



FortiVoice™ Enterprise Phone System
LDAP Authentication Configuration
Technical Note



FortiVoice Enterprise Phone System LDAP Authentication Configuration Technical Note

January 6, 2015

1st Edition

Copyright© 2015 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Configuring LDAP Authentication for Administrators and Extension Users

The FortiVoice unit can work with LDAP servers such as OpenLDAP or MS Active Directory to authenticate the administrators or extension users. This technical note uses examples to show how to configure LDAP authentication on the FortiVoice unit and MS Active Directory.

This technical note assumes that you use the FortiVoice firmware v 3.0.1 or later and MS Server 2012 Active Directory.

Use this note in conjunction with the *FortiVoice Enterprise Phone Administration Guide*.

Configuring LDAP authentication for administrators

Follow the procedures below to configure LDAP authentication for administrators on the FortiVoice administrator web GUI.

Configuring an LDAP profile

1. Go to *Phone System > Profiles > LDAP*
2. Click *New* to add a profile or double-click a profile to modify it.

For MS Active Directory, *Schema* should be *User Define* and LDAP user query is `(&(objectClass=user)(cn=$u))` as shown below.

The screenshot displays the FortiVoice 200D web interface. The top navigation bar includes 'Status', 'SIP', 'Caller ID Modification', 'Schedule', 'Phone', 'LDAP', and 'User Privileges'. The left sidebar shows 'System', 'Phone System', 'Settings', 'Advanced Settings', 'Audio', and 'Profiles'. The main content area is titled 'Edit LDAP Profile' and contains the following fields:

- Profile name: ldap_ad_admin
- Server name/IP: 172.20.141.199 (Port: 389)
- Fallback server name/IP: (Port: 389)
- Use secure connection: None (with a [Test LDAP Query...] button)
- Base DN: dc=fv,dc=qa
- Bind DN: cn=administrator,cn=users,dc=fv,dc=qa
- Bind password: (masked with asterisks, with a [Browse...] button)

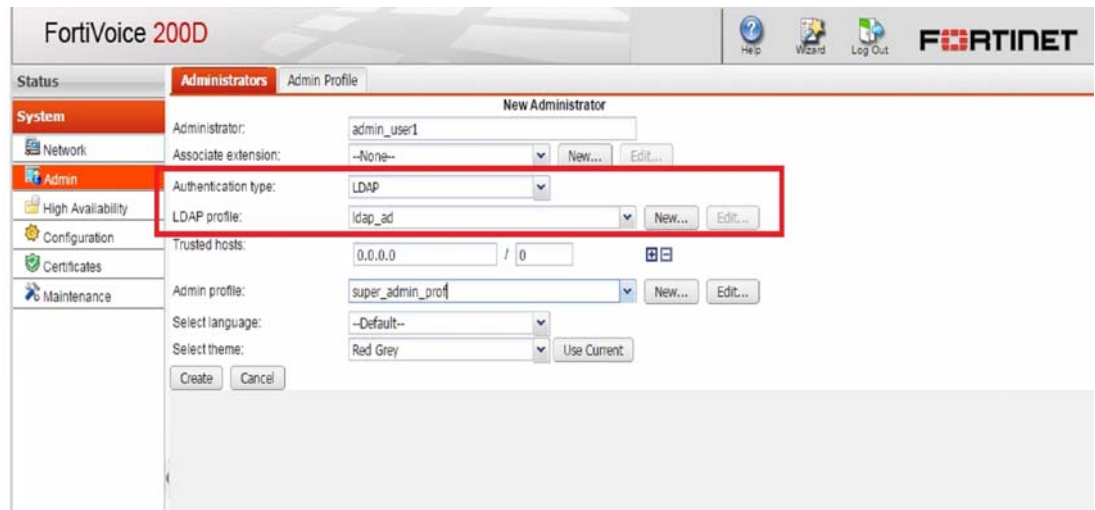
The 'User Authentication Options' section is expanded and highlighted with a red box. It contains:

- Try common name with base DN as bind DN
- Search user and try bind DN
- Common name ID: (empty field)
- Schema: User Defined (dropdown menu)
- LDAP user query: (&(objectClass=user)(cn=\$u)) (text field)
- Scope: Subtree (dropdown menu)
- Derefer: Never (dropdown menu)

At the bottom, there are 'Advanced Options' and buttons for 'Apply', 'OK', and 'Cancel'.

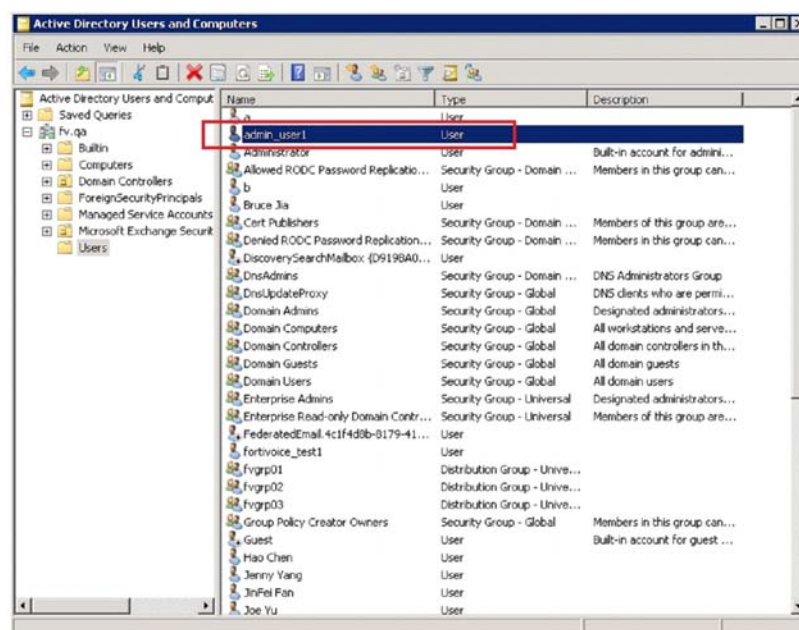
Configuring an administrator profile

1. Go to *System > Admin > Administrators*,
2. Click *New* to add a profile or double-click a profile to modify it. In this example, we create an administrator user: `admin_user1`.



Configuring the Active Directory on MS Server 2012

1. Open Active Directory Users and Computers.
2. Go to *Start > Control Panel*.
3. Double-click *Administrative Tools*, and then double-click *Active Directory Users and Computers*.
4. In the console tree, go to *Active Directory Users and Computers* and select the domain node and *Users* folder. In this example, the domain node is `fv.qa` and user name is `admin_user1`.



Verifying the configuration

1. Open the FortiVoice administrator web GUI such as `https://x.x.x.x/admin`.
2. Login as an administrator such as `admin_user1`.



Configuring LDAP authentication for extension users

Follow the procedures below to configure LDAP authentication for extension users.

Once completed, extension users can login from the FortiVoice user web portal using the login information assigned to them by the administrator.

Configuring LDAP authentication without authentication ID

You may configure LDAP authentication without authentication ID. In this case, each user must have the extension number configured in the Active Directory.

Configuring an LDAP profile

1. Go to *Phone System > Profiles > LDAP*.
2. Click *New* to add a profile or double-click a profile to modify it.

3. Select Active Directory for Schema.

The screenshot shows the FortiVoice 200D configuration interface for an LDAP profile. The 'Edit LDAP Profile' window is open, showing various fields for profile configuration. A red box highlights the 'User Authentication Options' section, specifically the 'Search user and by bind DN' radio button, the 'Schema' dropdown menu set to 'Active Directory', and the 'LDAP user query' field containing the query: `[&(objectClass=user)(telephoneNumber=$u)]`. Other visible fields include Profile name (ldap_ad), Server name/IP (172.20.141.199), Port (389), Base DN (dc=fv,dc=qa), Bind DN (cn=administrator,cn=users,dc=fv,dc=qa), and Bind password (masked with asterisks).

Applying the LDAP profile to extension

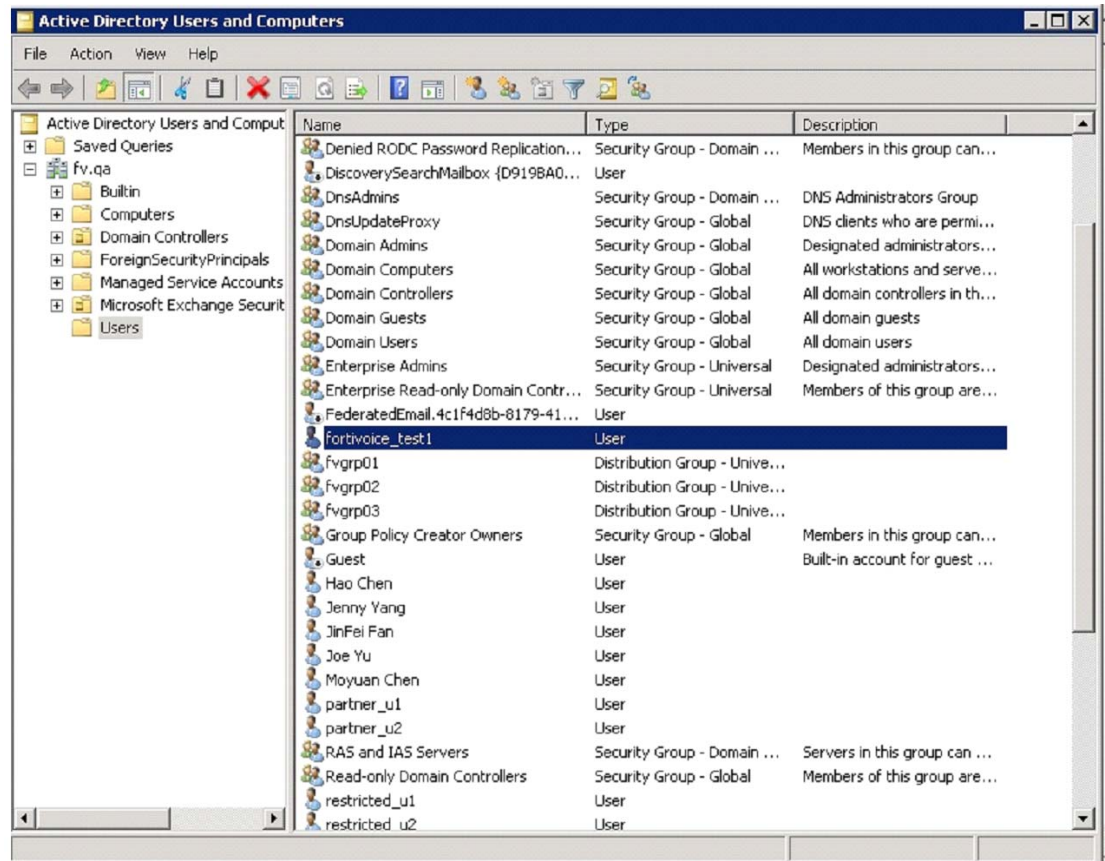
1. Go to *Extensions > Extensions > IP extensions*.
2. For *Authentication type*, select *LDAP*.
3. For LDAP profile, select the profile created in the previous step. In this example, the extension number is 2001.

The screenshot shows the FortiVoice 200D configuration interface for an IP extension. The 'IP Extensions' window is open, showing the 'Extension Setting' section. A red box highlights the 'Authentication type' dropdown menu set to 'LDAP' and the 'LDAP profile' dropdown menu set to 'ldap_ad'. Other visible fields include User ID (2001), Number (2001), Enabled (checked), Display name (Fortivoice test1), External caller ID (e.g. Jim <612223>), SIP password (masked), and User PIN (masked). The 'Advanced Setting' section is also visible, showing Location (Internal), SIP setting (None), User privilege (None), Department (None), Phone type (FortiFone-450/460), and Phone profile (Admin defined).

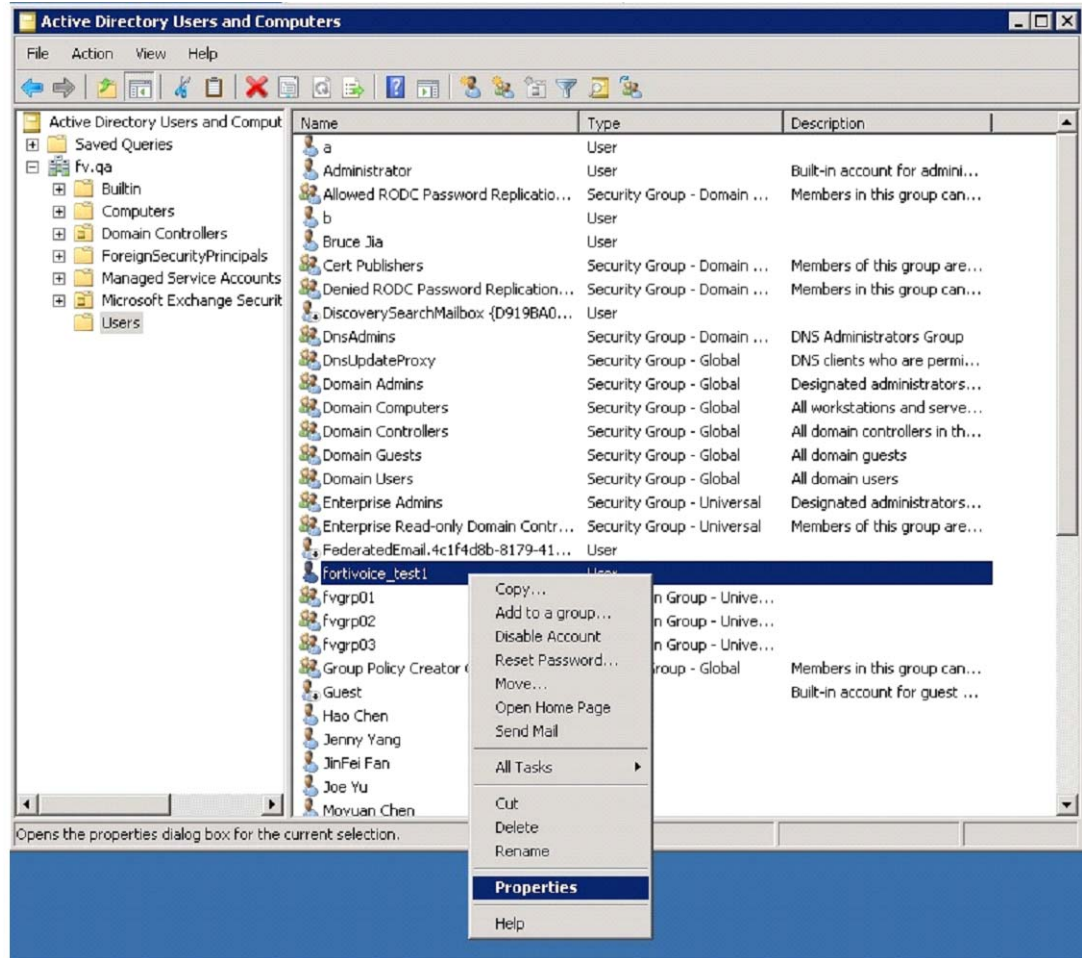
4. Leave the *Authentication ID* field empty.

Configuring Active Directory on MS Server 2012

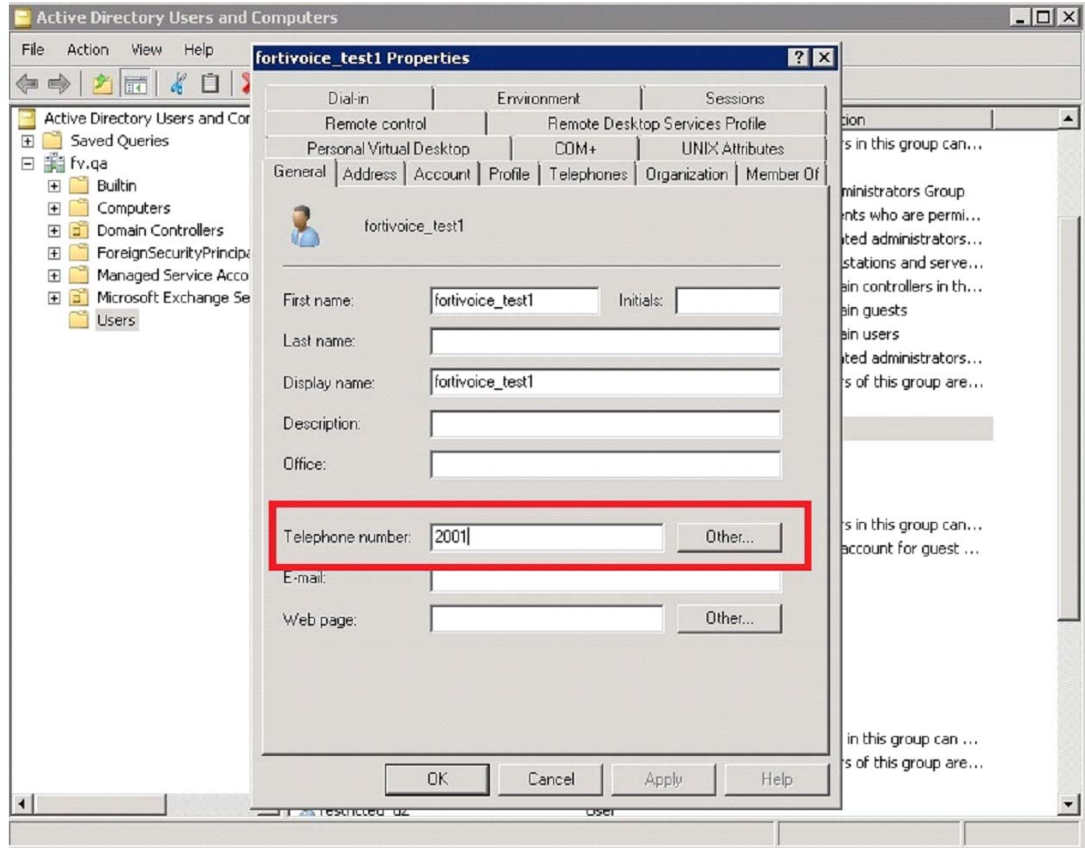
1. Open Active Directory Users and Computers.
2. Go to *Start > Control Panel*.
3. Double-click *Administrative Tools*, and then double-click *Active Directory Users and Computers*.
4. In the console tree, go to *Active Directory Users and Computers* and select the domain node and *Users* folder. In this example, the domain node is *fv.qa* and user name is *fortivoice_test1*.



5. Right-click *fortivoice_test1* > *Properties*.

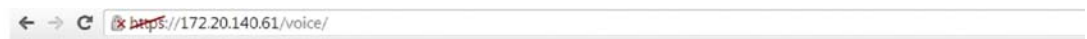


6. Select *General* and enter 2001 (extension number) for *Telephone number*.



Verifying the configuration

1. Open the FortiVoice user web portal such as <https://x.x.x.x/voice>.
2. Login as an extension user such as 2001.



Configuring LDAP authentication with authentication ID

This section shows how to configure LDAP authentication with the authentication ID. By using the authentication ID, you do not need to configure the extension number for each user in the Active Directory.

Configuring an LDAP profile

1. Go to *Phone System > Profiles > LDAP*
2. Click *New* to add a profile or double-click a profile to modify it.

For MS Active Directory, *Schema* should be *User Define* and LDAP user query is `(&(objectClass=user)(cn=$u))` as shown below.

The screenshot displays the FortiVoice 200D web interface. The top navigation bar includes 'Status', 'SIP', 'Caller ID Modification', 'Schedule', 'Phone', 'LDAP', and 'User Privileges'. The 'LDAP' tab is active, showing the 'Edit LDAP Profile' configuration page. The profile name is 'ldap_ad_ext_auth_id'. The server name/IP is '172.20.141.199' and the port is '389'. The Base DN is 'dc=fv,dc=qa' and the Bind DN is 'cn=administrator,cn=users,dc=fv,dc=qa'. The 'User Authentication Options' section is expanded, and the 'Search user and try bind DN' radio button is selected. The 'Schema' dropdown is set to 'User Defined', and the 'LDAP user query' text box contains the query '(&(objectClass=user)(cn=\$u))'. The 'Scope' is set to 'Subtree' and 'Derefer' is set to 'Never'. The 'Advanced Options' section is collapsed. At the bottom, there are 'Apply', 'OK', and 'Cancel' buttons.

Applying the LDAP profile to extension

1. For *Authentication type*, select *LDAP*.

2. For LDAP profile, select the profile created in the previous step. In this example, the extension number is 2002.

The screenshot shows the FortiVoice 200D web interface. The left sidebar contains navigation options: Status, System, Phone System, Extensions (selected), Groups, General Voicemail, and Virtual Number. The main content area is titled 'Extension Setting' and includes the following fields:

- Number: 2002
- User ID: 2002
- Enabled:
- Display name: Fortivoice test02
- External caller ID: (empty)
- Warning: Password policy is disabled
- SIP password: 9e4^Qh8V
- User PIN: 123123
- Authentication type: LDAP (highlighted in a red box)
- LDAP profile: ldap_ad_ext_auth_id (highlighted in a red box)
- Authentication ID: fortivoice_test2 (highlighted in a red box)
- Phone language: --Default--

Below the main settings is the 'Advanced Setting' section, which includes:

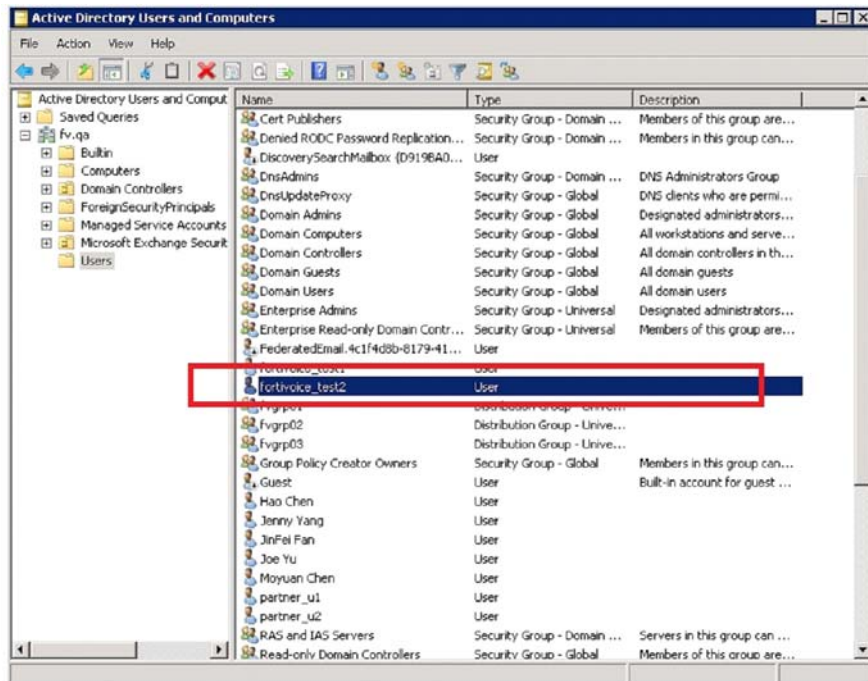
- Location: Internal
- SIP settings: --None--
- User privileges: --None--
- Department: --None--
- Phone type: FortFone-350/360i
- MAC address: (empty)
- Phone profile: Admin defined

3. For *Authentication ID*, enter `fortivoice_test2`.

Configuring Active Directory on MS Server 2012

1. Open Active Directory Users and Computers.
2. Go to *Start > Control Panel*.
3. Double-click *Administrative Tools*, and then double-click *Active Directory Users and Computers*.

- In the console tree, go to *Active Directory Users and Computers* and select the domain node and *Users* folder. In this example, the domain node is *fv.qa* and user name is *fortivoice_test2*.



Verifying the configuration

- Open the FortiVoice user web portal such as `https://x.x.x.x/voice`.
- Login as an extension user such as 2002.



