. **PBX Name**: Enter the name that was entered in the *MiVB Network Element form*.
b. **IP Address or FQDN**: Enter the IP address or the FQDN value that is displayed in the *MiVB Network Element form*. Make sure the FQDN entered in MiVoice Business matches the FQDN entered for MiVoice Business, MiVoice Border Gateway, and MiCollab (optional).

Note:

- FQDN can be resolved to internal IP of MiVoice Business.
- If Mitel Administration for MiVoice Business is to be enabled and **MiCollab** is part of the solution, enter **MiCollab IP address/FQDN** and the **MiCollab Password**.

c. **MBG IP Address or FQDN**: Enter the MBG IP address or FQDN.
d. **MBG Password**: Enter the password.
e. Upload or modify the certificate.

Note:
It is an optional step, perform this step only if you have custom certificate.

- Click **Choose file** and select the certificate from your local folder.

After you select the certificate, the certificate name is displayed under **Upload CA Root Certificate**. To remove the selected certificate, click **Remove CA Root Certificate**.

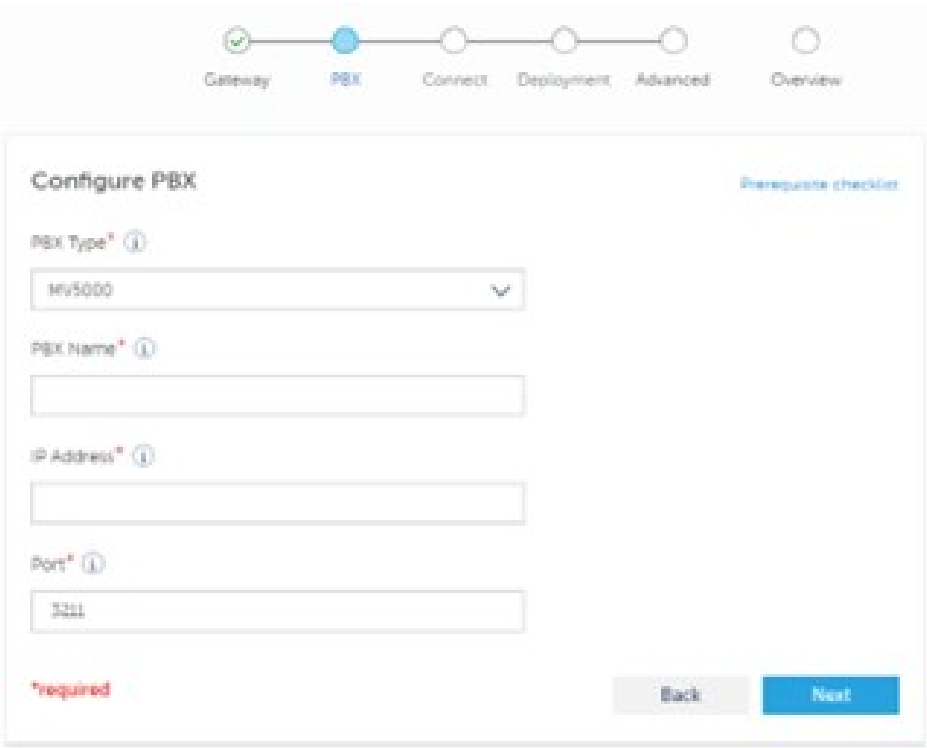
- If a certificate is already uploaded, the **Previously uploaded certificate** is displayed. To upload a new certificate, you must remove the previous certificate by clicking **Remove CA Root Certificate** and then upload the new certificate.

Note:

If the data entered while configuring MiVoice Business is incorrect, the following error might be displayed.

Error Message	Possible Reason
MBG FQDN/IP address is invalid	The MBG or FQDN IP address is not reachable
Could not update PBX Link	Could not connect to the PBX
Failed to authorized MBG	The MBG password is incorrect
Failed to initiate MiCollab	Check Trusted Networks are configured correctly on the MiCollab server

- For MiVoice Office 5000:



a. **PBX Name**: Enter PBX name.
b. **IP Address**: Enter the IP address of the selected PBX.
c. **Port**: Enter the port number if it is different from the default port number selected for the CSTA service.

2. Click **Next** if you are onboarding for the first time or click **Save** to save any changes you have made.

4.6 Connect or Sync the PBX

This step of the customer onboarding process is to connect or sync the Gateway to the PBX.

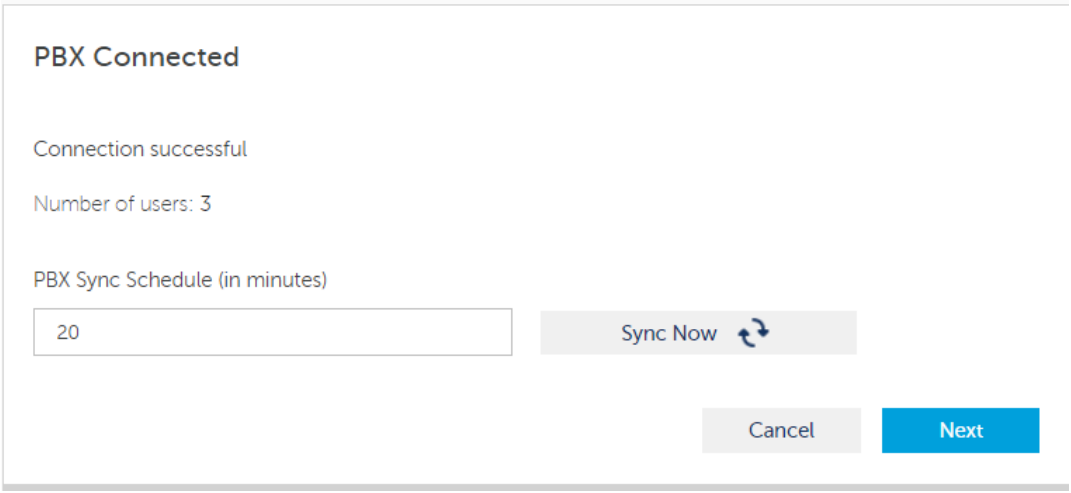
Connect or Sync your MiVO400 PBX to the CloudLink Gateway using the instructions below for your platform type:

Standalone Platform with External Gateway on page 70

SMBC/VA Platform with Embedded Gateway on page 70

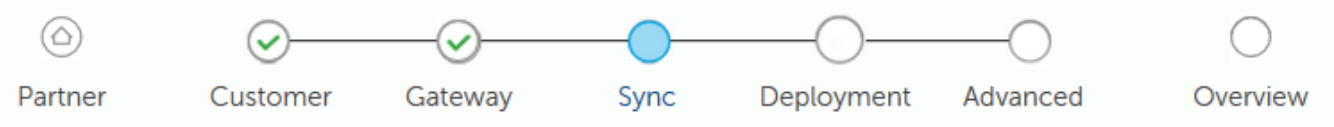
Standalone Platform with External Gateway

1. When you see the Start PBX Connection dialog, click the green **Connect** button. A "Connection successful" message appears as shown below.

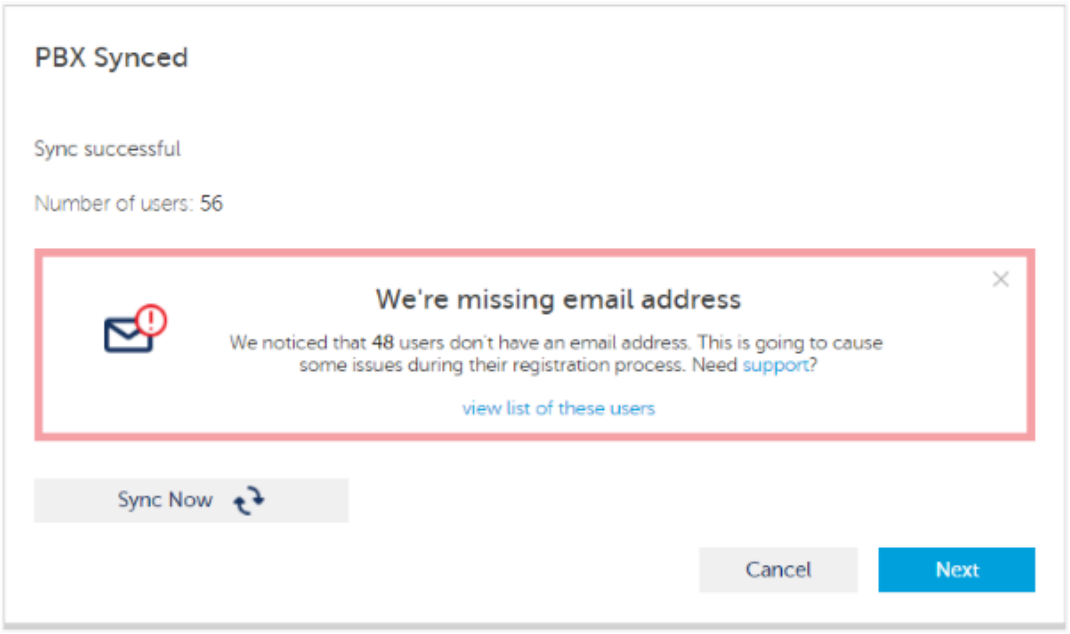


2. In the **PBX Sync Schedule** box, enter the number of minutes after which you want the PBX to be synchronized again.
3. If an error message is displayed, see Troubleshoot Errors for information about resolving errors.
4. Click **Next**.

SMBC/VA Platform with Embedded Gateway



1. When you see the Sync PBX Data dialog, click the green **Sync** button. A "Sync successful" message should appear as shown below. If this includes a warning message about missing email addresses, click the **view list of these users** link to identify the users who are missing an assigned email address in the PBX. Without an assigned email address, a user cannot register their Mitel One application.



2. If an error message is displayed, see Troubleshoot Errors for information about resolving an error.
3. Click **Next**.

Note:
For PBX users who have already been imported into CloudLink, any change in the user name made on the PBX can be synced with CloudLink by clicking **Sync** option.

For both standalone SMBC platforms, see Deploy the CloudLink App for details about the next step of the onboarding process (Mitel One).

4.7 Deploy the CloudLink App (optional)

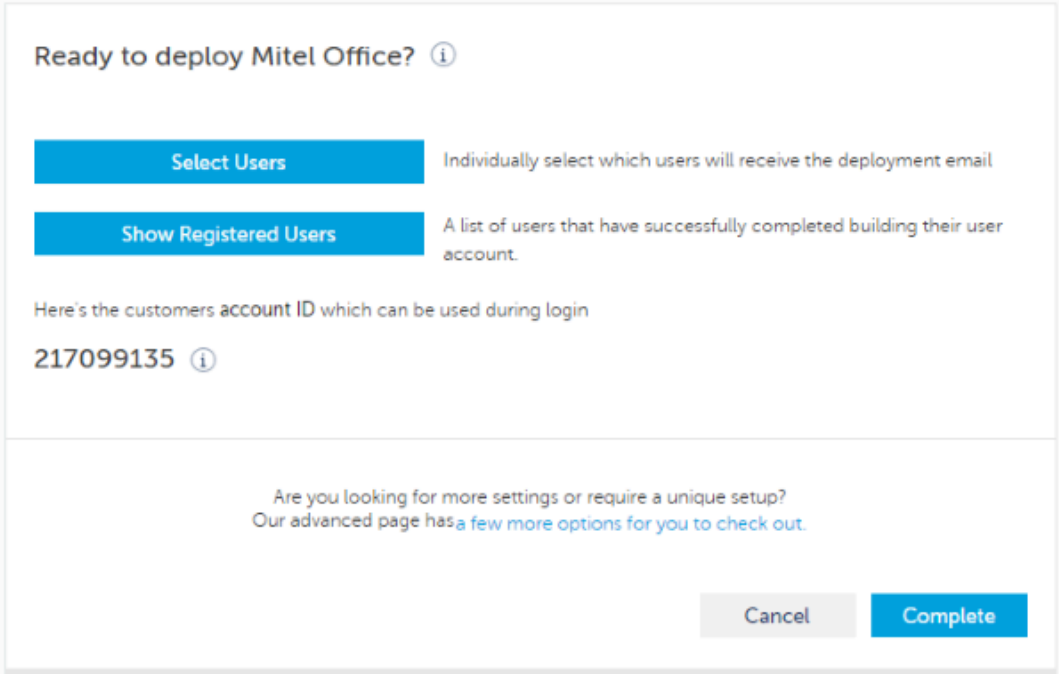
This optional step of the customer onboarding process enables you to deploy the CloudLink application.

Note:
For SMBC platforms, the **Sync** step is used instead of the **PBX** and **Connect** steps shown above.

Deploying the Mitel One require sending deployment emails.

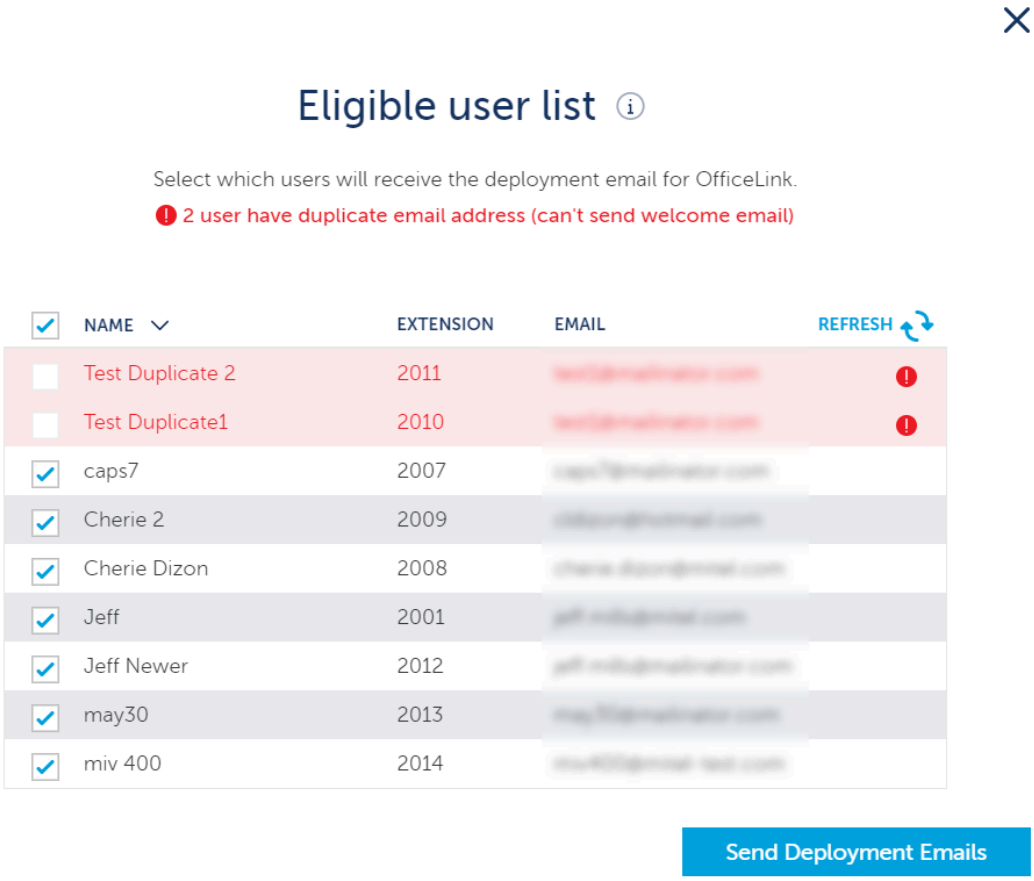
Send Deployment Emails

To specify the users to whom deployment emails will be sent, use the **Select Users** option (see the following figure).



Clicking this option displays the **Eligible user list** (see the following figure) which lists all users who have a configured email address in the MiVoice Office 250 PBX. To specify users to whom deployment emails (welcome emails) will be sent, select the checkbox beside their name and then click **Send Deployment Emails**.

Note:
You cannot send deployment emails to eligible users who have the same email address.



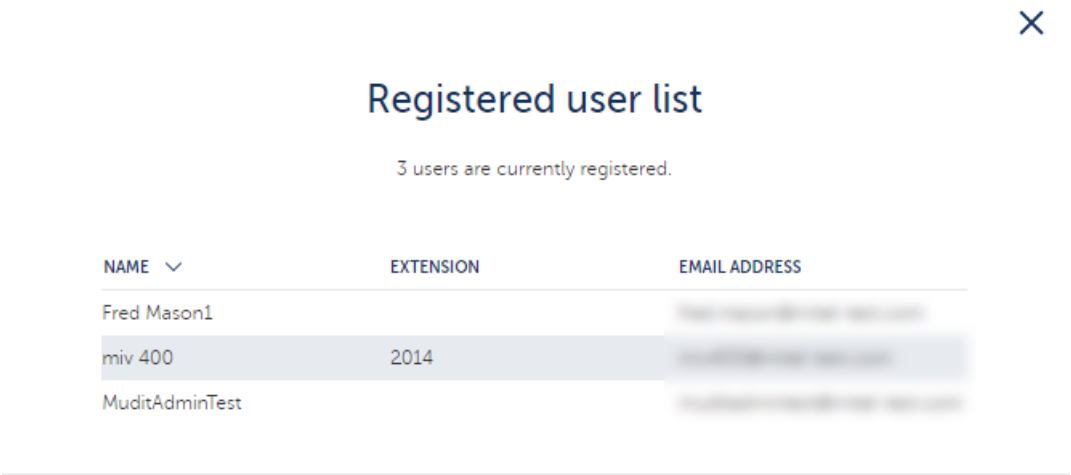
For both platforms (standalone and SMBC), see Configure Advanced Settings and Options for information about the next and last (optional) step of the onboarding process (Advanced).

Finish building the Account

Users must click the **Finish building your account** button in the welcome email they receive to register their information with Mitel and build an account to be able to log in to the Mitel One Application. For more information see, Register and Access the Mitel One Web Application.

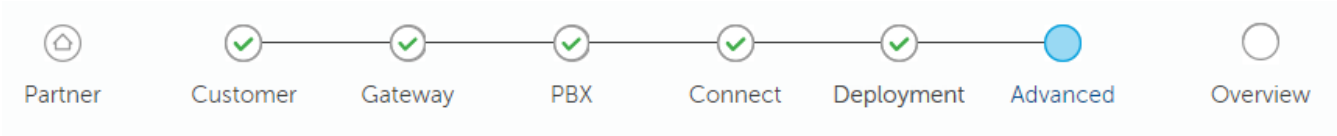
Registered Users

To view a list of all users who have successfully completed building their user accounts, click the **Show Registered Users** option. The **Registered user list** page opens (see the following figure), listing the name, phone extension number, and the email address of all registered users.



For both platforms (standalone and SMBC), see Configure Advanced Settings and Options for information about the next and last (optional) step of the onboarding process (Advanced).

4.8 Configure Advanced Settings and Options



Note:

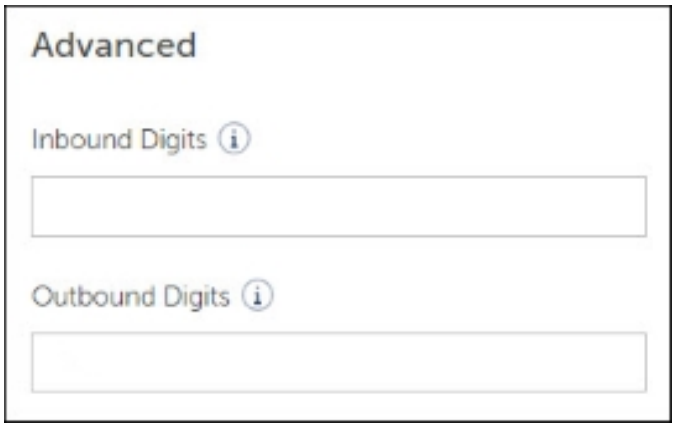
For SMBC platforms, the **Sync** step is used instead of the **PBX** and **Connect** steps shown above.

This step of the customer onboarding process enables selecting advanced settings and options that are useful for troubleshooting issues, especially when working with Mitel Support.

Advanced Settings

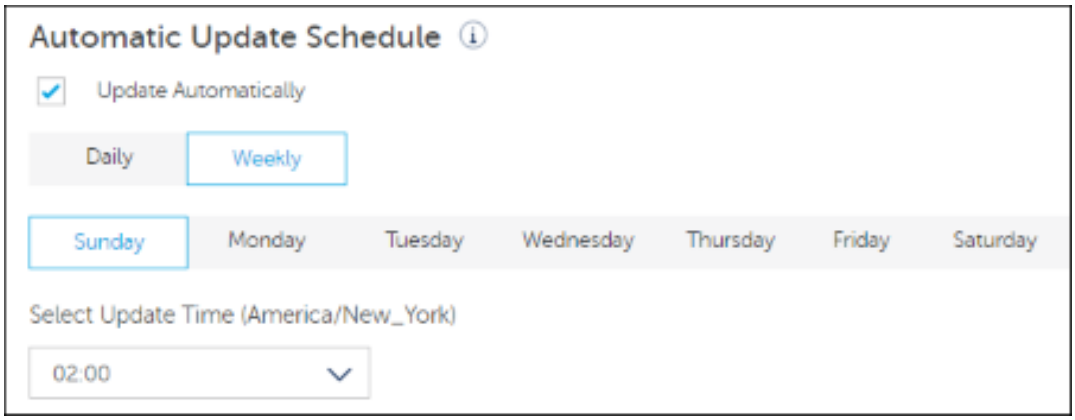
You can define leading digits for the following types of calls to manage conflicts for complex route selection plans.

- **Inbound Digits** - Define digits that will be used to route calls directed from CloudLink applications to the PBX.
- **Outbound Digits** - Define digits that will be used to route calls directed from the PBX to CloudLink applications.



Automatic Update Schedule

When the Gateway installs an update, a short service outage can occur where users may have trouble placing calls through the Gateway. It is recommended that you select an automatic update time as shown below and click **Save** to minimize the impact of the service outage. Note that updates are periodic, there may be no update when the schedule calls for an update checkpoint, and not every update causes an outage.

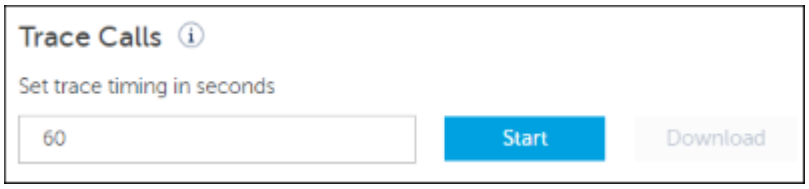


Logs

Mitel product support may request logs from the Gateway if it is not connected to the CloudLink platform. Use the Download Logs button to copy the logs to your browser so you can provide them to Mitel support.

Trace Calls

Mitel product support may request that you trace calls for a specific period of time during which the Gateway can collect detailed information about your Voice Over IP (SIP) calls. You can then download the traced call information to your browser so you can provide it to Mitel support. This option is typically used for forensic analysis of degraded call quality.



System Options

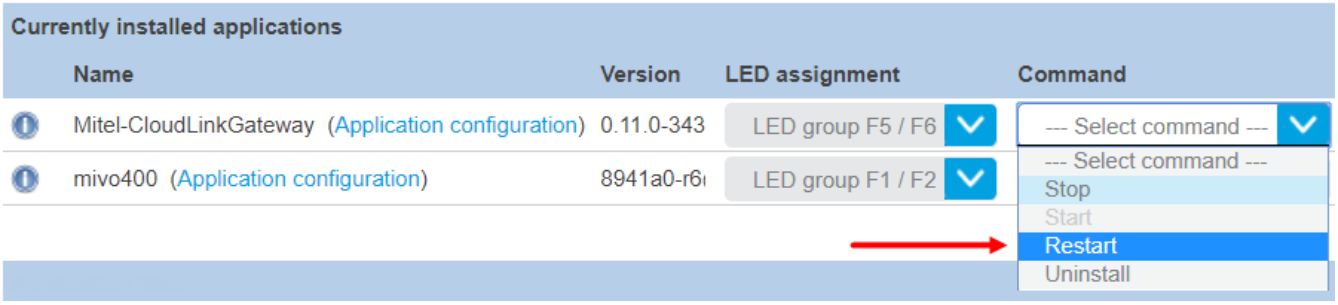
If you have a **standalone** platform with an external Gateway, as a last resort, after consulting with Mitel Support, you may need to use one of the System Options shown below:

- Factory Default – Choose this option to reset the Gateway to the factory default settings. The Gateway will need to be reprogrammed after choosing this option. If needed, contact Mitel Support for guidance.

> **Note**:
> The Factory Default option is available only for the physical gateway; it is not available for the virtual gateway.

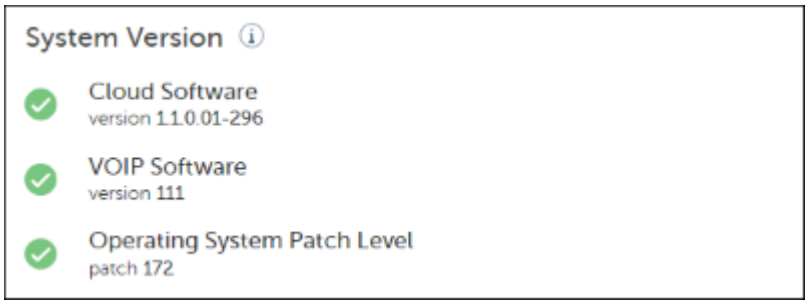
- Reboot – Choose this option to reboot the Gateway and recover service if the Gateway is not working correctly.

If you have an **SMBC** platform with an embedded Gateway, the System Options shown above are not available. However, an administrator can apply the **Restart** command to the Mitel-CloudLink Gateway in the **Software** > **Applications** screen of the SMB Controller Manager admin console as shown below.



System Version

This section of the screen indicates when updates are available and enables you to apply the updates immediately without waiting for the next scheduled update checkpoint.


System Version
Cloud Software
version 1.1.0.01-296
VOIP Software
version 111
Operating System Patch Level
patch 172

Configure a MiVoice Office 400 PBX 5

This chapter contains the following sections:

The following deployments are supported for MiVoice Office 400 PBXs on the CloudLink Platform.

Supported Deployments

- MiVoice Office 400 PBX on a **standalone platform** with an external gateway
  - M470 is supported
  - Virtual Appliance (VA) is supported
- MiVoice Office 400 PBX on an **SMBC platform** with an embedded gateway
- MiVoice Office 400 PBX on a **VA platform** with an embedded gateway

Prerequisites

- MiVoice Office 400 PBX Release 6.3 or later for embedded gateway on SMBC and external gateway.
- MiVoice Office 400 PBX Release 7.0 or later for embedded gateway on VA.
- Requires current Software Assurance and end user licensing.
- The CloudLink Gateway must be on the Master Node in an AIN (Advanced Intelligent Network) environment.
- The CloudLink Gateway for SMBC is required for SMBC platforms.
- The CloudLink Gateway for VA is required for VA platforms.

For more information about configuration prerequisites, see Configuration Prerequisites

Note:

CloudLink applications can be installed on a customer's MiVoice Office 400 PBX along with most other applications except the MiCollab client.

To find out whether a customer deployment has been successfully completed or whether more work is required, access the Partner Dashboard in the CloudLink Gateway Portal and view the status message for the desired customer.

When the PBX configuration work has been completed, which includes all Customer Onboarding work, the CloudLink Gateway is automatically configured and there is no additional programming to do. Note that all changes made to the MiVoice Office PBX are propagated immediately to the CloudLink Platform.

Number of Mitel One users supported on MiVoice 400 PBX

The following table summarizes the maximum number of Mitel One users supported on the MiVoice 400 PBX.

Testing Environment	Minimum Releases	MiVoice Office 400	CloudLink Gateway	Maximum Mitel One Users	Maximum Simultaneous Call (Direct Switching)	Maximum Simultaneous Call (Indirect Switching)
SMBC - Internal CloudLink Gateway	6.3 or later	SMBC	Embedded in SMBC	50	• 25 Mitel One to Mitel One • 50 Mitel One to Internal • 50 Mitel One to PSTN • 16 Mitel One to Mitel One (GSM) • 12 Mitel One (GSM) to Mitel One (GSM)	• 15 Mitel One to Mitel One • 15 Mitel One to Internal • 15 Mitel One to PSTN • 16 Mitel One to Mitel One (GSM) • 12 Mitel One (GSM) to Mitel One (GSM)
Mitel 470 - External CloudLink Gateway	6.3 or later	Physical Mitel 470	CloudLink Gateway	300	• 25 Mitel One to Mitel One • 50 Mitel One to Internal • 50 Mitel One to PSTN • 16 Mitel One to Mitel One (GSM) • 12 Mitel One (GSM) to Mitel One (GSM)	Same as Direct Switching
Virtual Appliance - Virtualized CloudLink Gateway	6.3 or later	Virtual Appliance	OVA	300	**Default appliance with 1 core CPU and 2GB RAM** • 25 Mitel One to Mitel One • 50 Mitel One to Internal • 50 Mitel One to PSTN • 16 Mitel One to Mitel One (GSM) • 12 Mitel One (GSM) to Mitel One (GSM)	**Default appliance with 1 core CPU and 2GB RAM** • Same as Direct Switching

Testing Environment	Minimum Releases	MiVoice Office 400	CloudLink Gateway	Maximum Mitel One Users	Maximum Simultaneous Call (Direct Switching)	Maximum Simultaneous Call (Indirect Switching)
					Medium appliance with 4 cores CPU and 2 GB RAM • 30 Mitel One to Mitel One • 60 Mitel One to Internal • 60 Mitel One to PSTN • 20 Mitel One to Mitel One (GSM) • 15 Mitel One (GSM) to Mitel One (GSM) **Note**: Medium profile supports up to 120 RTP ports. Call capacity is calculated based on this limit. The same limits apply for both Direct and Indirect Switching.	**Medium appliance with 4 cores CPU and 2 GB RAM** • Same as Direct Switching

Testing Environment	Minimum Releases	MiVoice Office 400	CloudLink Gateway	Maximum Mitel One Users	Maximum Simultaneous Call (Direct Switching)	Maximum Simultaneous Call (Indirect Switching)
					Large appliance with 8 cores CPU and 4GB RAM • 125 Mitel One to Mitel One • 125 Mitel One to Internal • 125 Mitel One to PSTN • 16 Mitel One to Mitel One (GSM) • 12 Mitel One (GSM) to Mitel One (GSM) **Note**: 125 simultaneous calls are supported only if the appliance is upgraded to OVA version 1.1.3 or later.	**Large appliance with 8 cores CPU and 4GB RAM** • Same as Direct Switching
MSL	7.0 HF2 or later	Virtual Appliance/MSL	OVA/MSL	300	**Default appliance with 2 cores CPU and 2GB RAM** • 25 Mitel One to Mitel One • 50 Mitel One to Internal • 50 Mitel One to PSTN • 16 Mitel One to Mitel One (GSM) • 12 Mitel One (GSM)to Mitel One (GSM)	**Default appliance with 2 cores CPU and 2GB RAM** • Same as Direct Switching

Testing Environment	Minimum Releases	MiVoice Office 400	CloudLink Gateway	Maximum Mitel One Users	Maximum Simultaneous Call (Direct Switching)	Maximum Simultaneous Call (Indirect Switching)
					Medium appliance with 4 cores CPU and 2 GB RAM • 30 Mitel One to Mitel One • 60 Mitel One to Internal • 60 Mitel One to PSTN • 20 Mitel One to Mitel One (GSM) • 15 Mitel One (GSM) to Mitel One (GSM) **Note**: Medium profile supports up to 120 RTP ports. Call capacity is calculated based on this limit. The same limits apply for both Direct and Indirect Switching.	**Medium appliance with 4 cores CPU and 2 GB RAM** • Same as Direct Switching
					Large appliance with 8 cores CPU and 5GB RAM • 125 Mitel One to Mitel One • 125 Mitel One to Internal • 125 Mitel One to PSTN • 16 Mitel One to Mitel One (GSM) • 12 Mitel One (GSM) to Mitel One (GSM)	**Large appliance with 8 cores CPU and 5GB RAM** • Same as Direct Switching

Note:
The maximum values mentioned in the table are subject to available bandwidth. For information about Bandwidth, see CloudLink Platform.

Documentation

Choose one of the following topics for the platform being used to configure your MiVoice Office 400 PBX (MiVO400) to integrate with CloudLink. For PBX documentation, click here.

- Configure MiVO400 on Standalone Platform
- Configure MiVO400 on SMBC Platform
- Configure MiVoice Office 400 on Virtual Appliance on page 100

5.1 Configure MiVoice Office 400 on Standalone Platform

This topic explains how to configure a MiVoice Office 400 PBX on an standalone platform (with external Gateway) to integrate with CloudLink. For detailed PBX instructions, see the MiVoice Office 400 technical documentation.

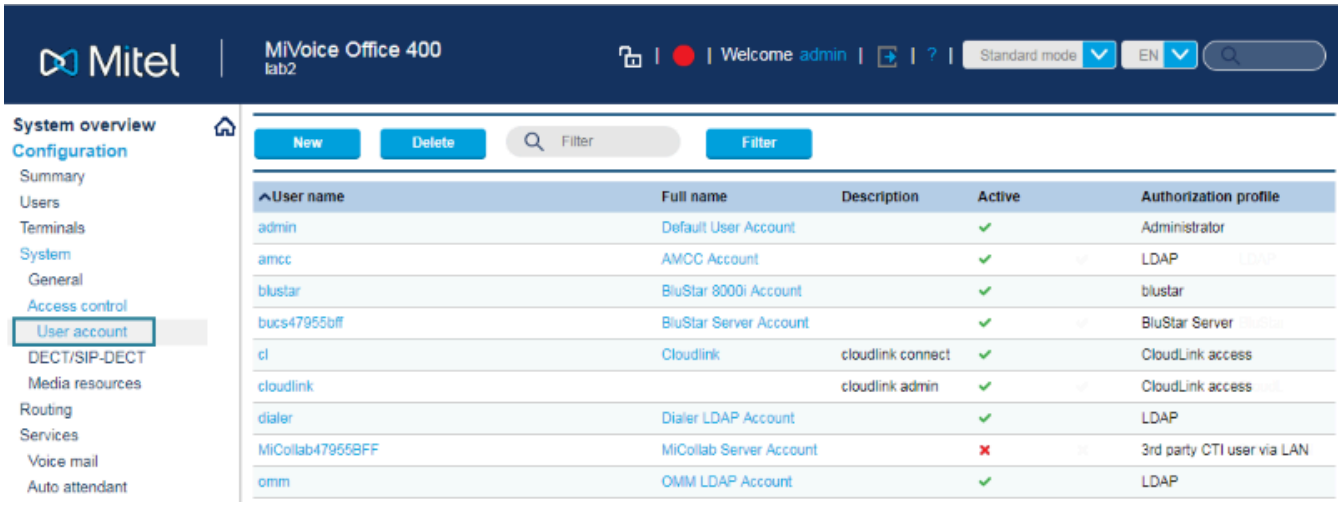
Use the instructions in the sections below in this specific order to ensure that your MiVoice Office 400 is correctly integrated with CloudLink. Leave all other settings (not specifically mentioned in these sections) set to the default value.

1. Create CloudLink Application Credentials
2. Enable CSTA Service
3. Add CloudLink App Users
4. Configure SIP Multi Lines and Manage Call Permission on page 88
5. Enable CTI Service on page 89
6. Onboard Customers
7. Verify SIP Networking
8. Verify Mitel CloudLink Gateway Service
9. Configure GSM Call Through Feature

Create CloudLink Application Credentials

For licensing purposes, an admin user must be added to the MiVoice Office 400 PBX to create CloudLink application credentials, which sets the CloudLink Gateway as a trusted application.

1. Navigate to **Configuration** > **System** > **Access Control** > **User account** and click the **New** button.



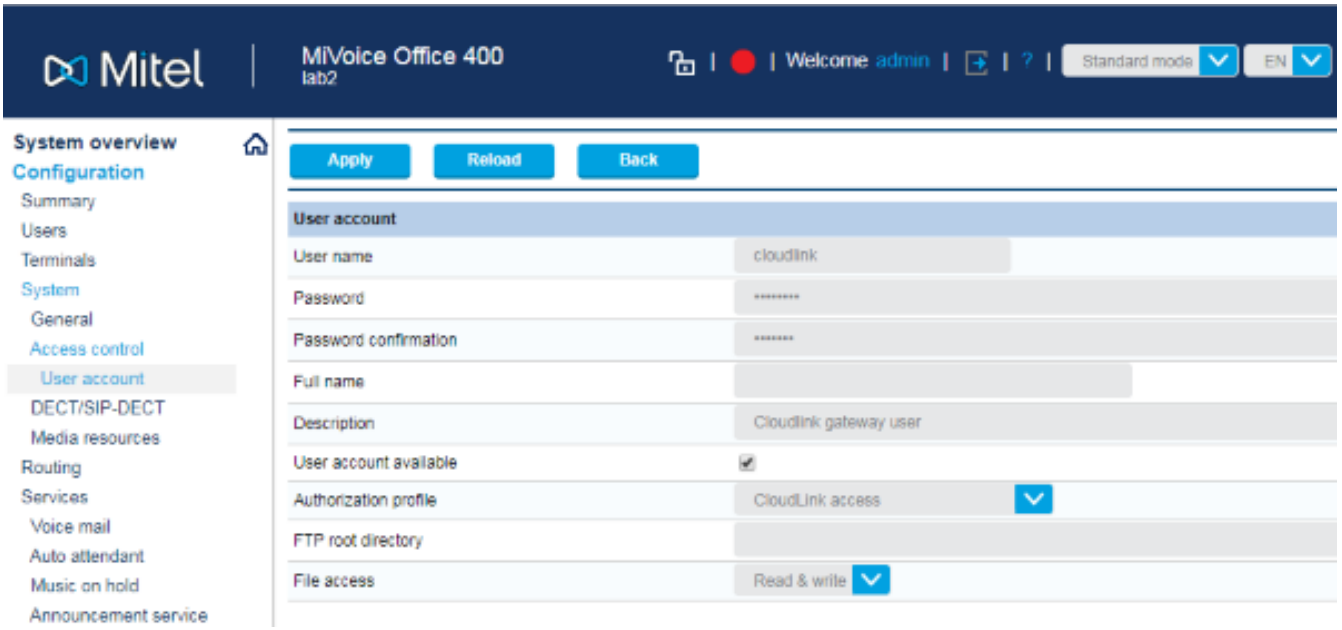
2. Create an admin user as indicated below.

- In the **User name** field, enter any username that is 25 characters or less.
- In the **Password** field, enter any valid password that is 255 characters or less.

Note:

The username and password values entered here must also be entered in the **CloudLink System Username** and **CloudLink System Password** fields in the Configure PBX section of the CloudLink Gateway Portal during customer onboarding. For more information, see MiVoice Office 400 PBX information.

- In the **Password confirmation** field, re-enter the same password.
- In the **Authorization profile** field, select the **CloudLink access** option.
- In the **File access** field, select the **Read write** option.



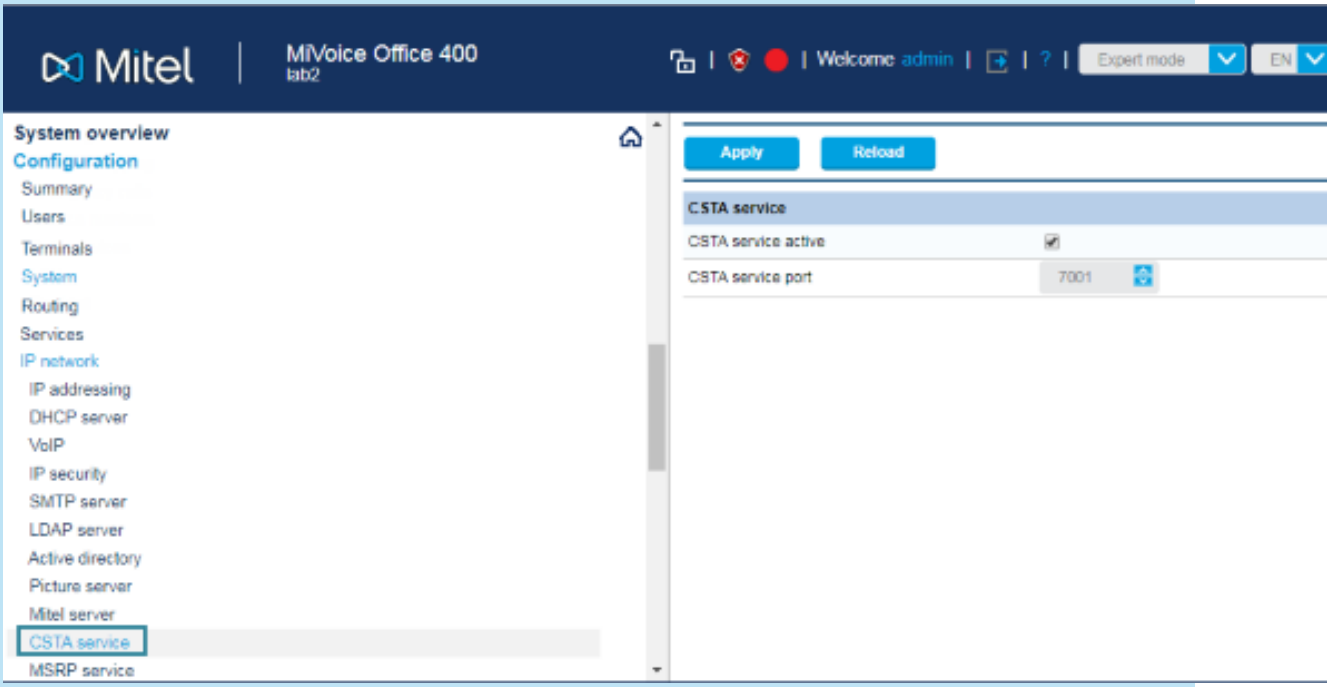
3. Click the **Apply** button to create this user. Verify that a green check mark appears in the Active column next to new user.

Enable CSTA Service

The CSTA (computer-supported telecommunications applications) service needs to be enabled.

1. Navigate to **Configuration** > **IP network** > **CSTA service**.
2. Select the check box next to the **CSTA service active** field.
3. Leave the **CSTA service port** set to the default value of 7001. If needed, you can set this to a different number.

Note:
The service port number set here must also be set in the **Port** field in the Configure PBX section of the CloudLink Gateway Portal during customer onboarding. For more information, see MiVoice Office 400 PBX information.



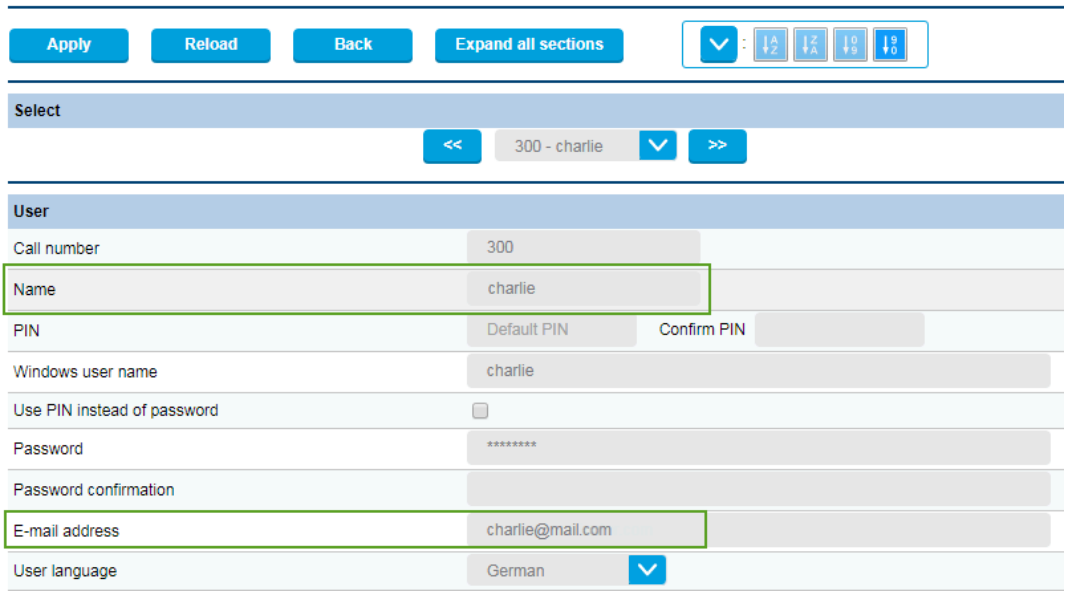
Add CloudLink App Users

The MiVoice Office 400 PBX needs to be programmed to add all of the users who will be able to access CloudLink applications like the Mitel One.

To create a user:

1. Navigate to **Configuration** > **Users**
2. Enter the following required information for each user of the Mitel One application:
   - **Name**
   - **E-mail address**

3. Click **Apply**. Users will be propagated through push notifications to the CloudLink Platform.



Note:
When users register their Mitel One application for the first time, the MiVoice Office softphone terminal is created and assigned to those users on the MiVoice Office 400 PBX.

To log in to the Mitel One application, a user must have a valid:

- MiVoice 400 Software Assurance (SWA) license from Mitel
- MiVoice Office softphone terminal license in the MiVoice 400 PBX.

If the user does not have these two licenses or if these licenses have expired, a **No License Available** alert appears when the user attempts to log in to the Mitel One application and the user will not be able to log in. The user must then obtain new licenses or renew the existing licenses to continue using the Mitel One application.

To edit the email address of a user:

1. Navigate to **Configuration** > **Users**.
2. Enter the new email of the user in the **E-mail address** field.
3. Click **Apply** to save the changes.
4. Sync the MiVoice Office 400 PBX with the CloudLink Gateway for the changes to reflect in the CloudLink Platform.

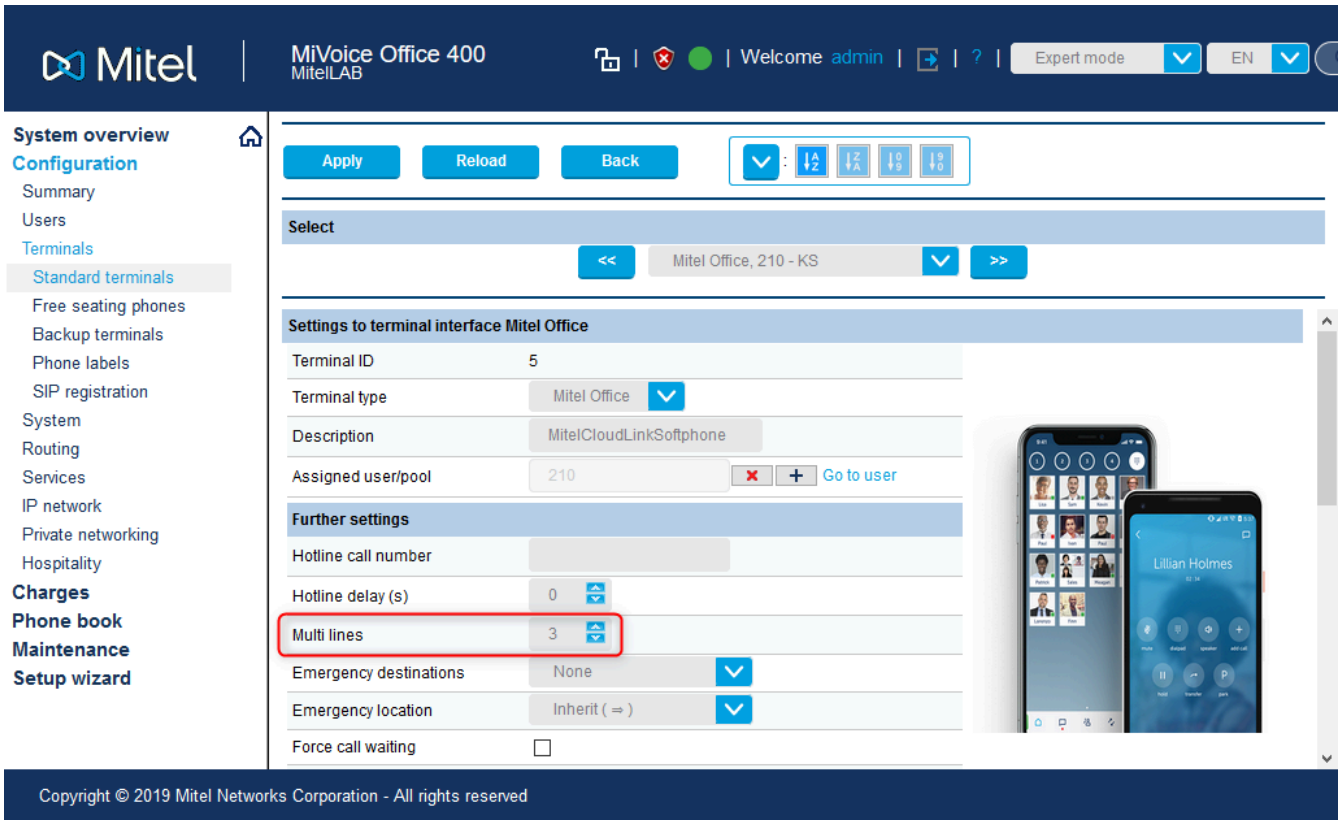
Configure SIP Multi Lines and Manage Call Permission

To enable call waiting in the Mitel One application, you must:

- configure the MiVO-400 SIP terminal representing the SIP softphone to set the **Multi lines** value set to 3.
- in **Permission Set**:
  - enable **Call Waiting** for the softphone
  - disable **Busy on busy** for the softphone.

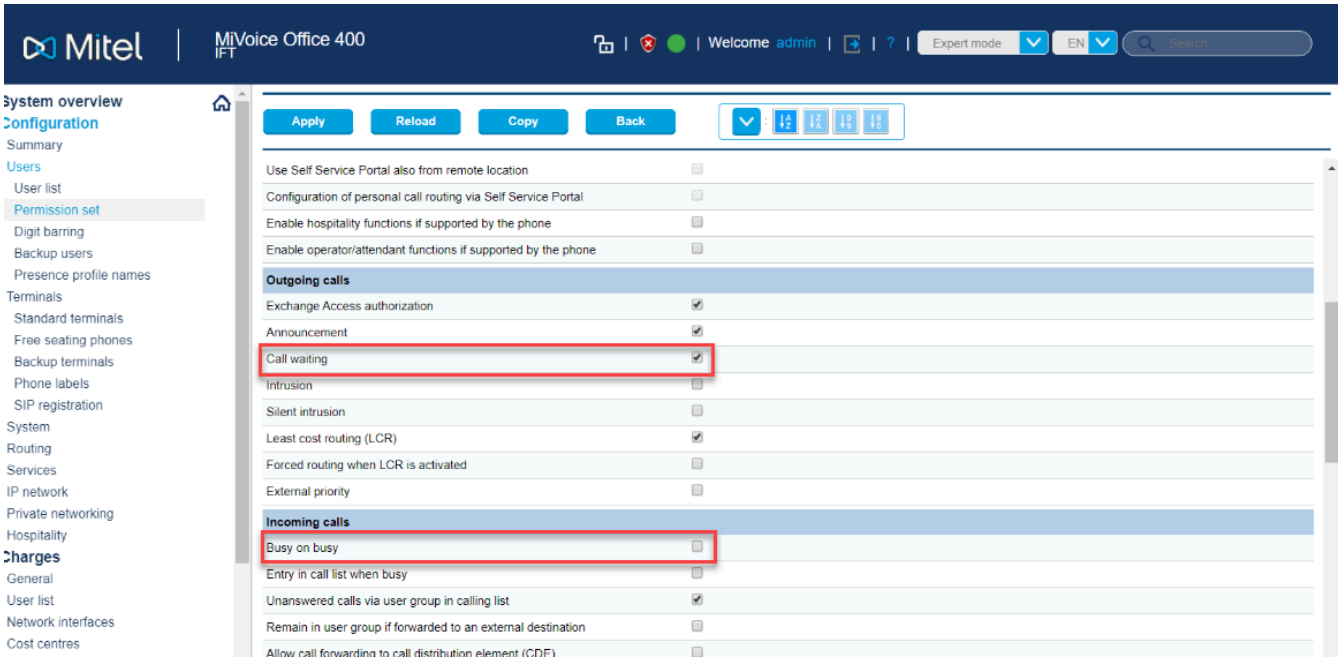
To configure these settings, proceed as follows:

1. Navigate to **Configuration** > **Terminals** > **Standard Terminals**.
2. Set the value to 3 in the **Multi lines** field under the **Further settings** section.



3. Click **Apply** to save the changes.
4. Navigate to **Users** > **Permission Set**.
5. Click the required permission set from the list. A panel opens.
6. Under **Outgoing calls**, select the check box beside **Call waiting** to enable it.

7. Under **Incoming calls**, clear the check box beside **Busy on busy** to disable it.



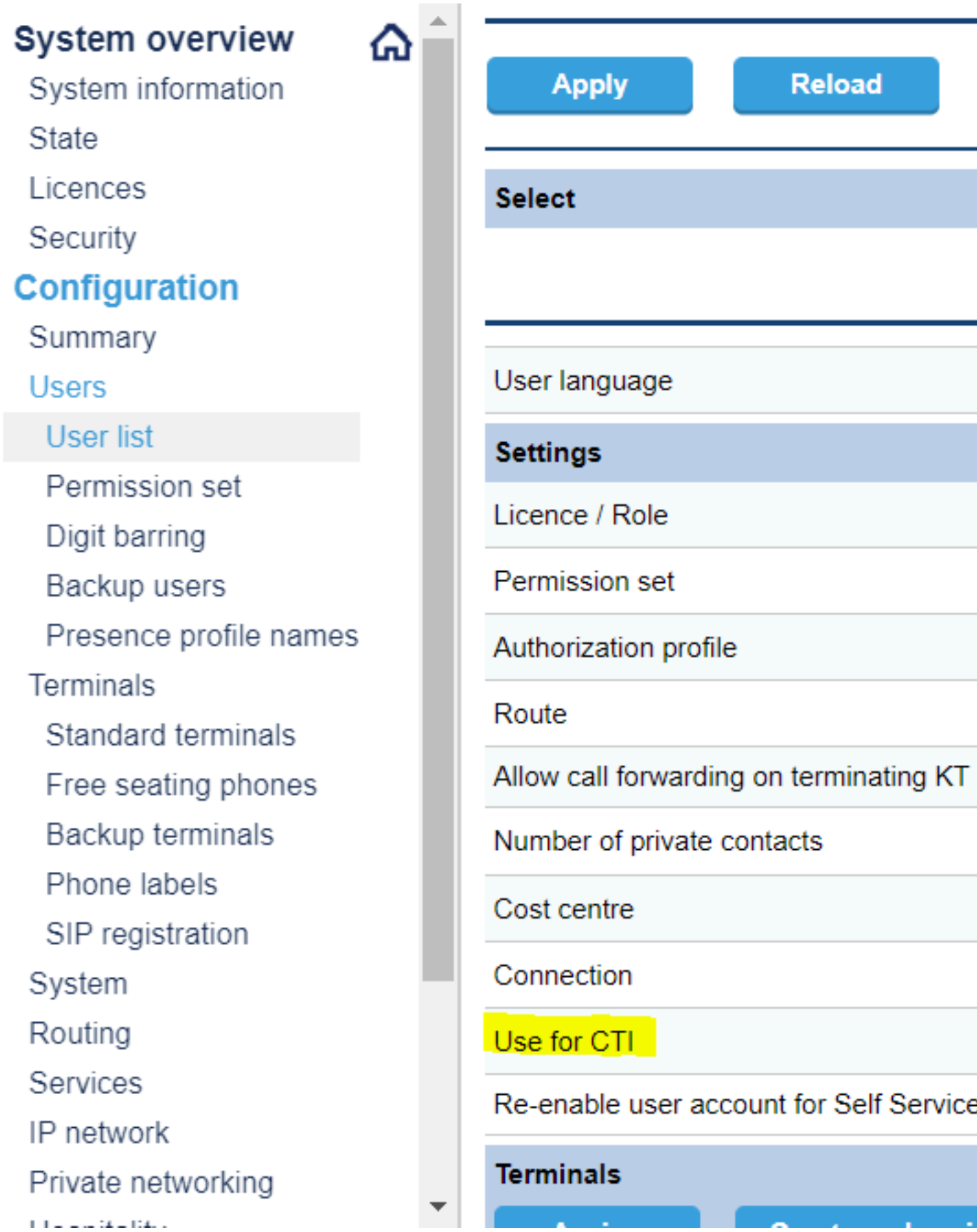
8. Click **Apply** to save the changes.

Enable CTI Service

To control the call features on a user's deskphone using the Mitel One Web Application, you must enable Computer Telephony Integration (CTI) service on the deskphone associated with the user's Mitel CloudLink account. To enable this setting, the user must have a functioning MiVO400 deskphone and verified the extension number indicated in the Mitel CloudLink account.

To enable CTI service on the deskphone, proceed as follows:

1. Navigate to **Configuration** > **Users** > **User list**.
2. Select the user whose deskphone you need to configure. The User page opens.
3. In the **Settings** section, click the drop-down list associated with the **Use for CTI** option and choose the deskphone associated with the user's Mitel CloudLink account.
4. Click **Apply** to save the changes.

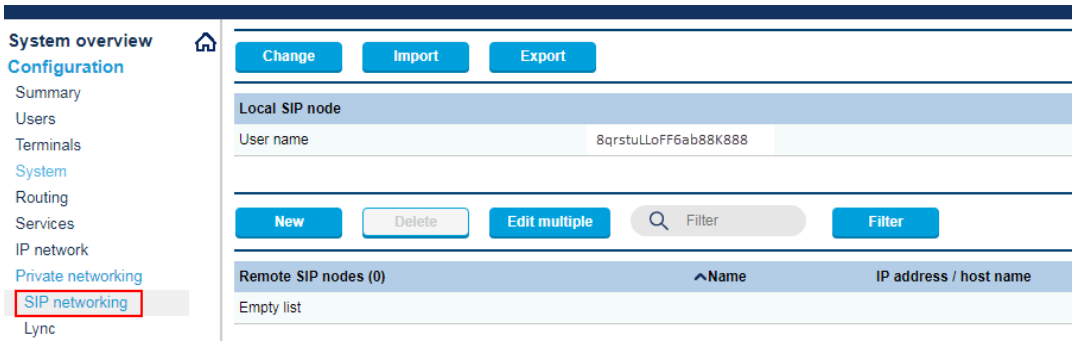

System overview
System information
State
Licences
Security
Configuration
Summary
Users
User list
Permission set
Digit barring
Backup users
Presence profile names
Terminals
Standard terminals
Free seating phones
Backup terminals
Phone labels
SIP registration
System
Routing
Services
IP network
Private networking
Apply
Reload
Select
User language
Settings
Licence / Role
Permission set
Authorization profile
Route
Allow call forwarding on terminating KT
Number of private contacts
Cost centre
Connection
Use for CTI
Re-enable user account for Self Service
Terminals

Onboard Customer

The next step of the integration process is to complete the Onboard Customers steps. When onboarding is completed, updates to the MiVoice Office 400 are completed automatically. Return to this page to continue with the next section below.

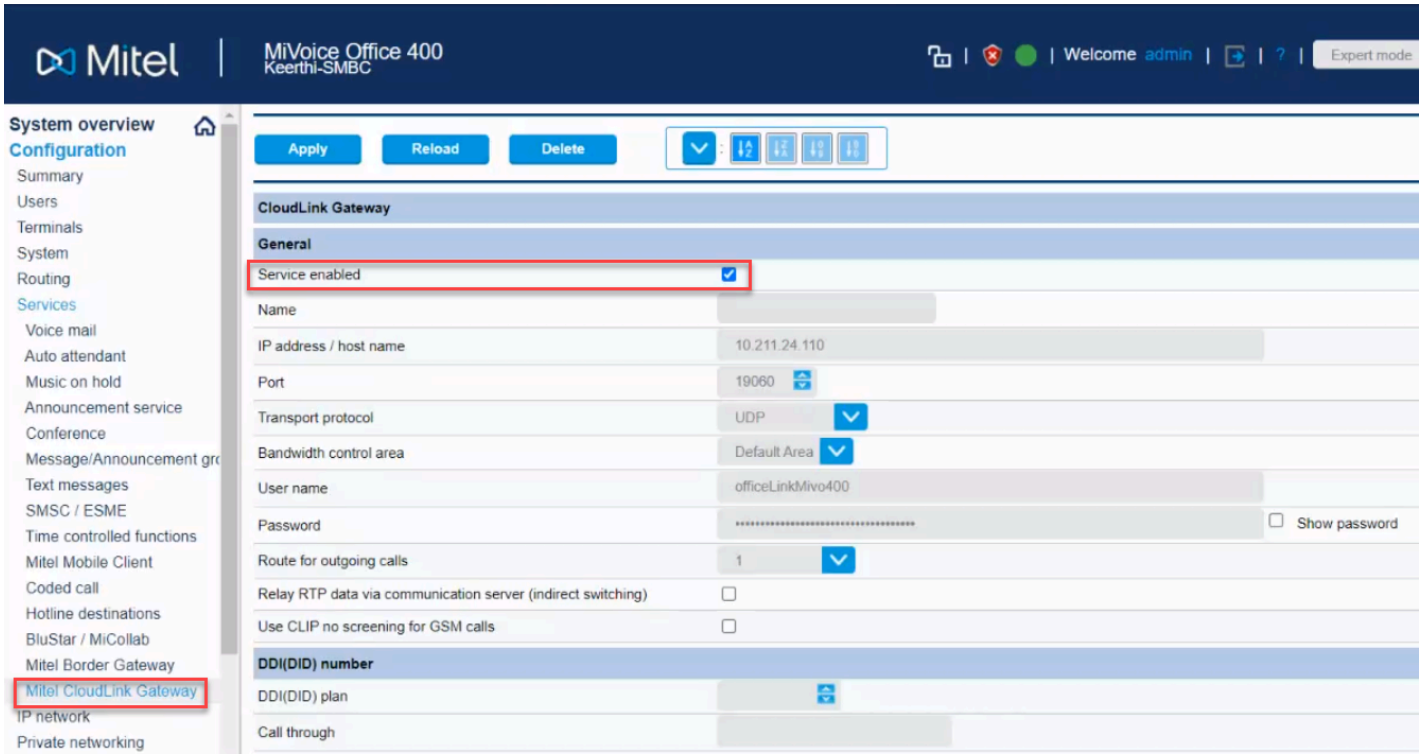
Verify SIP Networking

For SIP networking, a **Local SIP node** user is automatically created. To verify this, navigate to **Configuration** > **Private networking** > **SIP networking** and ensure that a user name was created under **Local SIP node** as shown below.



Verify Mitel CloudLink Gateway Service

To verify service, navigate to **Configuration** > **Services** > **Mitel CloudLink Gateway** and ensure that the check box next to the Service enabled field is selected as shown below.

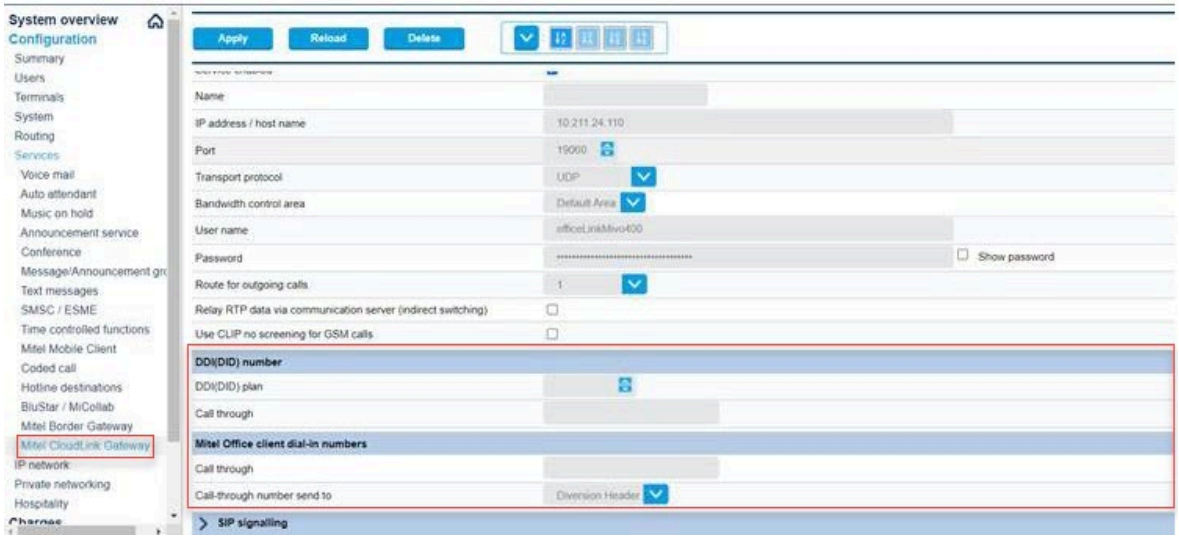


Configure GSM Call Through Feature

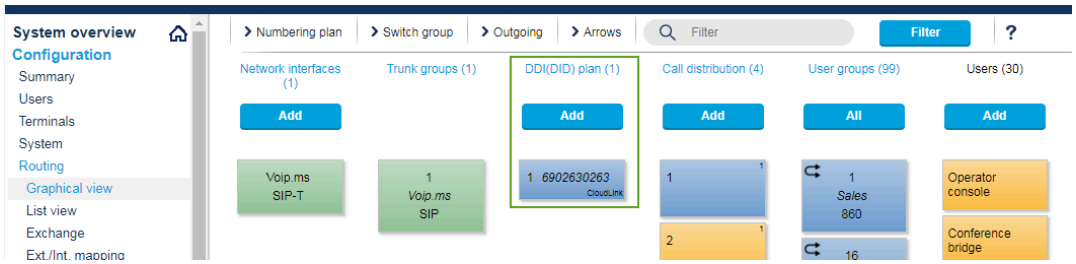
The MiVoice Office 400 PBX needs to be configured as explained below to support the GSM **Call through** feature for CloudLink applications.

1. Navigate to **Configuration** > **Services** > **Mitel CloudLink Gateway**.
2. Under the **DDI (DID) number** heading, select the used **DDI (DID) plan** and an unused DDI in **Call through** number.
3. Under the **Mitel Office client dial-in numbers** heading, set the full dialable **Call through** number.

> **Note**:
> The Call through number under the **Mitel Office client dial-in numbers** heading must be configured in the E.164 format.

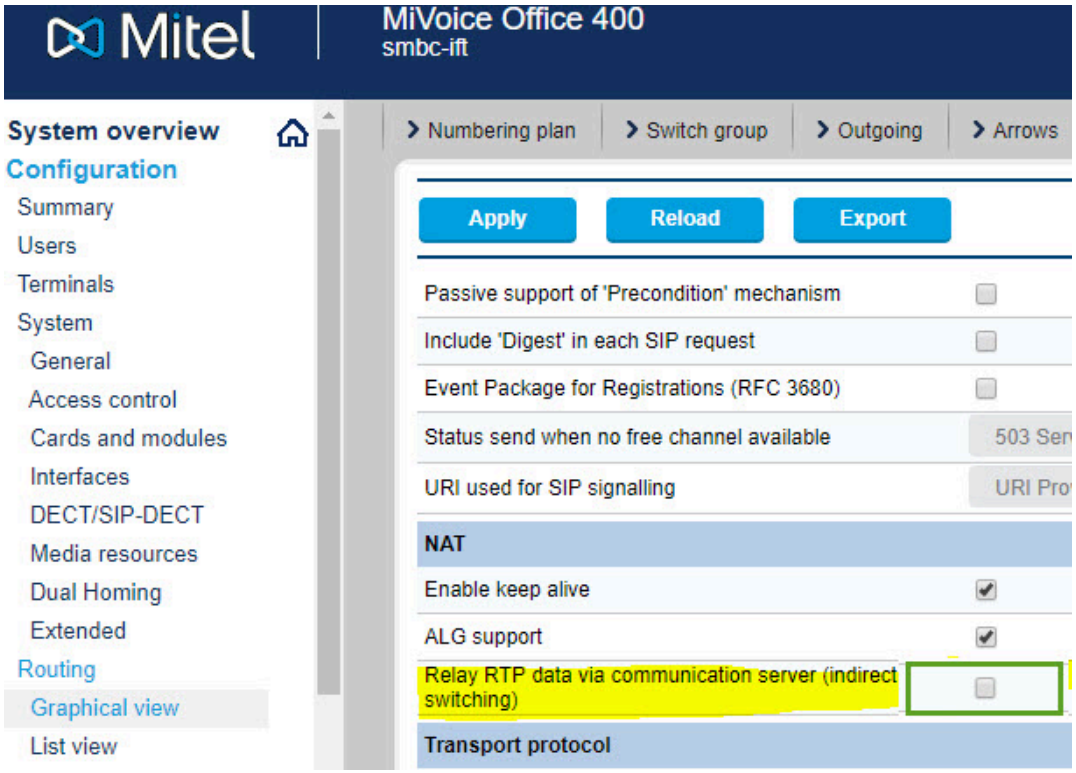


4. To verify the DDI (DID) number that was created above, navigate to **Configuration** > **Routing** > **Graphical view** to confirm that the correct number appears under the DDI (DID) plan heading shown below.

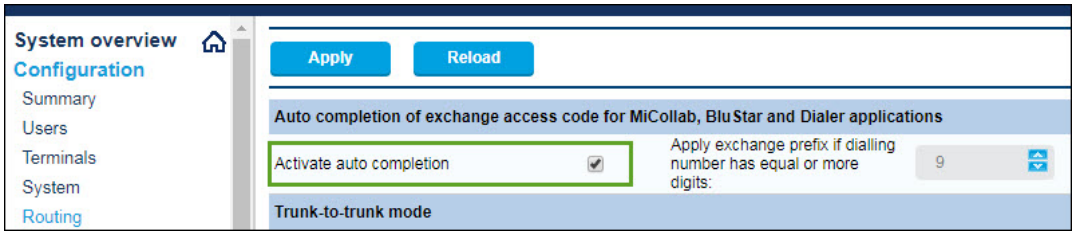


5. If the GSM Call Through feature uses SIP trunk access, the **Relay RTP data via communication server (indirect switching)** setting is disabled (not selected) by default for the trunk interface.
   If incoming GSM calls cannot be received, it might be due to a firewall configuration issue. Data addressed with the ports 65336-65534 / udp (rtp) should be forwarded to the CloudLink Gateway IP address.Alternatively, RTP relay must be enabled: navigate to **Configuration** > **Routing** > **List View**

> **Network Interfaces**, and in the NAT section of the interface, select the check box **Relay RTP data via communication server (indirect switching)**. Note that enabling RTP relay requires more VoIP channels.



6. If your MiVoice Office 400 PBX is configured to use exchange access codes for other Mitel applications, the **Activate auto completion** setting shown below must be selected. To do this, navigate to **Configuration** > **Routing** > **Exchange** > **General** and select the **Activate auto completion** check box in the **Auto completion of exchange access code...** section.



5.2 Configure MiVoice Office 400 on SMBC Platform

This topic explains how to configure a MiVoice Office 400 PBX on an SMBC platform (with embedded Gateway) to integrate with CloudLink. For detailed PBX instructions, see the MiVoice Office 400 technical documentation.

Use the instructions in the sections below in this specific order to ensure that your MiVoice Office 400 is correctly integrated with CloudLink. Leave all other settings (not specifically mentioned in these sections) set to the default value.

1. Add CloudLink App Users

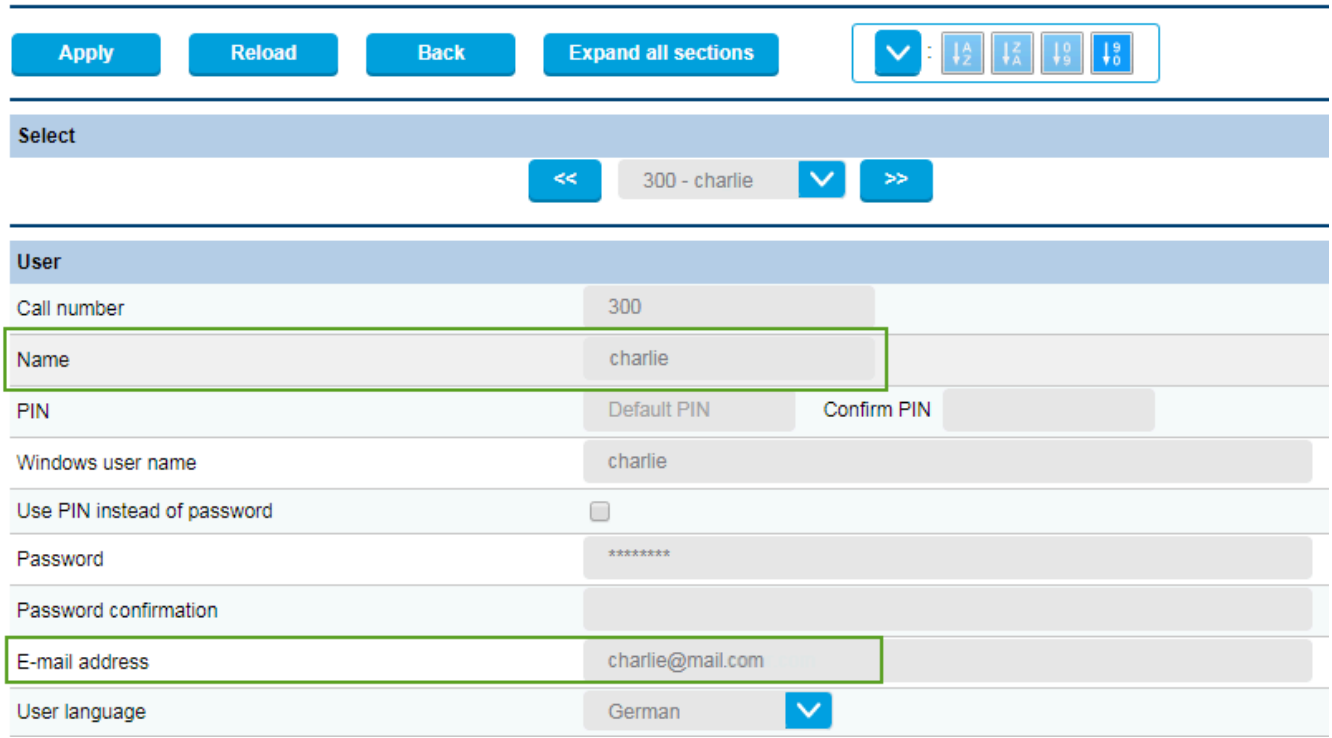
2. Install Mitel CloudLink Gateway Application
3. Access Application Configuration Link
4. Onboard Customers
5. Verify CloudLink SMBC
6. Verify CSTA Service
7. Verify SIP Networking
8. Verify Mitel CloudLink Gateway Service
9. Configure GSM Call Through Feature

Add CloudLink App Users

The MiVoice Office 400 PBX needs to be programmed to add all of the users who will be able to access CloudLink applications like the Mitel One application.

To create a user:

1. Navigate to **Configuration** > **Users**
2. Enter the following required information for each user of the Mitel One application:
   - **Name**
   - **E-mail address**
3. Click **Apply**. Users will be propagated through push notifications to the CloudLink Platform.



Note:
When users register their Mitel One application for the first time, the MiVoice Office softphone terminal is created and assigned to those users on the MiVoice Office 400 PBX.

To log in to the Mitel One application, a user must have a valid:

- MiVoice 400 Software Assurance (SWA) license from Mitel
- MiVoice Office softphone terminal license in the MiVoice 400 PBX.

If the user does not have these two licenses or if these licenses have expired, a **No License Available** alert appears when the user attempts to log in to the Mitel One application and the user will not be able to log in. The user must then obtain new licenses or renew the existing licenses to continue using the Mitel One application.

To edit the email address of a user:

1. Navigate to **Configuration** > **Users**.
2. Enter the new email of the user in the **E-mail address** field.
3. Click **Apply** to save the changes.
4. Sync the MiVO 400 PBX with the CloudLink Gateway for the changes to reflect in the CloudLink Platform.

Install Mitel CloudLink Gateway Application

Install the Mitel CloudLink Gateway application software using the SMB Controller Manager admin console. The MiVO400 technical documentation provides detailed instructions for installing application files and configuring associated LED indicators in the SMB Controller Manager.

After this software is installed, you will see **Mitel CloudLink Gateway (Application configuration)** listed under **Currently Installed applications** in the SMB Controller Manager.

Note:
The performance profile in use is displayed.

Access Application Configuration Link

To properly complete the customer onboarding, the first time the CloudLink Gateway Portal is accessed, it must be accessed from the SMB Controller Manager.

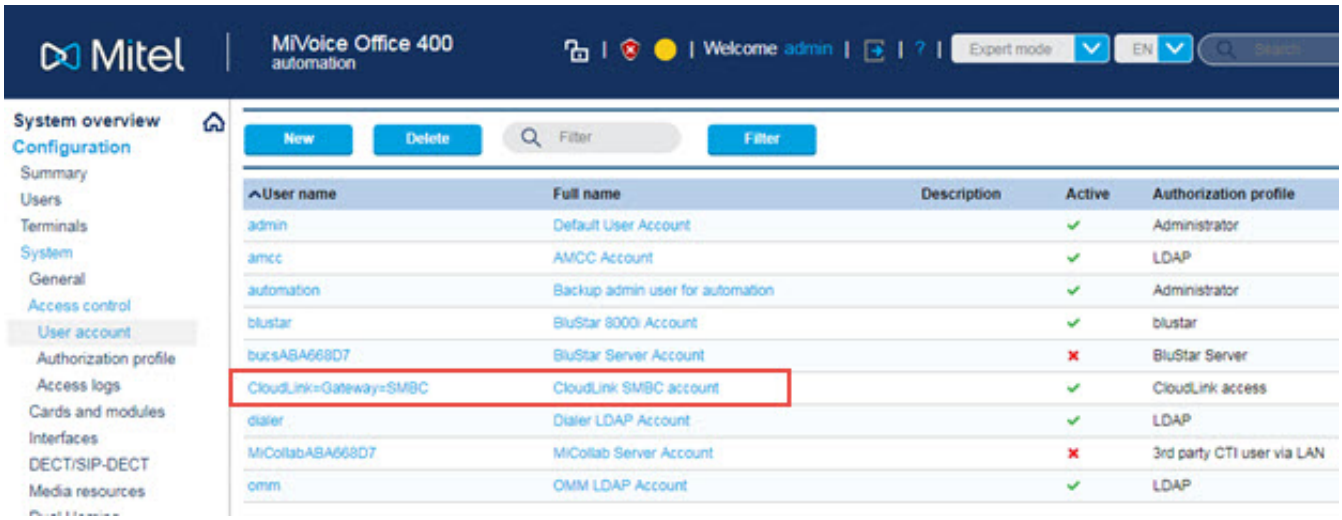
Navigate to **Software** > **Applications** and click the **Application configuration** link shown in the image above. After customer onboarding is completed, the CloudLink Gateway Portal can be accessed several different ways. For details, see Access the CloudLink Gateway.

Onboard Customer

The next step of the integration process is to complete the Onboard Customers steps. When onboarding is completed, updates to the MiVO400 are completed automatically. Return to this page to continue with the next section below.

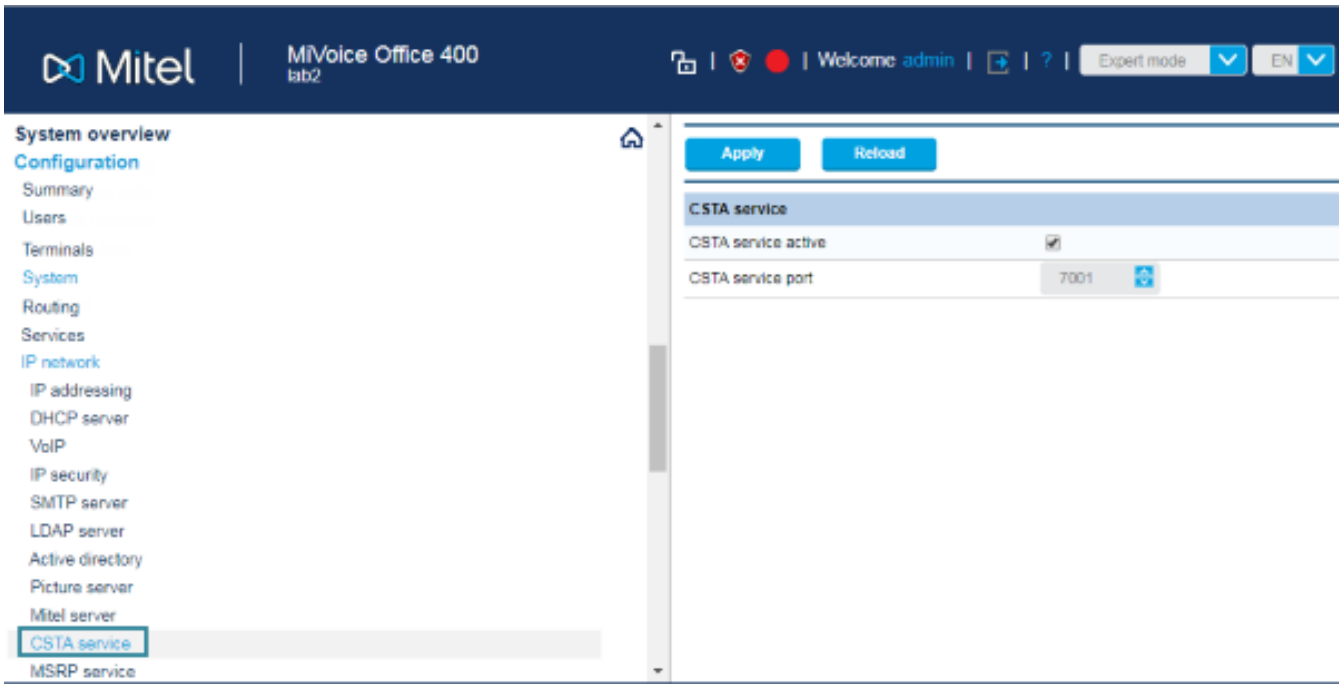
Verify CloudLink SMBC/VA Account

A user name is automatically created and configured as part of the Mitel CloudLink Gateway application installation. To verify that a user name was set to **CloudLink=Gateway=SMBC** (**CloudLink=Gateway** for VA platform) as shown below, navigate to **Configuration** > **System** > **Access control** > **User account**.



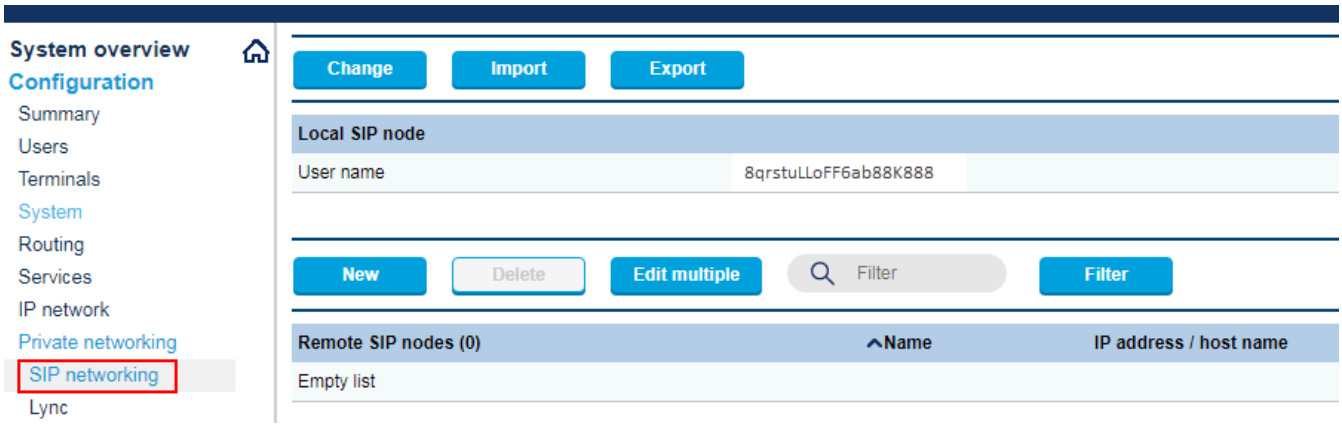
Verify CSTA Service

The CSTA (computer-supported telecommunications applications) service is automatically enabled and set to port 7001 by default. To verify this, navigate to **Configuration** > **IP network** > **CSTA service** and ensure the check box is selected next to **CSTA service active** as shown below.



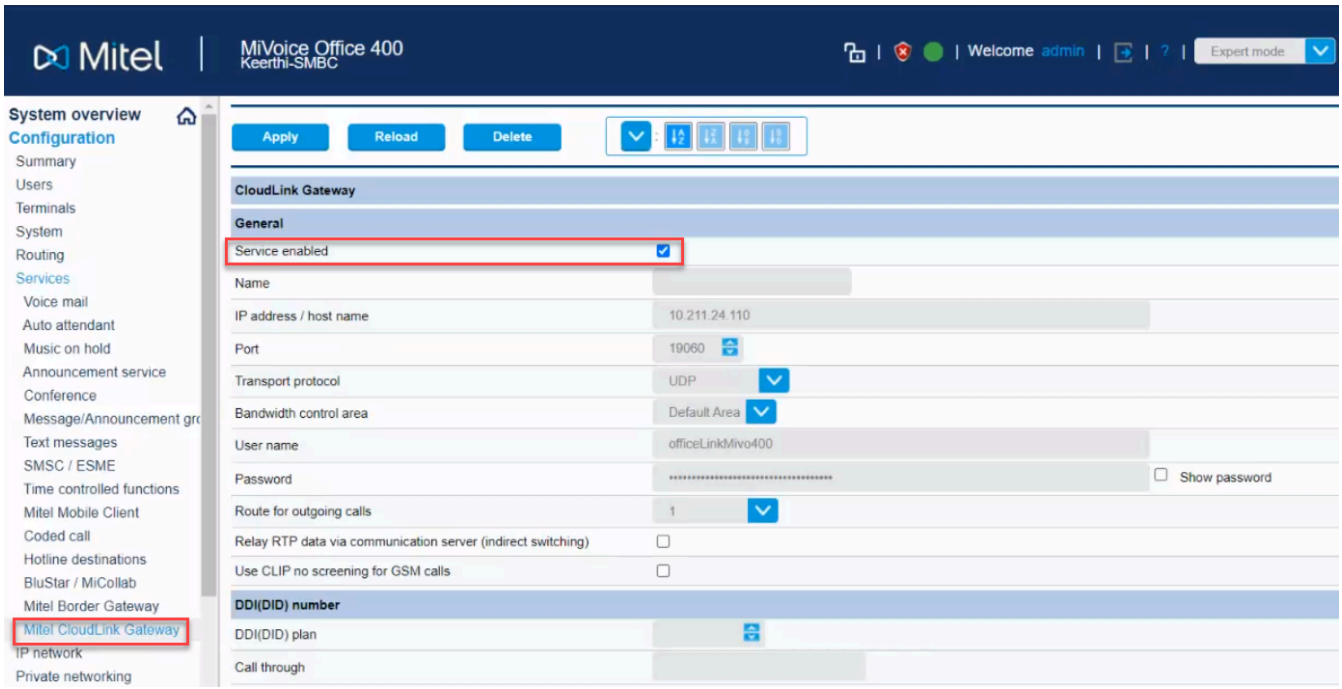
Verify SIP Networking

For SIP networking, a **Local SIP node** user is automatically created. To verify this, navigate to **Configuration** > **Private networking** > **SIP networking** and ensure that a user name was created under **Local SIP node** as shown below.



Verify Mitel CloudLink Gateway Service

To verify service, navigate to **Configuration** > **Services** > **Mitel CloudLink Gateway** and ensure that the check box next to the **Service enabled** field is selected as shown below.

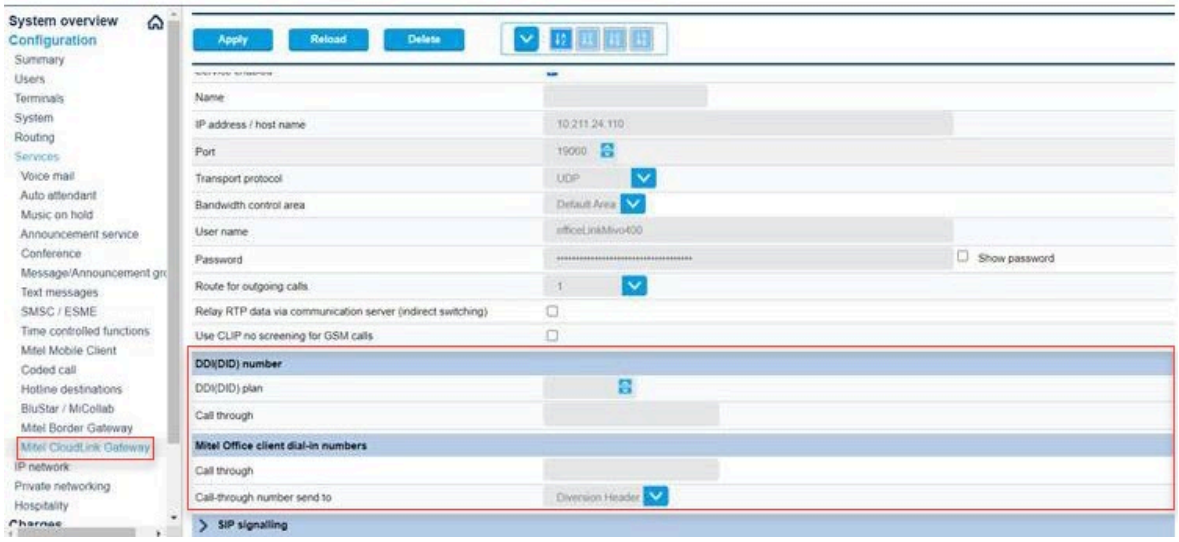


Configure GSM Call Through Feature

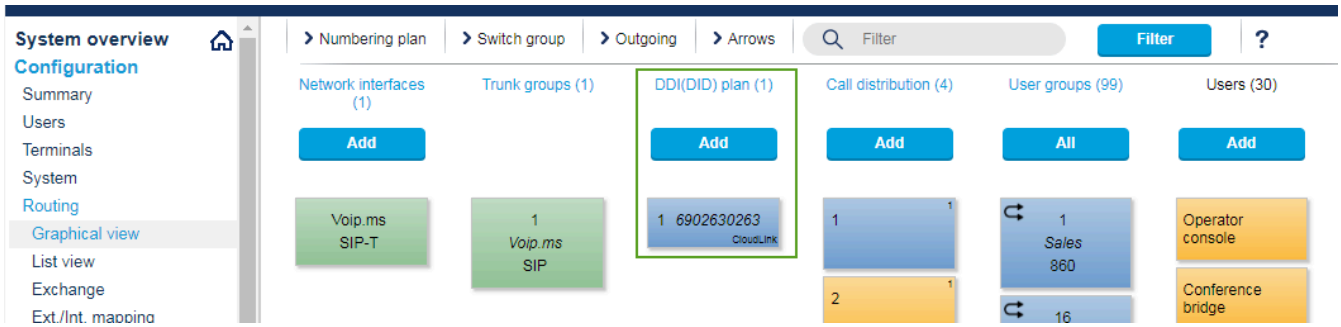
The MiVoice Office 400 PBX needs to be configured as explained below to support the GSM "Call through" feature for your CloudLink applications.

1. Navigate to **Configuration** > **Services** > **Mitel CloudLink Gateway**.
2. Under the **DDI (DID) number** heading, select the used **DDI (DID) plan** and an unused DDI in **Call through** number.
3. Under the **Mitel Office client dial-in numbers** heading, set the full dialable **Call through** number.

Note:
The Call through number under the **Mitel Office client dial-in numbers** heading must be configured in the E.164 format.

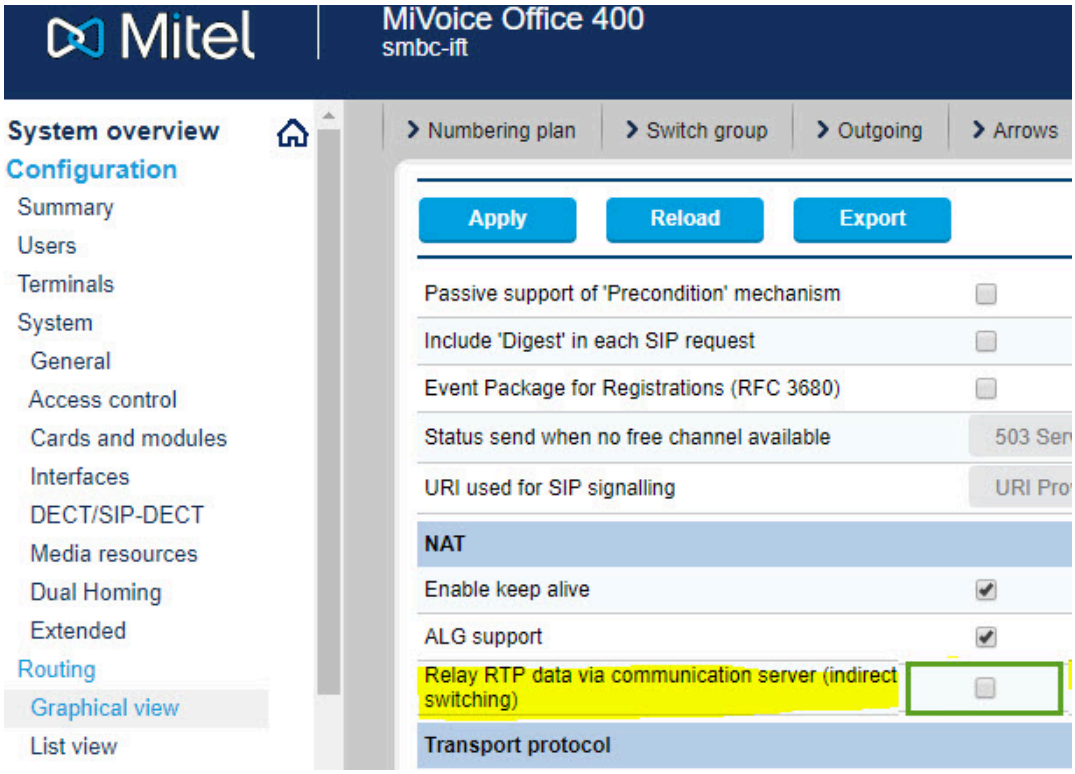


4. To verify the DDI (DID) number that was created above, navigate to **Configuration** > **Routing** > **Graphical view** to confirm that the correct number appears under the DDI (DID) plan heading shown below.

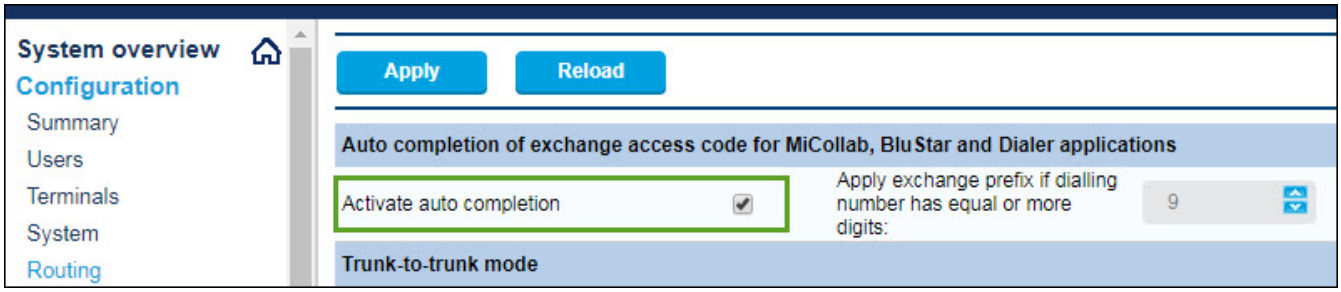


5. The **Relay RTP data via communication server (indirect switching)** setting is disabled by default (not selected). If this setting is enabled for any reason, incoming GSM calls will not be received. To prevent or resolve this issue, navigate to **Configuration** > **Routing** > **List View** > **Network Interfaces**

and in the **NAT** section of the interface, ensure that the **Relay RTP data via communication server (indirect switching)** check box is not selected.



6. To enable placing a call without adding the external prefix, you must select the **Activate auto completion** option and enter the number of digits valid for your configuration. To do this, navigate to **Configuration** > **Routing** > **Exchange** > **General** and select the **Activate auto completion** check box in the **Auto completion of exchange access code...** section.



5.3 Configure MiVoice Office 400 on Virtual Appliance

This topic explains how to configure a MiVoice Office 400 PBX on a Virtual Appliance (VA) (VMware or Hyper-V) (with embedded Gateway) to integrate with CloudLink. For detailed PBX instructions see, MiVoice Office 400 technical documentation.

Use the instructions in the sections below in this specific order to ensure that your MiVoice Office 400 is correctly integrated with CloudLink. Leave all other settings (not specifically mentioned in these sections) set to the default value.

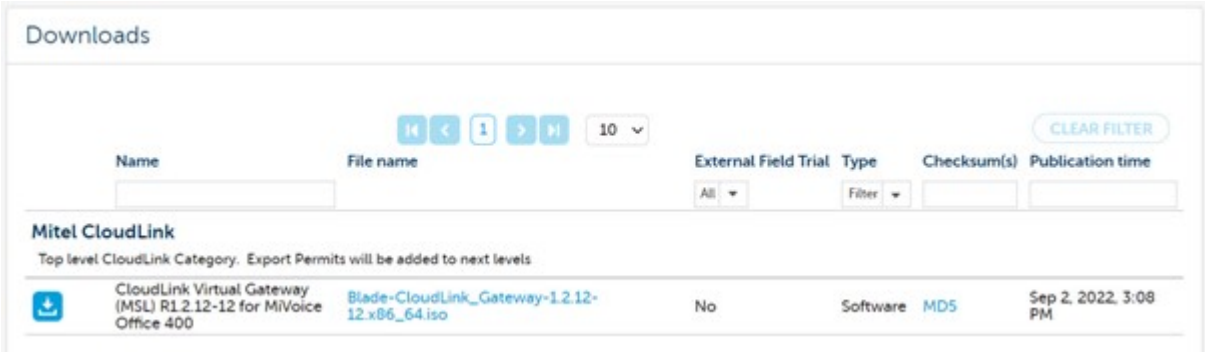
1. Add CloudLink App Users on page 94
2. Install CloudLink Gateway Application on page 101
3. Configure CloudLink Gateway
4. Access Application Configuration Link on page 96
5. Onboard Customer on page 96
6. Verify CloudLink SMBC/VA Account on page 96
7. Verify CSTA Service on page 96
8. Verify SIP Networking on page 97
9. Verify Mitel CloudLink Gateway Service on page 97
10. Configure GSM Call Through Feature on page 98

Install CloudLink Gateway Application

Install the CloudLink Gateway application using MSL Server-Manager.

Note:
Ensure that the Virtual Machine has at least two CPU cores assigned.

1. Download the ISO file from MiAccess Portal under **Software Download Center** option.



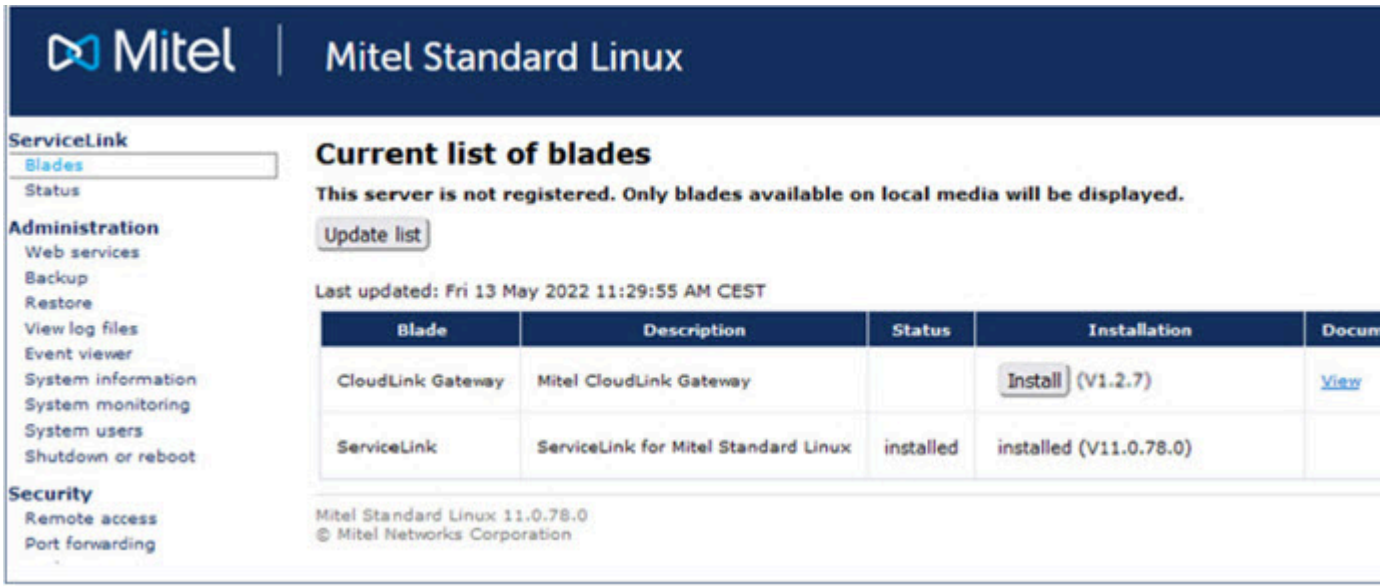
2. Copy the ISO file to the storage of your hypervisor (VMware or HyperV).

Note:
It is recommended that the **Connect at power on** settings is on. If the **Connect at power on** is not on, the admin must mount the virtual CD/DVD drive in order to display the ISO file in MSL Server-Manager.

3. Browse to MSL Server-Manager (https://<IP-Address>:8443).

4. Log in by entering *admin* as User name and *admin-password* as password.

   The Mitel Standard Linux window is displayed.



5. Navigate to **ServiceLink** > **Blades**.

   CloudLink Gateway is displayed in the table.
6. Click **Install** and accept the licence agreement.
7. Remove CD-ROM ISO-image.
8. Click **Clear this report**.

   The CloudLink Gateway downloads the required components from the cloud in the background.

Configure CloudLink Gateway

1. In the MSL Server-Manager, navigate to **Applications** > **CloudLink Gateway**.
2. Click **CloudLink portal**.

   You are redirected to the CloudLink portal.

   For more information about onboarding customers see, Onboard Customers Using Navigation Bar or a Single Page on page 59.

Note:
To restart CloudLink Gateway, you must click **Restart CloudLink Gateway**.

Configure a MiVoice Business PBX 6

This chapter contains the following sections:

The following topics contains information about how to install, deploy, integrate, and govern call processing behaviors for CloudLink solution with existing MiVoice Business solution.

6.1 Prerequisites for MiVoice Business

This section section provides details about the prerequisites to configure MiVoice Business with CloudLink.

6.1.1 System Requirements

There are no new MiVoice Business (MiVB) Licenses related to CloudLink Onboarding, nor has the MiVB licensing model changed. Although CloudLink, MiVoice Business, and MiVoice Border Gateway use SIP trunks for the integration, SIP Trunk licenses are not consumed for this integration.

Partners must have Software Assurance (SWA) to have access to the CloudLink API program.

Refer to the *MiVoice Border Gateway release 11.4 or later version Engineering Guideline* documentation for the latest VMware, Azure and CloudLink Gateway guidelines - including CloudLink Gateway resource impacts bandwidth requirements and system size - as well as impacts to MiVoice Border Gateway usability.

6.1.2 Network Requirements

This section provides details of the network connections required between CloudLink Gateway and MiVoice Business. You must ensure that the ports on MiVoice Business are reserved for operational use for the CloudLink Gateway and that the connections are routed properly through the corporate network.

For more information about the network connections required between CloudLink Gateway and MiVoice Business, see the following sections in the *CloudLink Gateway User Guide*:

- Configuration Prerequisites
- Network View
- Connections Between the CloudLink GW and PBX/Call Server > MiVoice Business Considerations

6.1.3 System Capacities

The following requirements and capacities are based on a MiVoice Business with CloudLink solution involving MiVoice Border Gateway and MiCollab.

- The solution currently supports a virtual (VMWare or Azure) or SMB Controller deployment that includes MiVoice Border Gateway paired with a CloudLink Gateway.
- If the MiVoice Business system is using a Mitel self-signed certificate, then no certificate is required to be uploaded in the Mitel Administration Portal at the time of onboarding.
- Support for up to 2500 users and 5000 devices on a standalone or resilient virtual MiVoice Business deployment. This implies a maximum of 2500 users with 3 devices, or 1666 users with 3 devices, and so on.
- (For SMBC only). Support for 150 UC users on a standalone or resilient MiVoice Business deployment. The UC user supports from 1 to 3 devices plus one hot-desk number, allowing up to 450 registered devices.
- The CloudLink Gateway uses Trunk Service 78 on the MiVB. If the MiVB database has been flexed to have less than 78 Trunk Service groups, then it will need to be re-flexed to have at least that many to allow the Gateway to use the Trunk Service 78.

Note:
Users on other MiVoice Business platforms are not onboarded by CloudLink.

- Single MBG or clustered MBGs
  - A single MBG is required to communicate with CloudLink Gateway. The MBG will continue to support the same feature set it does today for SIP trunking and PBX devices. If the customer deployment is small enough and MBG resiliency not required, the solution might be deployed using one MBG.
    - The resources required to deploy CloudLink Gateway on MBG depend on the MBG resources required for MBG functionality (that is, Teleworker devices, SIP trunking, call recording, and so on.) and an additional 1 GB of RAM and 1 vCPU for the CloudLink Gateway.
  - Additional MBGs can be deployed, each on a different virtual machine, and clustered to provide resiliency and scaling for non-CloudLink devices. But the additional MBGs will not communicate with the CloudLink Gateway. The CloudLink Gateway will communicate only with the MSL\MBG it is deployed on.
- MiCollab is not required to be part of the solution, but it is expected to be present in most cases because of MiCollab still being the primary UC application.

Note:
MiCollab has an embedded MBG. MBG running on MiCollab and the MBG running CloudLink Gateway must be running the same version. See the *MiCollab and/or MBG training material or documentation* for details.

- The CloudLink solution is primarily an enabler for development of third-party CTI applications on the CloudLink Platform. CloudLink APIs support:
  - Call, Answer, Clear/Release, Hold/Retrieve, Consultation Hold, and Transfer
  - Call History
  - Basic Voice Mail (currently, no support for Visual Voice Mail). Message Waiting Indicator and click-to-call voice mail (to retrieve messages). Support includes EMEM, NuPoint Messaging, and MiCollab Advanced Messaging (MiCAM).

- Engineering guidelines such as the number of users supported is provided in the documentation. As enhancements are expected to Mitel PBX/CloudLink solutions, check the Mitel Documentation Center and Release Notes for new updates.
- For a user to be successfully imported from MiVoice Business into CloudLink, the following user details are required:
  - Email Address
  - Extension Number
  - First or Last Name

As a high-level recommendation for Administrators, observe the following guidelines for MiVB, MiCollab, and MBG:

- Administrators should be familiar with MiVB and MBG (recommend MiVB and MBG training certification) before making any changes to the MiVB or MBG. Mitel Product Support assists only technicians who are certified on the product/solution.

Note:
If MiCollab is part of the solution, it is recommended that the Administrators of the solution be certified on MiCollab.

- It is assumed that the MiVoice Business is already set up for the users, along with the required call flows, before the CloudLink Gateway is installed and configured.
- This document does not include information on CloudLink Applications and does not focus on CloudLink Onboarding. After an Administrator has successfully integrated a CloudLink Application to the Customer Account on CloudLink and applied services to the users, this service might require users to have a license in CloudLink. This information is available in the CloudLink Application training or documentation.
- Connectivity (SIP Trunk) between the MiVoice Business and MBG, and a SIP Trunk between MBG and the CloudLink Platform will automatically be set up from CloudLink during the synchronization step discussed in the next section. As indicated in the System Requirements section, licenses for connections to CloudLink do not need to pre-exist.

Note:

- CloudLink recognizes a user on MiVoice Business only if the user has valid Email Address, Last Name, and Directory Number. If any of these values are not present, the user will not be onboarded.
- CloudLink will onboard only CloudLink Services and it is not responsible for the configuration of other user services or endpoints (that is, MiNet or SIP sets or EHDUs).
- .For initial onboarding of CloudLink Gateway connections to the CloudLink Platform, Administrators of the CloudLink Gateway on MSL must use the CloudLink Portal button to connect to the CloudLink Platform and complete CloudLink Gateway Integrations.

6.1.4 CloudLink Solution Prerequisites

Following are the prerequisites that must be ensured before deploying CloudLink Solution to the users.

- MiVoice Business PBX Release 9.4 or later.
- MiVoice Border Gateway Release 11.4 or later
- MiCollab (not a prerequisite). However, if there is a requirement to have an MBG cluster with the MBG/MSL containing the CloudLink Gateway, the MBG software versions within MiCollab and on MBG servers must be the same software version (that is, MBG Release 11.4 or later) as per existing engineering guidelines.
- CloudLink enablement requires current Software Assurance (SWA) and End User licensing as indicated in the System Requirements section.

Note:

Software Assurance is a requirement for CloudLink and CloudLink Applications. Expiring Software Assurance may result in CloudLink features being denied. Please consult the following link.

6.1.5 CloudLink Gateway Prerequisites

The following are the prerequisites for CloudLink Gateway:

- An Internet connection that provides enough bandwidth.
- A DNS server that the CloudLink Gateway uses to resolve domain names.
- An Ethernet connection to the LAN.
- Passwords to be entered during the MiVoice Business configuration.
- Mitel MiAccess account.
- Ports: CloudLink Gateway requires certain ports to be accessible to communicate with the MiVoice Business. For information about these ports, see Connections Between the CloudLink GW and PBX/Call Server > MiVoice Business Considerations.

6.2 Deploying the CloudLink Gateway

For additional information about the topics in this chapter, see the Mitel Administration User Guide (mitel.com) on the Mitel website.

To configure the CloudlLink telephones

1. Integrate CloudLink Gateway with the ClouldLink Customer account. See the section Integrating CloudLink Gateway with Mitel Administration in Mitel Administration User Guide (mitel.com) for more information.
2. Send welcome emails to the users in the customer account. See the section Managing Users in Mitel Administration User Guide (mitel.com) for more information.

3. Enable the MiNet Teleworker Devices in the MiVoice Border Gateway server manager application and connect the device to the primary configured ICP. See the section Add or Edit MiNet Devices in the MiVoice Border Gateway Online Help for more information.

Deployment Strategy

CloudLink will be integrated with both new and existing customers. The following strategy outlines and simplifies the deployment scenarios:

1. The CloudLink solution will not be integrated until the customer has fully deployed the rest of their MiVB solution, which might include MiCollab. “Fully deployed” infers that the site is fully licensed (MiVB, MBG, and MiCollab (if applicable)) and users are configured with functioning phones. This gives CloudLink a deterministic solution in which to integrate.

> **Note**:
> For existing customer sites with MiCollab, MiCollab might already be integrated with CloudLink. For the same Customer Account on CloudLink, you must integrate MiVoice Business with CloudLink Gateway.

2. If a customer already has an MBG in the solution through MiCollab or standalone, there will be no attempt to integrate it with the MBG packaged with CloudLink Gateway. The existing MBG will continue to support the solution as it already does (that is, Teleworker) and a new MBG with CloudLink Gateway will be used for CloudLink-specific activities related to the CloudLink SIP Trunk.
3. CloudLink is solely responsible for the provisioning and management of CloudLink services. All other solution provisioning and management is done in the same manner as with any other MiVoice Business Solution. More specifically, MiCollab would continue to manage the user as a whole and all their other non-CloudLink devices.

Collecting CloudLink Gateway Logs

Installing Virtual Machine CloudLink Gateway

The gateway logs are collected as a part of an SOS report. If you discover connection issues while deploying CloudLink Gateway blade, collect the gateway logs. Perform the following steps to collect the gateway logs:

1. Open MSL server manager.
2. Navigate to **Administration** > **View Log Files**.
3. Check in the section *Collect log files & diagnostic data* contains an entity for the CloudLink gateway and the checkbox is selected (it should be enabled by default). Then click **Start** to create SOS package.
4. Once the SOS package is created, download the package.
5. Check the downloaded tarball contains files from */var/clgw* and */var/log/clgw*. If it does not then check step number 3.
6. You can investigate the issue using plain text logs. For further assistance, share the logs as per your standard support process.

The CloudLink Gateway software will be available as a blade on MSL when MiVoice Border Gateway (MBG Release 11.4 or later) is installed.

Note:
The Partner/Customer can choose whether or not the CloudLink Gateway will be installed.

6.3 Configure MiVoice Business

You can configure MiVoice Business on the following hardware platforms:

- Mitel 3300 ICP controllers, including MXe III, MXe III-L, CX II, CXi II,
- Mitel EX Controller
- Mitel SMB Controller
- Industry standard servers (x64 Intel based)
- VMware® vSphere™ and Microsoft® Hyper V™ virtualization platforms
- Public Cloud services as virtual servers including Microsoft Azure and Amazon Web Services (AWS)

For information about configuring MiVoice Business using various platforms, see the following sections in the latest *System Administration Tool Online Help* located at Mitel Doc Center:

- *Initial Configuration*
- *Programming an AX Controller*
- *Programming a CX II/CXi II/MXe III Controller*
- *Programming an EX Controller*
- *Programming a SMB Controller*

Note:
For detailed information about configuring MiVoice Business on EX Controller and SMB Controller platforms see the *MiVoice Business EX Controller Installation and Administration Guide* and *MiVoice Business - System Manual for Mitel SMB Controller* documents located

at Mitel Doc Center..

Configure a MiVoice MX-ONE PBX 7

The following topics contains information about how to install, deploy, integrate, and govern call processing behaviors for CloudLink solution with existing MiVoice MX-ONE solution.

Configure a MiVoice Office 5000 PBX 8

To access the *CloudLink - Deployment Guide with MiVoice 5000* guide, click https://www.mitel.com/document-center/technology/cloudlink/all-releases/en/cloudlink-deployment-guide-with-mivoice-5000.

Manage a Customer 9

This chapter contains the following sections:

The topics listed below provide instructions for managing your CloudLink customers.

- Edit a Customer
- Deactivate an Existing Customer
- Delete an Administrator

9.1 Edit a Customer

To keep your customers' accounts updated and accurate, you can edit their information and settings as needed.

To edit a customer:

1. Log into the Mitel Administration.
2. In the Partner Dashboard that opens, review the status messages in the customer list, which indicate what steps are required (if any) for each existing customer.
3. Click anywhere in the row of an existing customer to access that customer's account settings.
4. Make the required changes.
5. Click **Save**.

9.2 Deactivate an Existing Customer

To deactivate an existing customer:

1. Click the X at the far right of the customer in the Partner Dashboard.
2. To confirm that you want to deactivate the customer, type the word “deactivate” in the text box that appears.
3. Click **Deactivate**.

You can modify or delete an existing customer from the Partner Dashboard, which is the home page of the CloudLink Gateway Portal.

Customers who have already been deactivated are not displayed in the Partner Dashboard.

Reactivate a Deactivated Customer

To reactivate a previously deactivated customer, contact Mitel Partner Technical Support via a login at https://www.mitel.com/en-ca/login.

Customer Accounts and Account Admin

10

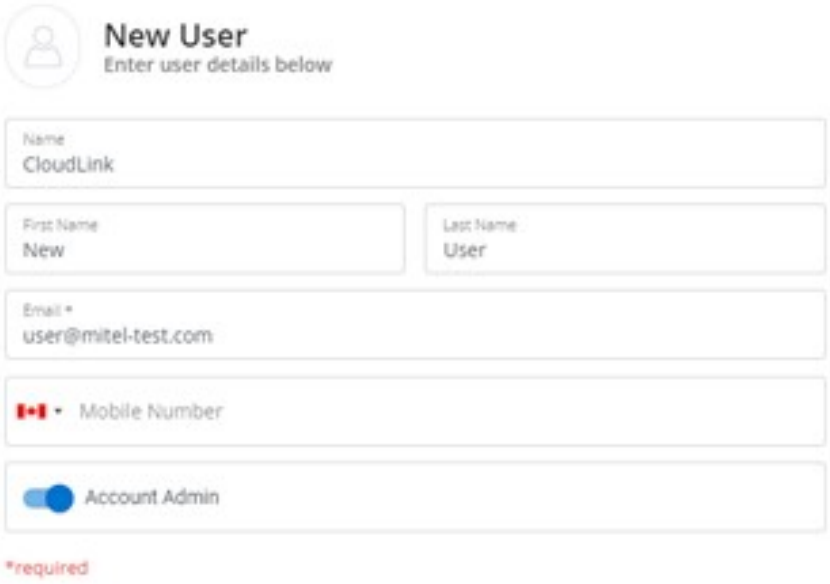
Customer Accounts

In CloudLink, a customer account is where the users for that account are added. All users in a specific customer account may interact with each other using a CloudLink application. For example, users who work for XYZ Company can use the Mitel One application to place and receive calls and chats to other users who also work for XYZ Company.

Account Admin

Administrative permissions can be enabled for an existing or a new user by sliding the toggle button to the right associated with **Account Admin**. The following images displays the **Account Admin** permission for:

- New user:



- Existing user:

When one of these users registers their account, they will receive advanced CloudLink applications permissions, which are not available to regular end users.

Note:
When you slide the toggle button associated with **Account Admin** to the left, the user only loses their advanced permissions (the user is not deleted from the account).

Troubleshoot Errors 11

Use the following table to troubleshoot issues and resolve problems you may encounter with the CloudLink Gateway and Mitel Administration.

Note:
A standalone platform with an external Gateway appliance requires a DHCP server on the LAN. If a DHCP server is not running, the Gateway appliance will be unable to obtain an IP address and will not function correctly.

Accessing the Gateway Appliance

Message (Issue)	Possible reason	Try this
Update Error on an SMBC platform (Problem with downloading an update to an embedded Gateway)	The Gateway might not be able to connect to https://download.mitel.io/.	An Administrator can apply the "Restart" command to the Mitel-CloudLink Gateway in the **Software** > **Applications screen** of the SMB Controller Manager admin console.
Unable to connect to CloudLink Gateway (http://cloudlink.local/ does not resolve)	No DHCP server or DHCP server failed to allocate an IP address.	Log in to the domain DHCP server and try to locate the CloudLink Gateway.
	Did not use the http:// prefix	Connect using an "http://" prefixed IP address (for example, http://192.168.0.1)
	Bonjour service not installed or working.	Uninstall and then reinstall Bonjour Print Services.
	Unsupported browser	Use a supported browser
Access Denied (You are not allowed to access this page on the Mitel MiAccess site)	The CloudLink 'policy' has not yet been assigned to you.	Contact the Mitel MiAccess Administrator in your organization to request this access.

Message (Issue)	Possible reason	Try this
Update Error on a standalone platform (Problem with downloading an update to an external Gateway) 	The Gateway might not be able to connect to https://download.mitel.io/. The Gateway may not be able to resolve https://download.mitel.io/.	Check firewall settings to see if outgoing 'https' access to https://download.mitel.io/ is permitted. Check DHCP configuration to check whether there is a DNS server provided to the Gateway. Ping download.mitel.io from a machine connected to the same LAN subnet as the Gateway. The Gateway Appliance Software Update on page 33 topic provides more information.
Lost Connection to Gateway (The connection to the Gateway appliance is not working)	Your browser is not able to communicate with the gateway.	Generally, this is a temporary condition encountered when key services are not running inside the Gateway. If this condition persists for an unusual length of time (more than 15 minutes) then reset the Gateway by pressing the **Recessed** button.
The update operation did not succeed (There was a problem with downloading an update to the Gateway)	Power outage	Ensure that the MiVoice 400 and the Gateway are always connected to a UPS.
Update Error (network not reachable) 	DNS or firewall issue	Ensure that the customer network including Firewall/ Gateway network is configured properly.

Message (Issue)	Possible reason	Try this
Get "https://download.mitel.io/compat.yaml?timestamp=1676355747592924443": dial tcp: lookup download.mitel.io on <dns-sever-ip>:53: read udp <gateway-ip>:<src-port> -><dns-sever-ip>:53: read: connection refused Get "https://download.mitel.io/compat.yaml?timestamp=1676357072469896898": dial tcp: lookup download.mitel.io on <dns-server-ip>:53: read udp <gateway-ip>:<src-port>-><dns-server-ip>:53: i/o timeout	The DNS server might be blocked by firewall or configured DNS server is incorrect.	Ensure that the DNS Server configuration on the Gateway and firewall is configuration is correct.
Get "https://download.mitel.io/compat.yaml?timestamp=1676356165676153908": dial tcp <ip-address>:443: connect: connection refused No Internet connectivity: host not reachable: mitel.io:443: dial tcp <ip-address>:443: i/o timeout	download.mitel.io might be block ed by firewall.	Ensure that the gateway has access to download.mitel.io.
CLGW_ALARM_CRITICAL_PHASE_FAILED	Power interruption when software update was in progress.	Power cycle the gateway. The system will attempt to reset to factory default and start the update process again.
CloudLink Gateway unable to connect to PBX w hen PBX deployed with MSL	IP address of gateway is not res ponded due to MSL rejecting connection.	Make sure the IP address of the gateway is included in the MSL t rusted networks.
SIP peer on the MiVB is out of service	MiVB database uses 20 trunk service numbers.	The CloudLink Gateway uses Trunk Service 78 on the MiVB. If the MiVB database has been flexed to have less than 78 Trunk Service groups, then it will need to be re-flexed to have at least that many Trunk Service groups to allow the Gateway to use Trunk Service 78.

Accessing the CloudLink Gateway Portal

Message (Issue)	Possible reason	Try this
Invalid email address	When configuring admin contacts or support contacts, or sending Welcome emails, you are unable to validate email addresses.	The CloudLink Platform validates a user's email address before accepting it. In general, role-based email addresses (for example admin@, help@, support@, info@, and so on.) are not accepted by the CloudLink Platform and are flagged as invalid, contact your Administrator or Mitel Technical Support.
Error occurred while sending welcome email. Please try again	When sending welcome emails, the email validation service flags the email to be invalid.	• The email address is spelt incorrectly • The email server or hosted domain has restrictive response policies • Email Users which frequently report spam There may be other reasons for the email to be flagged as invalid, contact your Administrator or Mitel Technical Support.

Message (Issue)	Possible reason	Try this
Welcome email not received	Users having role based emails are not accepted by the CloudLink Platform.	It's against industry practice to use role based emails as they encourage poor security practices such as credential sharing and fraud. Individual accounts are more secure with unique logins and clear accountability. Additionally, once a user logged into the system, these users would share a chat and call history eroding personnel privacy. Examples of role based emails include `admin`, `help`, `support`, and `info`. CloudLink rejects role based emails. However, while some limited cases exist, manually allowing role-based email is discouraged. If this is required, contact your Administrator or Mitel Technical Support.

For more information about downloading gateway logs see, Gateway.

For more information about configuring prerequisites see, Configuration Prerequisites.

If you need further assistance, contact Mitel Partner Technical Support via a login at https://www.mitel.com/en-ca/login.