



Installation & Administration Guide

IP Conferencing Phone

Model No. **KX-HDV800**



Thank you for purchasing this Panasonic product.
Please read this manual carefully before using this product and save this manual for future use.

In this manual, the suffix of each model number is omitted unless necessary.

Document Version 2019-06

Introduction

Outline

This document only includes setup, registration of accounts, and configuration.

Related Documentation

USER GUIDE

Describes information about the operation of the product.

Manuals and supporting information are provided on the Panasonic Web site at:
<https://panasonic.net/cns/pcc/support/sipphone/>

Technical Support

When technical support is required, contact your phone system dealer/service provider.

Trademarks

- The Bluetooth® word mark and logos are owned by the Bluetooth SIG, Inc. and any use of such marks by Panasonic Corporation is under license.
- Microsoft and Excel are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.
- SD Logo is a trademark of SD-3C, LLC.
- All other trademarks identified herein are the property of their respective owners.
- Microsoft product screen shot(s) reprinted with permission from Microsoft Corporation.

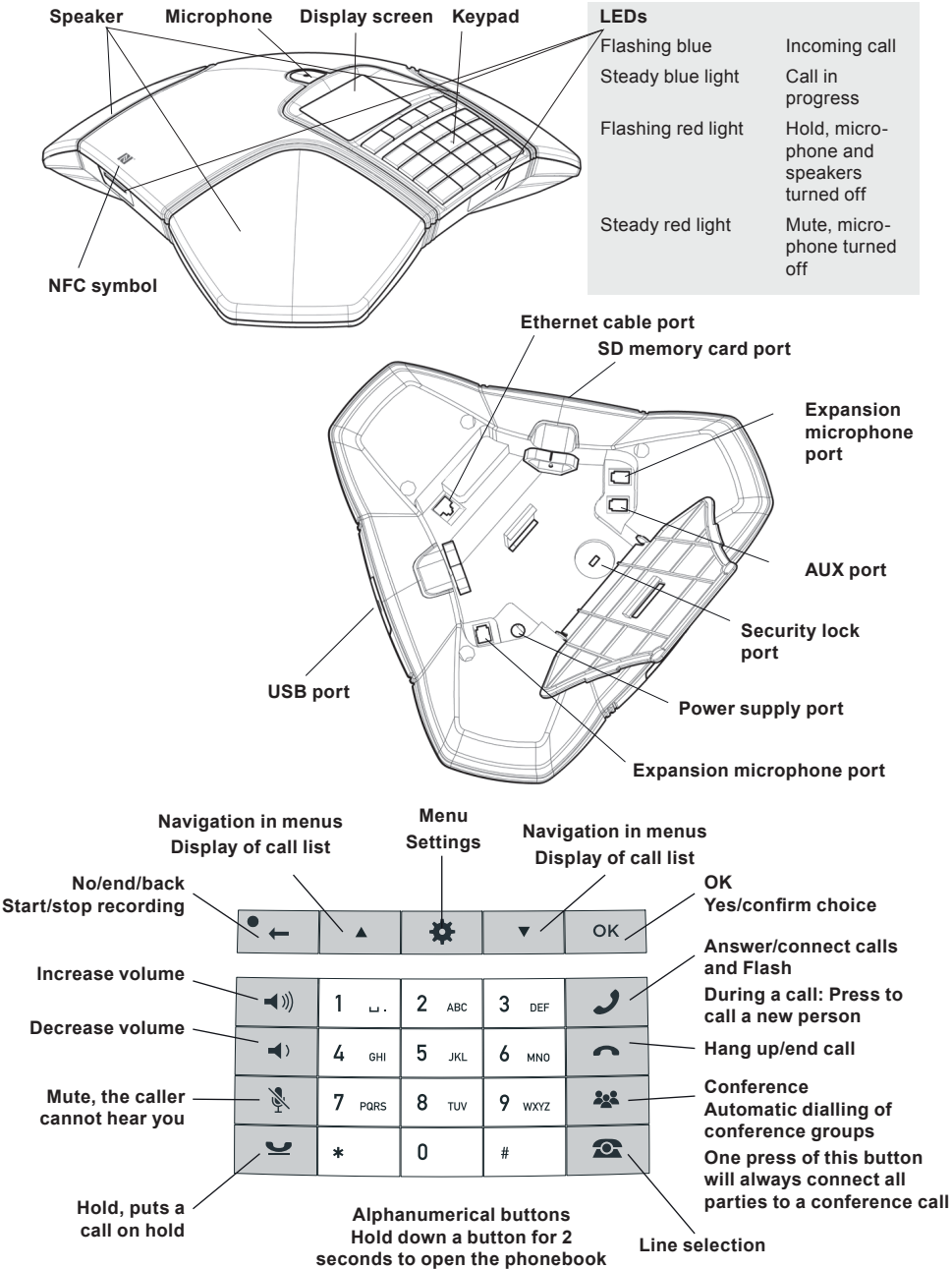
Note

- The screen shots shown in this guide are provided for reference only, and may differ from the screens displayed on your PC.

CONTENT

DESCRIPTION	4
DISPLAY INFORMATION AND WEB INTERFACE	5
DISPLAY SCREEN	5
NAVIGATION AND SELECTION IN MENUS	6
USING THE WEB INTERFACE	8
INSTALLATION	9
CONNECTING	9
OBTAINING A NETWORK ADDRESS	10
LOGIN	10
SOFTWARE UPGRADE AND BASIC SETTINGS	11
REGISTERING AN ACCOUNT	14
SETTINGS	16
LOGIN	16
BASIC	16
SIP	19
NETWORK	25
MEDIA	27
LDAP	30
WEB INTERFACE	32
TIME & REGION	33
PROVISIONING	34
SYSTEM	35
HEADSET INSTALLATION	36
CONNECTING A WIRELESS HEADSET	36
HARD SYSTEM RECOVERY	37
PROVISIONING – UPGRADE AND CONFIGURATION	38
FIRMWARE UPGRADE ON A SINGLE PHONE	38
USING A CONFIGURATION FILE	39
USING A DEVICE MANAGEMENT SERVER	45
MANAGING PHONE BOOK AND CONF. GUIDE	50
IMPORTING AND EXPORTING CONTACTS	50
IMPORTING AND EXPORTING CONFERENCE GROUPS	52
CHECKING STATUS AND LOGS	53
DEVICE	53
NETWORK	53
TIME & REGION	54
SIP	54
MEDIA	55
LOG	56
SPECIFICATIONS	58

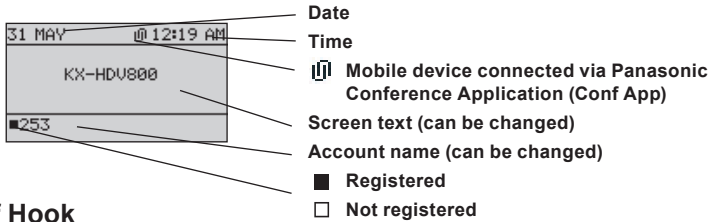
DESCRIPTION



DISPLAY SCREEN

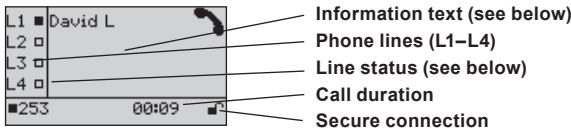
On Hook

Press  to display this screen.



Off Hook

Press  to display this screen.



Line status:

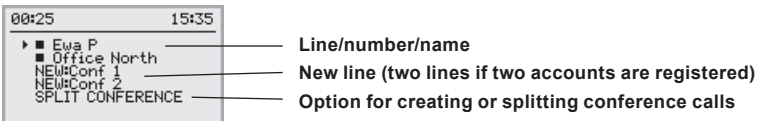
- ☐ Line free (Before account name – telephone not registered)
- ☒ Line connected (Before account name – telephone registered)
- ☒ Line on hold ("HOLD" displayed on the screen – all calls on hold)
- ☒ Line (called party) busy
- ☒ Own line put on hold by other party
- ☒ Recording call
- ☒ Secure connection

Information text displays one of the following:

- Number or name of each phone line
(The name will be displayed if a number is in the phone book)
- Explanation of what you should do (For example **ENTER NUMBER**)
- Status (For example **HOLD** when you place all calls on hold)

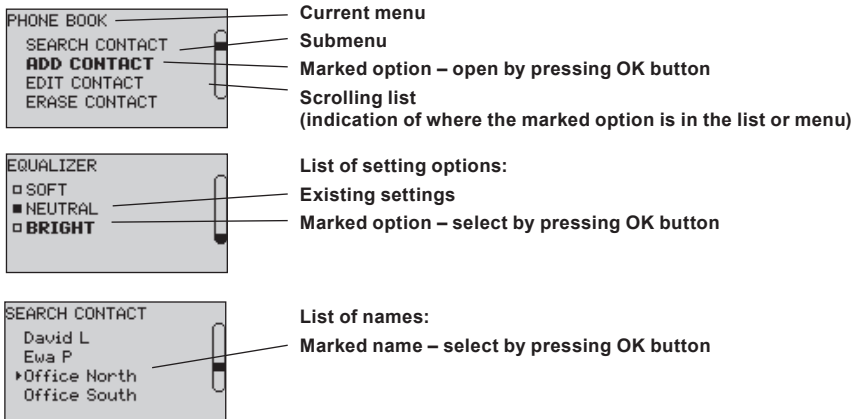
Line menu

Press  (**LINE**) to switch to and from this menu.



Menu

Press **⚙ (MENU)** to switch to and from a menu.



NAVIGATION AND SELECTION IN MENUS

- ⇒ Press **⚙ (MENU)** .
- ⇒ Select the option you want from the menu using the arrow buttons.
- ⇒ Confirm by pressing **OK** to select the marked option.
- ⇒ Cancel the setting or go back one level in the menu by pressing **⬅**.
- ⇒ Quit the menu by pressing **⚙ (MENU)** again.
- ① Note that after you have made changes to a setting, you must press **OK** to activate the setting.
- 💡 It is possible to open a menu option directly by pressing the number button that corresponds to the position of the option in the menu (e.g. 2 to open PHONE BOOK and then 3 to select EDIT CONTACT).

Writing style in instructions

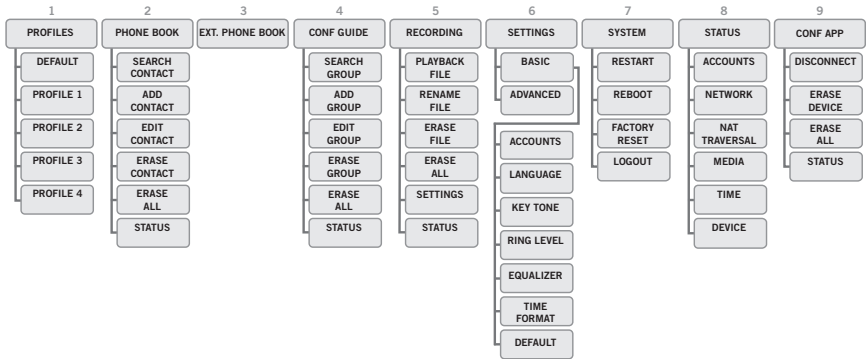
In the instructions, **⚙ (MENU) > SETTINGS (6)** means you should:

- ⇒ Press **⚙ (MENU)** .
- ⇒ Mark the **SETTINGS** option using the arrow buttons and confirm by pressing **OK** to open the menu (or press button number **6**).

Correspondingly, **Phone book > Conference Guide** in the web interface means you should select Phone book menu and the Conference Guide tab.

DISPLAY INFORMATION AND WEB INTERFACE

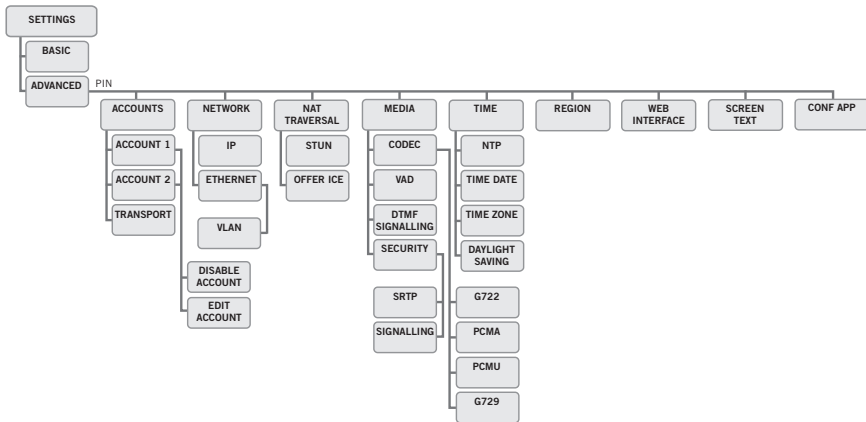
Menu tree




Menu tree, advanced settings

The advanced settings are protected by administrator's PIN code.

The default value is **12345678**.



 The simplest way to make settings and edit contacts is using a PC and the KX-HDV800 web interface.

USING THE WEB INTERFACE

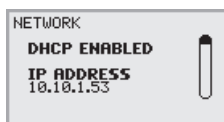
You can use the web browser of a PC connected to the same network to manage contacts, conference groups and settings in the KX-HDV800.

For security reasons, recordings can only be managed directly on the KX-HDV800. All other settings that can be made directly on the KX-HDV800 can also be made via the web interface. It is also possible to import and export contacts and conference groups, name user profiles and change PIN codes, which can only be done via the web interface. The administrator can also view logs, update software and create a configuration file.

The default setting for the PIN code is **00000000** for the user account (Default, Profile 1, Profile 2, Profile 3 and Profile 4) and **12345678** for the administrator's account (Admin). We recommend that you change the PIN codes in order to protect the settings. The administrator can always view and change the PIN codes to the user accounts. The administrator's PIN code can only be reset with a complete reset to factory settings.

Checking IP address

- ⇒ Press **⚙️ (MENU)** and select the sub menu **STATUS > NETWORK** (8,2).
- ⇒ Check the conference phone's network address under the heading **IP ADDRESS**.



- ① Use this address to log into the web server in the conference phone.

Login

- ⇒ Log into the web server in KX-HDV800 by entering the phone's network address in your computer's web browser.
- ⇒ Select **Admin** as Profile and enter your PIN.
- ① Default PIN is 12345678.

A screenshot of a web browser displaying the KX-HDV800 web interface. At the top, it says "KX-HDV800" and "You are logged out Login". Below this is a navigation bar with "Status", "Phone book", "Call list", and "Settings". The "Login" section is active, showing a "Profile" dropdown menu set to "Admin", a "PIN" field with eight dots, and a "Login" button.

INSTALLATION

The printed Installation Guide provides brief and simplified installation instructions. The guide includes the basic settings for a quick start and works in most cases.

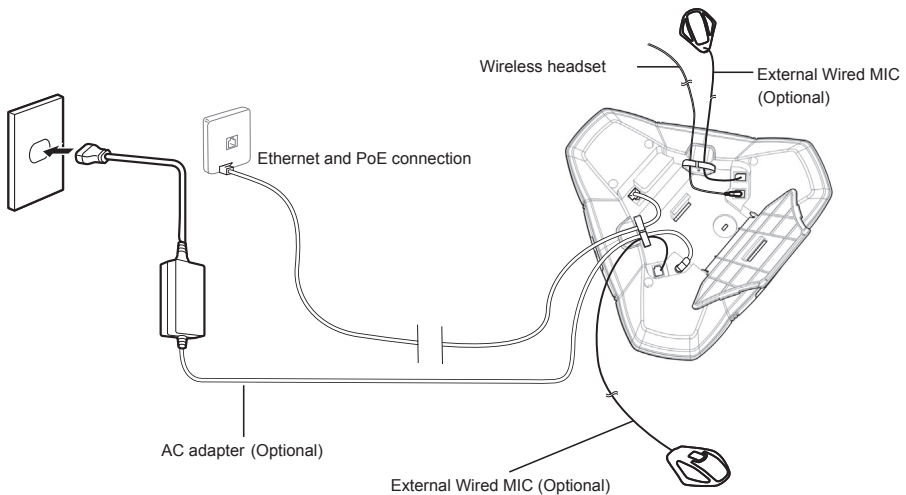
Note

- Panasonic assumes no responsibility for injuries or property damage resulting from failures arising out of improper installation or operation inconsistent with this documentation.

CONNECTING

⇒ Connect the KX-HDV800 to the network as illustrated below. KX-HDV800 supports PoE (Power over Ethernet).

- ① If the network does not support PoE, an optional AC adapter must be used for connection to the mains.



The headsets can be used with this unit. (Not all operations with the headsets can be guaranteed.) For up-to-date information about headsets that have been tested with this unit, refer to the following web sites:

<https://panasonic.net/cns/pcc/support/sipphone/>

⇒ Place the conference phone in the middle of the table.

The KX-HDV800 must obtain a network address and be registered in a SIP PBX before it can be used. The easiest way to register an account and make the settings in the KX-HDV800 is using a computer connected to the same network and via the integrated web server.

OBTAINING A NETWORK ADDRESS

Connecting to a network with DHCP

See “Check IP address” under “USING THE WEB INTERFACE” on page 8.

Connecting to a network with static IP addresses

You need the IP address, host name, domain, (**MENU**), gateway, DNS 1, and DNS 2. The host name can be set freely. The domain and secondary DNS can be left blank.

- ⇒ Press **⚙** (**MENU**) and select **SETTINGS > ADVANCED** (6,2).
- ⇒ Enter the PIN code.
 - ① The default code is **12345678**.
- ⇒ Select **NETWORK** (2)
- ⇒ Select **STATIC IP**.
- ⇒ Enter values for the IP ADDRESS.
 - ① Enter three digits (begin with 0 if necessary), press **OK**, enter three digits, and so on.
- ⇒ Enter HOST NAME
 - Default is KX-HDV800.*
- ⇒ Enter DOMAIN
- ⇒ Enter NETMASK
- ⇒ Enter GATEWAY
- ⇒ Enter DNS 1
- ⇒ Enter DNS 2
 - The display shows DONE.*

LOGIN

See “Login” under “USING THE WEB INTERFACE” on page 8.

SOFTWARE UPGRADE AND BASIC SETTINGS

The following settings should be done during installation.

- ① See page 45 about Device management if you are responsible for installing or upgrading many phones.

Note that all settings on the Basic tab also affect the user profile Default. Other user profiles can be changed individually. The settings on the Basic tab, except the name and PIN for Admin, can be modified by any user. Other settings require a login as Admin.

Upgrade software

See the heading “PROVISIONING – UPGRADE AND CONFIGURATION” on page 38 for a detailed description and upgrading options.

- ⇒ Select **Settings** > **Provisioning**.

The screenshot shows the KX-HDV800 web interface. At the top, it says "KX-HDV800" and "You are logged in as ADMIN Logout". Below this is a navigation bar with tabs: Status, Phone book, Call list, Settings, Provisioning, System, and Conference Application. The "Settings" tab is selected, and within it, the "Provisioning" sub-tab is active. The main content area is divided into three sections: "Firmware upgrade", "Configuration", and "Device management".

Firmware upgrade

Current version: 2.5.48

File: HDV800_v2.0.3.kt [Upgrade]

Configuration

File: [Choose file] No file chosen [Import]

Export: [Export] Passwords will not be exported!

Device management

Enable: ☒ On ☐ Off

Use DHCP option: ☒ On ☐ Off

DHCP option: 43: Vendor specific ▼

File server address: [Text box]

HTTPS protocol: TLSv1 ▼

- ⇒ Compare the latest version with the current version (shown on the web page).
- ⇒ If you want to upgrade, select the desired version in the list box and click on **Upgrade**.

The browser window and the display on the KX-HDV800 shows that the upgrade has begun.

- ① The download and installation can take several minutes. Do not interrupt the upgrade and do not disconnect plugs to the KX-HDV800 during the upgrade. Interrupting the upgrade may render the conference phone inoperable.
- ⇒ When installation is complete, the text “Upgrade Complete. The unit will be rebooted.” is shown in your browser, and after a while you hear the music signature, which indicates that the conference phone has started.

Setting time and region

⇒ Select **Settings > Time & Region**.

The screenshot shows the KX-HDV800 web interface. At the top, the title 'KX-HDV800' is on the left, and 'You are logged in as ADMIN Logout' is on the right. Below the title bar is a navigation menu with tabs: Status, Phone book, Call list, Settings, Basic, SIP, Network, Media, LDAP, LLDP, Web interface, Time & Region (selected), Provisioning, System, and Conference Application. The 'Time & Region' section is active and contains three sub-sections: 'Time', 'Region', and 'Daylight saving'. The 'Time' section has 'Enable NTP' set to 'On', 'Time' set to '12:10:19', 'Date' set to '2017-02-09', 'Timezone' set to 'UTC+1' with a '00' offset, and 'NTP Server' set to 'pool.ntp.org'. The 'Region' section has 'Region' set to 'SWE Sweden'. The 'Daylight saving' section has 'Enable DST' set to 'Yes', 'DST Timezone (hh:mm)' set to 'UTC+2' with a '00' offset, and 'DST Mode' set to 'Automatic'.

⇒ Select the time zone and, if you wish, correction for DST (Daylight saving).

① It is also possible to set the time and date manually or choose a different time server.

⇒ Select the region where you are.

① This setting affects the signalling.

⇒ Save the setting.

The KX-HDV800 reboots with the new settings.

INSTALLATION

Changing the language

⇒ Select **Settings** > **Basic**.

KX-HDV800 You are logged in as ADMIN [Logout](#)

Status Phone book Call list **Settings**

Basic SIP Network Media LDAP LLDP Web interface Time & Region Provisioning System Conference Application

Profiles

	Name	PIN	Edit	Set
Default	DEFAULT	*****	Edit	Set
Profile 1	PROFILE 1	*****	Edit	Set
Profile 2	PROFILE 2	*****	Edit	Set
Profile 3	PROFILE 3	*****	Edit	Set
Profile 4	PROFILE 4	*****	Edit	Set
Admin	ADMIN	*****	Edit	Set

Default account

Account ☒ Account 1 ☐ Account 2

Preferences

Phone language

Ring level

Key tone ☒ On ☐ Off

Recording ☒ On ☐ Off

Recording tone ☒ On ☐ Off

Time format ☒ 12 Hour ☐ 24 Hour

Equalizer ☐ Soft ☒ Neutral ☐ Bright

Screen text

⇒ Select the desired language in the list box after Language and save the setting.

① Note, this only affects the phone language, not the web interface.

Changing the PIN

We recommend that you change the PIN code for Admin from the default setting to protect the settings. Make a note of the new PIN code and keep it in a safe place. The administrator's PIN code can only be reset by a full factory reset!

⇒ Select **Settings** > **Basic** and click the **Edit** button on the Admin line.

⇒ Enter a new PIN.

① The minimum length of PIN is 8 digits.

⇒ Click on the **Set** and **Save** buttons.

REGISTERING AN ACCOUNT

The conference phone can be registered in a company SIP PBX or with a public IP telephony service provider. You can store settings for two accounts in KX-HDV800. To register your phone, you must have access to the account information and all necessary settings that the SIP PBX or service provider requires.

See the heading "SIP" on page 19 for a detailed description of all settings.

⇒ Select **Settings > SIP**.

⇒ Click **Yes** at Enable account under Account 1.

⇒ Enter the account information you have received.

① Account name can be chosen freely and is the name or phone number you want to appear in the phone display.

⇒ Leave the default values if you have no other information.

KX-HDV800

Status Phone book Call list Settings

Basic **SIP** Network Media LDAP LLDP Web interface Time & Region Provisioning System Conference Application

Account 1

Enable account☒ Yes ☐ No

Account name ①

User ①

Registrar ①

Proxy ①

Enable keep-alive ①☒ Yes ☐ No

Realm ①

Authentication name ①

Password

Registration interval ①

Account 2

Enable account☐ Yes ☒ No

Account name

User

Registrar

Proxy

Enable keep-alive☒ Yes ☐ No

Realm

Authentication name

Password

Registration interval

NAT Traversal

STUN ①☐ On ☒ Off

Offer ICE☐ Yes ☒ No

TURN ①☐ On ☒ Off

TURN host

STUN host

TURN user

Password

Advanced

Runtime Credentials☐ Yes ☒ No

Enable SIP Fallback☐ Yes ☒ No

Enable SIP Replaces☐ Yes ☒ No

Enable Blind Transfer☐ Yes ☒ No

Allow contact rewrite☐ Yes ☒ No

Disable 'rport'☐ Yes ☒ No

Session timers☐ Disabled ☒ Optional ☐ Mandatory

Session expiration seconds

Outbound proxy

Transport

Protocol☒ UDP ☐ TCP ☐ TLS ☐ SIPs

Local UDP port

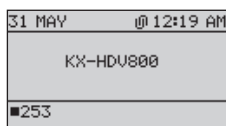
Please check corresponding media signalling setting

Save Cancel

INSTALLATION

- ⇒ Select a method of NAT traversal if you have received this information.
- ⇒ Select a different transport protocol if you have received this information. See page 22 about using a secure transport protocol.
- ⇒ Save the settings by clicking the **Save** button.

The KX-HDV800 responds by showing REGISTERING. If registration is successful, your selected account name will appear at the bottom of the display screen next to a shaded square.



Make media settings

- ⇒ Select a different codec priority, if you do not accept the default settings. See page 27.
- ⇒ Select a SRTP option if you need a secure media protocol. See page 28. Note that this also requires a corresponding transport setting on the SIP tab.

SETTINGS

Almost all settings can be done directly on the KX-HDV800. See “NAVIGATION AND SELECTION IN MENUS” on page 6 for using the menu system. We explain how to make settings using the web interface as this is the easiest method.

For safety reasons, recordings can only be managed directly on the KX-HDV800. All other settings can be changed via the web interface. The web interface also allows you to import and export contacts and conference groups, rename user profiles and change PIN codes. As an administrator, you can also study logs, upgrade the software and create an XML based configuration file for easier management of a set of phones.

LOGIN

See “USING THE WEB INTERFACE” on page 8 for a description of how to log in to the web server in the KX-HDV800.

BASIC

⇒ Select **Settings > Basic**.

KX-HDV800

You are logged in as ADMIN
[Logout](#)

StatusPhone bookCall listSettings

BasicSIPNetworkMediaLDAPLLDPWeb interfaceTime & RegionProvisioningSystemConference Application

Profiles

	Name	PIN		
Default	DEFAULT	**** *	Edit	Set
Profile 1	PROFILE 1	**** *	Edit	Set
Profile 2	PROFILE 2	**** *	Edit	Set
Profile 3	PROFILE 3	**** *	Edit	Set
Profile 4	PROFILE 4	**** *	Edit	Set
Admin	ADMIN	**** *	Edit	Set

Default account

Account

Account 1

Account 2

Preferences

Phone language

English

Ring level

Level 4

Key tone

On

Off

Recording

On

Off

Recording tone

On

Off

Time format

12 Hour

24 Hour

Equalizer

Soft

Neutral

Bright

Screen text

KX-HDV800

Save

Cancel

SETTINGS


These settings affect the Admin and Default profiles. To change the basic settings of a user profile, you need to log in with that profile.


Profiles – edit name and PIN

We recommend that you change the PIN code from the default setting to protect the settings.


- ⇒ Select **Settings** > **Basic** and click the **Edit** button on the account you want to change.
- ⇒ Enter a new PIN code.
- ① The minimum length of PIN is 8 digits.
- ① You can also choose to change the name of a user profile.
- ⇒ Click on the **Set** and **Save** buttons.
- ① Make a note of the new PIN code and keep it in a safe place.
- ① The administrator's PIN code can only be reset with a complete reset to factory settings!

Default account

This setting determines which account will be used as default. By pressing  (**LINE**) before dialling a number, you can choose the alternative account for the call.


- ⇒ Select Account 1 or Account 2 and click on the **Save** button.
- On phone:  (**MENU**) > **SETTINGS** > **BASIC** > **ACCOUNTS** (6,1,1).

Language

- ⇒ Select language using the list box and click on the Save button.
- On phone:  (**MENU**) > **SETTINGS** > **BASIC** > **LANGUAGE** (6,1,2).


Ring level

There are six volume levels plus a silent mode. You will hear the ring tone for each level you select. If you select silent mode, only the blue LEDs on the phone flash when an incoming call is received.

- ⇒ Select level using the list box and click on the Save button.
- On phone:  (**MENU**) > **SETTINGS** > **BASIC** > **RING LEVEL** (6,1,4).

Key tone

You can select whether or not you want a tone to be heard when you press a button.

- ⇒ Select On or Off and click on the Save button.
- On phone:  (**MENU**) > **SETTINGS** > **BASIC** > **KEY TONE** (6,1,3).

SETTINGS

Recording

It is possible to turn off the recording feature. This setting can only be done by the administrator and affects all profiles.

⇒ Select On or Off and click on the **Save** button.

Recording tone

A short beep is heard every 20 seconds so that all the parties in the call know it is being recorded. This feature can be turned off.

⇒ Select On or Off and click on the **Save** button.

On phone:  (MENU) > **RECORDING** > **SETTINGS** (5,5).

Time format

⇒ Select 12 hour or 24 hour and click on the **Save** button.

On phone:  (MENU) > **SETTINGS** > **BASIC** > **TIME FORMAT** (6,1,6).

Equalizer

The sound reproduction can be adjusted to the required pitch (SOFT, NEUTRAL or BRIGHT).

⇒ Select Soft, Neutral or Bright and click on the **Save** button.

On phone:  (MENU) > **SETTINGS** > **BASIC** > **EQUALIZER** (6,1,5).

Screen text

The text on the display screen is shown when the KX-HDV800 is in stand-by mode (on hook).

⇒ Enter your new text in the text box and click on the **Save** button.

On phone:  (MENU) > **SETTINGS** > **ADVANCED** > **SCREEN TEXT** (6,2,8).

① The text is also used to identify a KX-HDV800 when using the Conf App to connect.

SIP

⇒ Select **Settings** > **SIP**

KX-HDV800

StatusPhone bookCall listSettings

BasicSIPNetworkMediaLDAPLLDPWeb interfaceTime & RegionProvisioningSystemConference Application

Account 1

Enable account☒ Yes ☐ No

Account name ⓘ169

User ⓘ169

Registrar ⓘ192.168.0.101

Proxy ⓘ

Enable keep-alive ⓘ☒ Yes ☐ No

Realm ⓘ*

Authentication name ⓘ169

Password*****

Registration interval ⓘ1800

Account 2

Enable account☐ Yes ☒ No

Account name

User

Registrar

Proxy

Enable keep-alive☒ Yes ☐ No

Realm

Authentication name

Password*****

Registration interval1800

NAT Traversal

STUN ⓘ☐ On ☒ Off

Offer ICE☐ Yes ☒ No

TURN ⓘ☐ On ☒ Off

TURN host

STUN host

TURN user

Password

Advanced

Runtime Credentials☐ Yes ☒ No

Enable SIP Fallback☐ Yes ☒ No

Enable SIP Replaces☐ Yes ☒ No

Enable Blind Transfer☒ Yes ☐ No

Allow contact rewrite☒ Yes ☐ No

Disable 'rport'☐ Yes ☒ No

Session timers☐ Disabled ☒ Optional ☐ Mandatory

Session expiration1800 seconds

Outbound proxy

Transport

Protocol☒ UDP ☐ TCP ☐ TLS ☐ SIPs

Local UDP port5060

Please check corresponding media signalling setting

SaveCancel

The KX-HDV800 can store information for two accounts, e.g. one PBX and one public service provider.

Why use two accounts?

It may be sensible to register a second account if the PBX or SIP server is located in another country than the phone. Otherwise, local calls using the PSTN (telephone network), connected through the ordinary PBX or SIP server, would be connected as international calls.

SETTINGS

Account 1 and Account 2

Enable account	It is possible to store account information for future use, but temporarily disable it.
Account name	This is the name displayed on the screen. It can be set according to company standards.
User	The account (customer) name.
Registrar	Shall contain the IP address or the public name of the SIP server where the account is registered (e.g. 10.10.1.100 for a local SIP server or sip.company.net for a public VoIP service provider)
Proxy	Shall contain the proxy server used for Internet communication, if any. Can be left blank.
Realm	The protection domain where the SIP authentication (name and password) is valid. This is usually the same as the registrar. If left blank, or marked with a "*", the phone will respond to any realm. If specified, the phone will only respond to the specific realm when asked for credentials.
Authentication name	The name used for the Realm authentication. This may be the same as the user name, but must be filled in.
Password	The password used for the Realm authentication.
Registration Interval	This is a request to the SIP server for when the registration should expire. KX-HDV800 automatically renews the registration within the time interval if the phone is still on and connected to the server. The default value is 1800 seconds.

On phone:  (MENU) > **SETTINGS** > **ADVANCED** > (PIN) > **ACCOUNTS** (6,2,1).

Nat traversal

NAT (Network Address Translation) is a firewall or router function that operates by rewriting the IP addresses in the IP headers as packets pass from one interface to the other. When a packet, for example, is sent from the inside, the source IP address and port are rewritten from the private IP address space into the address space on the outside (Internet).

NAT rewrites the addresses but leaves the packets themselves untouched. This kind of translation works fine for many protocols, but causes a lot of trouble for SIP packets that contain address information in their content (for example an INVITE request from one IP address to another).

NAT traversal solves this problem, providing a "view from the outside" that makes it possible to replace the IP address in the SIP requests with the address shown on the other side of the firewall.

SETTINGS

Note that in some cases NAT traversal is not necessary. Some public service providers of IP telephony keep track of the actual IP address used to register a phone, and the one used in the SIP requests from the same phone, and then replaces the addresses in the SIP messages.

STUN

STUN (Simple Traversal of UDP through NATs) is a protocol that assists devices behind a NAT firewall or router with their packet routing. STUN is commonly used in real-time voice, video, messaging, and other interactive IP communication applications.

The protocol allows applications operating through a NAT to discover the presence and specific type of NAT and obtain the mapped (public) IP address (NAT address) and port number that the NAT has allocated for the application's User Datagram Protocol (UDP) connections to remote hosts. The protocol requires assistance from a 3rd-party network server (STUN server).

STUN should be activated if an external SIP server cannot connect to the KX-HDV800 behind a firewall NAT function and the SIP server supports STUN. A suitable STUN server is usually provided by the VoIP service provider.

Note: STUN might also be referred to as Session Traversal Utilities for NAT.

STUN host

The IP address or public name of the STUN server.

Offer ICE

ICE (Interactive Connectivity Establishment), is a STUN addition that provides various techniques to allow SIP-based VoIP devices to successfully traverse the variety of firewalls that may exist between the devices. The protocol provides a mechanism for both endpoints to identify the most optimal path for the media traffic to follow.

TURN

TURN (Traversal Using Relay NAT) TURN is an extension of the STUN protocol that enables NAT traversal when both endpoints are behind symmetric NAT. With TURN, media traffic for the session will have to go to a relay server. Since relaying is expensive, in terms of bandwidth that must be provided by the provider, and additional delay for the media traffic, TURN is normally used as a last resort when endpoints cannot communicate directly.

TURN User

User authentication name on the TURN server.

TURN host

The IP address or public name of the TURN server.

Password

User authentication password on the TURN server.

On phone:  (MENU) > **SETTINGS** > **ADVANCED** > (PIN) > **NAT TRAVERSAL** (6,2,3).

Advanced

Enable SIP Replaces Default is **Yes**. Setting this option to **No**, will instruct the PBX not to use the SIP replace header. Some PBXes try to take over the bridging functionality from KX-HDV800 using this command, which causes the calls to interrupt.

Enable Blind Transfer Default is **Yes**. Setting this option to **No**, will disable the transfer function (**☛ (MENU) > TRANSFER**) during a call. This may be used if the PBX does not support blind transfer.

Transport

The transport setting only concerns the protocol to be used for SIP messages between the devices involved. These settings do not include the media (the actual call). The settings on the Media tab should be set accordingly.

Note that if you choose to use a secure connection, both units must support it. Otherwise they cannot negotiate a connection. If an incoming call demands a secure TLS or SIPS connection, the KX-HDV800 uses the appropriate protocol even if you have set the phone to use UDP.

Protocol **UDP** (*User Datagram Protocol*) is a protocol on the transport layer in the Internet Protocol Suite. It is a stateless protocol for short messages – datagrams. Stateless implies that it does not establish any connection between sender and receiver in advance. UDP does not guarantee reliability or ordering in the way that TCP does. Datagrams may arrive out of order or go missing without notice. The advantages it offers are speed and efficiency. UDP is the default protocol for SIP.

TCP (*Transmission Control Protocol*) is a protocol on the transport layer in the Internet Protocol Suite. TCP is the standard protocol for Internet communication. TCP keeps track of all individual packets of data, ensuring that they reach the receiver and are put together properly. TCP is not the default protocol for SIP, because it is slower and uses more bandwidth than UDP.

With UDP and TCP, SIP packets travel in plain text. **TLS** (*Transport Layer Security*) is a cryptographic protocol that provides security and data integrity for communications over TCP/IP networks. TLS encrypts the datagrams of the transport layer protocol in use. The secure connection may be to the end device or to the first server (usually the SIP server where the phone is registered). There is no guarantee that there is a secure channel to the end point, but because the SIP server is the only part receiving the user authentication, this is still a rather secure solution.

SETTINGS

SIPS (*Secure SIP*) is a security measure that uses TLS to provide an encrypted end-to-end channel for the SIP messages. To use SIPS, however, both VoIP devices and the SIP server must support it.

① Even if Transport is set to TLS or SIPS, the KX-HDV800 still accepts incoming UDP or TCP signalling.

On phone:  (MENU) > **SETTINGS** > **ADVANCED** > (PIN) > **ACCOUNTS** > **TRANSPORT** (6,2,1,3).

TLS Settings

If you select TLS or SIPS under the transport setting, this additional setting appears on the page.

It may be possible to use secure communication without a certificate and make changes to these settings. In some cases, if you choose TLS or SIPS, the SIP server requires a certificate for user/client verification. This should be specified in the account information.

You can further increase security by requiring verification of the server, or the client when the KX-HDV800 acts as a server for incoming calls.

Enable Blind Transfer

☒ Yes ☐ No

Allow contact rewrite

☒ Yes ☐ No

Disable 'port'

☐ Yes ☒ No

Session timers

☐ Disabled ☒ Optional ☐ Mandatory

Session expiration

1800 seconds

Outbound proxy

Transport

Protocol

☐ UDP ☐ TCP ☒ TLS ☐ SIPS

Local TLS port

5061

Please check corresponding media signalling setting

TLS settings

Method

TLSv1.2

Negotiation timeout

0

Verify server

☐ On ☒ Off

Verify client

☐ On ☒ Off

Require client certificate

☐ On ☒ Off

Certificate

Browse...

No file selected.

Root certificate

Browse...

No file selected.

Private key

Browse...

No file selected.

Private key password

Save

Cancel

Method

The TLS includes a variety of security measures. The methods are defined in the versions of the standard (TLS v1.0, TLS v1.1, TLS v1.2). The default method is TLS v1.2.

Negotiation timeout

The TLS settings are negotiated during a call setup (both incoming and outgoing). If this negotiation does not succeed within the specified time (seconds) the negotiation is aborted. Timeout is disabled with 0 (zero).

23

SETTINGS

Verify client	When set to On, the KX-HDV800 will activate peer verification for incoming secure SIP connections (TLS or SIPS).
Require client certificate	When set to On, the KX-HDV800 rejects incoming secure SIP connections (TLS or SIPS) if the client does not have a valid certificate.
Verify server	When the KX-HDV800 is acting as a client (outgoing connections) using secure SIP (TLS or SIPS) it will always receive a certificate from the peer. If Verify server is set to On, the KX-HDV800 closes the connection if the server certificate is not valid.
Certificate	<p>Here you can upload a certificate to the KX-HDV800 to be used for TLS or SIPS communication.</p> <p>A certificate is a file that combines a public key with information about the owner of the public key, all signed by a trusted third party. If you trust the third party, then you can be sure that the public key belongs to the person/organization named in that file. You can also be sure that everything you decrypt with that public key is encrypted by the person/organization named in the certificate.</p>
Root certificate	<p>The public key in the root certificate is used to verify other certificates. A root certificate is only needed if you have selected client or server verification.</p> <p>A root certificate is signed by the same public key that is in the certificate, a so-called "self-signed" certificate. A typical root certificate is one received from a Certificate Authority.</p>
Private key	<p>Here you can upload a private key to the KX-HDV800 to be used for TLS or SIPS communication.</p> <p>A private key is one of the keys in a key-pair used in asymmetric cryptography. Messages encrypted using the public key can only be decrypted using the private key.</p>
Private key password	The password used for encryption of the private key, if it is encrypted.

NETWORK

⇒ Select **Settings** > **Network**.

KX-HDV800

You are logged in as ADMIN
Logout

StatusPhone bookCall listSettings

BasicSIPNetworkMediaLDAPLLDPWeb interfaceTime & RegionProvisioningSystemConference Application

Network

DHCP

☒ On ☐ Off

IP address

192.168.1.100

Netmask

255.255.255.0

Gateway

192.168.1.1

Primary DNS

Secondary DNS

Hostname

KX-HDV800

Domain

Leave blank for DHCP default

Leave blank for DHCP default

Quality of Service

SIP DiffServ

0

(0-63)

Media DiffServ

0

(0-63)

VLAN

☐ On ☒ Off

VLAN ID

1

VLAN map enable

☐ On ☒ Off

VLAN prio SIP

0 - Best Effort

VLAN prio media

0 - Best Effort

Save

Cancel

DHCP

Dynamic Host Configuration Protocol is used by network devices (clients) to obtain the parameters necessary for operation in the IP network. This protocol reduces system administration workload, allowing devices to be added to the network with little or no manual configuration.

DHCP should be set to On if no other information is given. When set to On, all information on this page will be set automatically.

IP address

IP address of the device (KX-HDV800). The address is provided by the network administrator or service provider if DHCP is not in use.

Hostname

Set to HDV800 as default. Can be changed to suitable name.

Netmask

Usually set to 255.255.255.0 to limit network traffic to the subnet.

Domain

The domain where the device is located. May be left blank.

Gateway

The device or server used for Internet communication.

Primary DNS

The address to the primary DNS (Domain Name System) server - a program or computer that maps a human-recognisable name to its computer-recognisable identifier (IP address).

Secondary DNS

The address of an optional secondary DNS server.

On phone: ⚙ (MENU) > **SETTINGS** > **ADVANCED** > (PIN) > **NETWORK** (6,2,2).

25

Quality of Service

Quality of service is used in IP networks to provide different priority to different applications, users, or to guarantee a certain level of performance to a critical data flow such as voice or video. Differentiated Services or DiffServ is a networking architecture that specifies a simple mechanism for classifying network traffic using a 6-bit field in the header of the IP packets. VLAN (Virtual LAN) is a technology to logically divide a physical network into several logical nets and thus to differentiate traffic.

SIP DiffServ	Enter a value between 0 and 63 to prioritize the SIP messages.
Media DiffServ	Enter a value between 0 and 63 to prioritize the media packets (voice).
VLAN	By enabling this option, all communication to and from KX-HDV800 is done via the VLAN specified under VLAN ID. Note that this VLAN also must be used to communicate with KX-HDV800 via the web interface.
VLAN ID	The ID number to be used for the IP telephony VLAN.
VLAN map enable	Enabling VLAN priority mapping from the DiffServ setting.
VLAN prio SIP	Set a value between 0 and 7 to prioritize the SIP messages in the VLAN.
VLAN prio media	Set a value between 0 and 7 to prioritize the media packets in the VLAN.

On phone:  (MENU) > **SETTINGS** > **ADVANCED** > (PIN) > **NETWORK** > **ETHERNET** > **VLAN**
(6,2,2,2,1).

TLS.

MEDIA

⇒ Select **Settings** > **Media**.

KX-HDV800

StatusPhone bookCall listSettings

BasicSIPNetworkMediaLDAPLLDPWeb interfaceTime & RegionProvisioningSystemConference Application

Codec

Priority

G7224 - High

G711 Alaw3

G711 Ulaw2

G7291 - Low

Security

☒ Disabled☐ Optional☐ Mandatory

SRTPSecure signalling☐ No☒ TLS☐ SIPS

Please check corresponding SIP transport setting

VAD

Enable VAD☐ Yes☒ No

DTMF

☒ RFC 2833☐ SIP Info☐ Inband

DTMF Signalling

RFC 2833 payload type101

Minium 96 and maximum 127

Advanced

First RTP port4000

Disable RTCP advertising☐ Yes☒ No

SaveCancel

The media settings determine how audio is sent between the devices. The devices negotiate via SIP before a call is connected. All devices must support the same media types, codecs and security settings.

Codec

Codecs are used to convert an analogue voice signal to a digitally encoded version and vice versa. Codecs vary in the sound quality they deliver and the bandwidth required. The KX-HDV800 supports the most common codecs and each codec can be given a precedence depending on your requirements for high quality audio or low bandwidth use.

The priority can be set to from 4 (high) to 1 (low) or 0 (disabled)

G722

G.722 is an ITU-T standard codec that provides 7 kHz wideband audio at a data rate within 64 kbit/s. It offers greatly improved speech quality compared with older narrowband codecs such as G.711, but requires a high quality network connection between the devices.

SETTINGS

- G711 Alaw** G.711 is an ITU-T standard codec that uses audio companding. Companding algorithms reduce the dynamic range of an audio signal. In analogue systems, this can increase the signal-to-noise ratio achieved during transmission and, in the digital domain, can reduce the quantization error.
- Two main compression algorithms are defined in the standard, the μ -law algorithm (used in North America and Japan) and A-law algorithm (used in Europe and the rest of the world).
- G711 Ulaw** See G711 μ -law above.
- G729** G.729 is an ITU-T standard codec that operates at 8 kbit/s. It is mostly used in VoIP applications with low bandwidth requirement.

On phone:  (MENU) > **SETTINGS** > **ADVANCED** > (PIN) > **MEDIA** > **CODEC** (6,2,4,1).

Security

The media in VoIP calls is usually sent using the RTP protocol (Real-time Transport Protocol). RTP is a standardized packet format for delivering audio and video over the Internet.

SRTP (Secure Real-time Transport Protocol) is an extension of RTP to provide encryption, message authentication and integrity for the audio and video streams.

All devices must support SRTP to establish a connection. It is therefore possible to set SRTP as disabled, optional or mandatory.

- SRTP**
- If set to disabled, the media is sent using RTP. Note that despite this setting, the KX-HDV800 will still use a secure channel if the opposite device demands it.
- If set to optional or mandatory, a padlock will be shown in the bottom right-hand corner of the screen. If the other devices support SRTP, the padlock will be locked. Otherwise, an open padlock will be displayed.
- If set to mandatory, the call will not be connected if the other devices do not support SRTP.
- Secure signalling** The SIP messages (signalling) and the SRTP cipher key are sent on a different channel than the media and are not affected by the RTP/SRTP setting. To ensure a secure connection, the signalling must be secured using **TLS** or **SIPS**, see page 22. Note that the SIP transport setting must be set accordingly.

On phone:  (MENU) > **SETTINGS** > **ADVANCED** > (PIN) > **MEDIA** > **SECURITY** (6,2,4,4).

SETTINGS

VAD

Voice Activity Detection (speech detection) is a technique used in speech processing to detect the presence or absence of human speech in regions of audio. In VoIP applications, VAD is mainly used to avoid unnecessary coding and transmission of silence packets, saving on computation and network bandwidth.

On phone:  (MENU) > **SETTINGS** > **ADVANCED** > (PIN) > **MEDIA** > **VAD** (6,2,4,2).

DTMF

DTMF (Dual-tone multi-frequency) signalling is used for telephone signalling over the line to the phone switch or PBX.

If the device itself generates the tones and they are sent in the voice-frequency band, the method is called **Inband**. This is not the best method when using VoIP. Low bit rate codecs may corrupt the signalling tones and make it difficult for the switch to identify them.

RFC 2833 is a method of carrying DTMF signals in RTP packets using a separate RTP payload format. With this method a PSTN gateway reproduces the DTMF tones sent from the end device.

With **SIP Info** the DTMF signals are sent as SIP requests. The SIP switch creates the tones if the call is transferred to the PSTN.

Use RFC 2833 or SIP Info as preferred methods. Switch to inband only if you encounter problems using DTMF signalling with your PBX/SIP switch.

On phone:  (MENU) > **SETTINGS** > **ADVANCED** > (PIN) > **MEDIA** > **DTMF SIGNALLING** (6,2,4,3).

Advanced

First RTP port	If the RTP packets must be directed to a specific port series, the first port number is set here.
----------------	---

LDAP

⇒ Select **Settings** > **LDAP**.

The screenshot shows the KX-HDV800 settings interface. At the top, it says 'KX-HDV800' and 'You are logged in as ADMIN Logout'. Below this is a navigation bar with tabs: Status, Phone book, Call list, Settings, Basic, SIP, Network, Media, LDAP, LLDP, Web interface, Time & Region, Provisioning, System, and Conference Application. The 'LDAP' tab is selected. The 'LDAP configuration' section contains the following fields:

- Enable LDAP: ☐ Yes ☒ No
- Name filter:
- Server URL:
- Search base:
- Username:
- Password:
- Max hits:
- Display name:
- Sort results: ☒ Yes ☐ No
- Number attributes:
- Country code:
- Area code:
- External prefix:
- Min length for external prefix:

At the bottom of the configuration section are 'Save' and 'Cancel' buttons.

KX-HDV800 has support for an external phone book, which means it can communicate with a directory server using LDAP (Lightweight Directory Access Protocol). The built in search function dynamically filters the content from the LDAP database, based on the search characters the user enter.

To make the LDAP phone book available, the administrator has to activate and configure the LDAP feature.

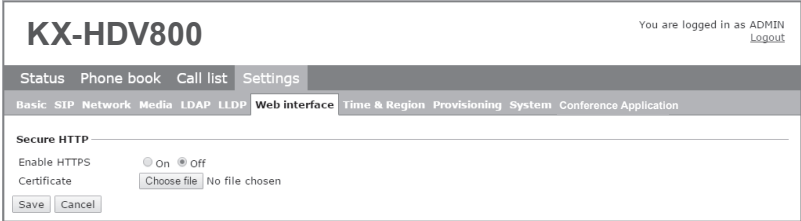
- | | |
|-------------|--|
| Enable LDAP | The LDAP feature is disabled by default because it has to be configured. |
| Name filter | Defines how the entered search characters are used. The filter is designed conforming to the string representation of LDAP search filters described in RFC2254. The character % in the filter string will be replaced with the search character entered by the user.
Example:
((sn=%*)(cn=%*)) – All entries with the search characters in the beginning of the sn OR cn attribute are presented to the user. |
| Server URL | The IP address of the LDAP server host. Supports ldap and ldaps. |
| Search base | The DN (distinguished name) of the search base
Example:
dc=domain, dc=com. |
| Username | Leave this field blank if the LDAP server does not require a username. |
| Password | Leave this field blank if the LDAP server does not require user-name and password. |

SETTINGS

Max hits	The maximum number of hits to return for each LDAP search.
Display name	<p>Specifies how the search hits shall be presented on the display in KX-HDV800.</p> <p>Example:</p> <p>%cn – shows the cn attribute.</p> <p>%givenName %sn – shows the givenName attribute and the sn attribute with a space in between.</p>
Sort results	Sorts the search hits based on the Display name.
Number attributes	<p>Here you define the attributes that shall be displayed for a selected search hit.</p> <p>Example:</p> <p>mobile telephoneNumber – shows the mobile phone number and office phone number on separate rows for the selected Display name.</p>
Country code	By entering the country code where the phone is located, the country code in any phone number attribute is ignored, if it is identical.
Area code	By entering the area code where the phone is located, the area code in any phone number attribute is ignored, if it is identical.
External prefix	If a special prefix is needed to dial external numbers, it should be added here. Use this if you for example need to dial 0 to get a dialing tone.
Min length for external prefix	Restricts the external prefix to be added only if the phone number is longer than the min length. This makes it possible to use short internal numbers.
Exact length for no external prefix	The external prefix is not added if the phone number has exactly the entered length.
Number prefix for no external prefix	All numbers that start with this number will not have the external prefix added. Useful if you know that all internal numbers start with a certain number.

WEB INTERFACE

⇒ Select **Settings** > **Web interface**.



The web server in the KX-HDV800 supports secure connections using HTTPS.

Enable HTTPS Set Enable HTTPS to On if you need a secure communication between the PC used for setup and the phone.

Certificate To use HTTPS you need to upload a certificate to the phone.

On phone: ⚙️ (MENU) > **SETTINGS** > **ADVANCED** > (PIN) > **WEB INTERFACE** (6,2,7).

TIME & REGION

⇒ Select **Settings** > **Time & Region**.

KX-HDV800

You are logged in as ADMIN
Logout

StatusPhone bookCall listSettings

BasicSIPNetworkMediaLDAPLLDPWeb interfaceTime & RegionProvisioningSystemConference Application

Time

Enable NTP

☒ On

☐ Off

Time

12:10:19

Date

2017-02-09

Timezone

UTC+1

00

NTP Server

pool.ntp.org

Region

Region

SWE Sweden

Daylight saving

Enable DST

☒ Yes

☐ No

DST Timezone (hh:mm)

UTC+2

00

DST Mode

☒ Automatic

☐ Manual

Save

Cancel

Time

- Enable NTP

NTP (*Network Time Protocol*) is a protocol for distributing the *Coordinated Universal Time* (UTC) by means of synchronizing the clocks of computer systems over packet-switched, variable-latency data networks.
- Time

This field shows the actual time if NTP is enabled. Otherwise enter the correct time (hh:mm:ss) and save the setting.
- Date


This field shows the actual date if NTP is enabled. Otherwise enter the correct date (yyyy-mm-dd) and save the setting.
- Timezone

Select the UTC time zone in your country.
- Daylight saving

Select the Yes radio button if DST (*Daylight Saving Time* or *Summer Time*) is currently used in your country. Note that this setting only adjusts the time by one hour and does not change the time automatically when the DST starts and ends.

SETTINGS

NTP Server The NTP pool is a dynamic collection of networked computers that volunteer to provide highly accurate time via NTP to clients worldwide. These computers are part of the pool.ntp.org domain and part of several subdomains divided by geographical zones. They are distributed to NTP clients via round robin DNS.

On phone:  (MENU) > **SETTINGS** > **ADVANCED** > (PIN) > **TIME** (6,2,5).

Region

Select the region where you are. This setting determines the signalling (disconnect tone, busy tone, etc).

On phone:  (MENU) > **SETTINGS** > **ADVANCED** > (PIN) > **REGION** (6,2,6).

Daylight saving

Enable DST Select the Yes radio button if DST (Daylight Saving Time or Summer Time) is used in your country.

DST Timezone Select the offset from UTC time when daylight saving is in use.

DST Mode When set to Automatic, KX-HDV800 uses dates stored in the phone to adjust for DST. When set to Manual, you need to manually set the offset two times a year.

Start/Stop fixed date Set to Yes if DST changes the same date every year in your country. Then select the time and date it changes.

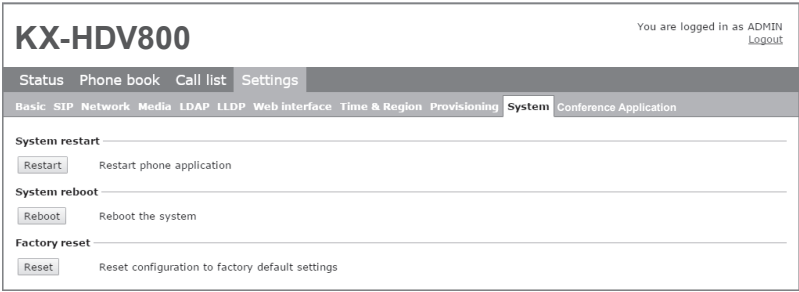
Set to No if DST changes a specific week and day each year. (For instance third sunday in March.) Then select the month, week and time it changes.

PROVISIONING

See “PROVISIONING – UPGRADE AND CONFIGURATION” on page 38.

SYSTEM

⇒ Select **Settings** > **System**.



Application restart

The Restart button restarts the phone application. This takes less than 30 seconds.

On phone: ⚙️ (MENU) > **SYSTEM** > **RESTART** (7,1).

System reboot

The Reboot button reboots the conference phone. The starting procedure may take about two minutes.

On phone: ⚙️ (MENU) > **SYSTEM** > **REBOOT** (7,2).

Factory reset

The Reset button resets the KX-HDV800 to factory default settings. All personal settings, including account information, are erased.

On phone: ⚙️ (MENU) > **SYSTEM** > **FACTORY RESET** (7,3).

Hard reset to factory settings

See page 37 about resetting the phone if you have forgotten the Admin PIN code.

CONNECTING A WIRELESS HEADSET

⇒ Connect the headset to the Aux port on KX-HDV800.

The microphones from the KX-HDV800 and the wireless headset will work simultaneously and transmit the call to other participants in the phone conference.

Please refer to the headset manual for further information.

Turning off the internal speakers when using a headset

The internal speakers can be turned off temporarily if you wish to use the KX-HDV800 as a personal telephone with a headset.

⇒ During a call, select  (MENU) > **HEADSET**.

⇒ Select **YES** when asked "SPEAKER OFF?".

① The speakers come on automatically when the call is ended.

Reset configuration

If you have forgotten the Admin PIN code, the only way to reset it to default is to do a hard factory reset. This is the same as the Factory reset in the system menu (**⚙ (MENU) > SYSTEM > FACTORY RESET**).

- ① This erases all settings including account information and contacts!
- ⇒ Disconnect the power supply cable. Note that this is the same as the network cable if the phone uses Power over Ethernet.
- ⇒ Press and hold the **⚙ (MENU)** button while you connect the cable again (i.e. starts the KX-HDV800). Hold the button pressed until the SYSTEM RECOVERY menu is shown on the display.
- ① You can press any other button than **1**, **2**, or **3** to start the phone without resetting.
- ⇒ Press **1** to select **Reset configuration** and confirm with **OK**.
- ⇒ Upgrade to the latest version of the software when the phone has started and redo the setup of account and other settings (see page 11).

Restore firmware

This replaces the current software with the one supplied with the phone. All settings are erased.

- ⇒ Disconnect the power supply cable. Note that this is the same as the network cable if the phone uses Power over Ethernet.
- ⇒ Press and hold the **⚙ (MENU)** button while you connect the cable again (i.e. starts the KX-HDV800). Hold the button pressed until the SYSTEM RECOVERY menu is shown on the display.
- ① You can press any other button than **1**, **2**, or **3** to start the phone without restoring the firmware.
- ⇒ Press **3** to select **Restore firmware** and confirm with **OK**.
All content in the phone's memory is erased and the firmware supplied with the phone is written to the memory.
- ⇒ Upgrade to the latest version of the software when the phone has started and redo the setup of account and other settings (see page 11).

FIRMWARE UPGRADE ON A SINGLE PHONE

It is possible to download the latest version, via the Panasonic website (<https://panasonic.net/cns/pcc/support/sipphone/>), and then install the file via the web interface or using a SD card (sold separately).

Using the web interface

⇒ Select **Settings > Provisioning**.

The screenshot shows the KX-HDV800 web interface. At the top, it says "KX-HDV800" and "You are logged in as ADMIN Logout". Below this is a navigation bar with tabs: Status, Phone book, Call list, Settings, Provisioning, System, and Conference Application. The "Provisioning" tab is selected. Under "Provisioning", there are three sections: "Firmware upgrade", "Configuration", and "Device management". The "Firmware upgrade" section shows the current version as 2.5.48 and a file input field containing "HDV800_v2.0.3.kt" with an "Upgrade" button. The "Configuration" section has a "File" input field with a "Choose file" button and an "Import" button. The "Device management" section has several options: "Enable" (On/Off), "Use DHCP option" (On/Off), "DHCP option" (43: Vendor specific), "File server address" (empty field), "HTTPS protocol" (TLSv1), and "Check server cert." (On/Off).

⇒ If you choose to upgrade, select version in the list box and click on the **Upgrade** button.

The browser window and the KX-HDV800 display shows that the upgrading has begun.

① The download and installation can take several minutes. Do not interrupt the upgrade and do not disconnect plugs to the KX-HDV800 during the upgrade. Interrupting the upgrade may render the conference phone inoperable.

When installation is complete, the text "Upgrade Complete. The unit will be re-booted." is shown in your browser, and after a while you hear the Panasonic music signature, which indicates that the conference phone has started.

Upgrading from downloaded file

It is possible to download a firmware file from

<https://panasonic.net/cns/pcc/support/sipphone/> and install it on the KX-HDV800 from the local hard disk.

- ⇒ Download the firmware file from **<https://panasonic.net/cns/pcc/support/sipphone/>**.
- ⇒ Click on the **Browse...** button and locate and select the downloaded file.
- ⇒ Click on the **Upgrade** button.

Upgrading from SD card (sold separately)

Upgrading from SD card may be suitable if you have many phones to upgrade. The phones do not have to be connected to the network.

- ⇒ Download the latest firmware as above and save it on a SD card.
- ⇒ Put the SD card in the phone you want to upgrade.
- ⇒ Disconnect the power supply cable. Note that this is the same as the network cable if the phone uses Power over Ethernet.
- ⇒ Press and hold the **⚙ (MENU)** button while you connect the cable again (i.e. starts the KX-HDV800). Hold the button pressed until the SYSTEM RECOVERY menu is shown on the display.
- ① You can press any other button than **1**, **2**, or **3** to start the phone without any change.
- ⇒ Press **2** to select **SD-card upgrade**.

The KX-HDV800 is upgraded with the firmware file on the SD card and starts when the upgrade is done.

After upgrading

If DHCP is used in the network, the IP address may have been changed. If the web browser loses contact with KX-HDV800, check the IP address on the conference phone (see “USING THE WEB INTERFACE” on page 8).

USING A CONFIGURATION FILE

It is possible to save a configuration xml file to be used as:

- Backup (i.e. if the system has been reset to factory default)

PROVISIONING – UPGRADE AND CONFIGURATION

- Configuration interface (there are some settings that are not configurable via the web interface)
- Management tool (export, edit and import settings to a set of phones instead of doing the settings on each phone)
- Use with a Device Management server, see page 45.

The structure of the xml file is as follows:

<locale>

<region>

<recording>

<enable>

<logging>

<level>

The phone application logs messages to log facility LOCAL0.
Log level 1–5 (equivalent to Fatal–Trace)

<log_sip>

Log SIP messages to log facility LOCAL1. Default is true.

<remote_log>

Log messages to a remote log server. Default is false.

<remote_host />

Remote log server.

<network>

<net>

<dhcp>

Specify if DHCP should be used to obtain network settings. If so, the other network settings won't be used.

<ip>

Specify the IP address of the KX-HDV800.

<netmask>

The netmask of the IP address.

<gateway>

Specify the default gateway to be used.

<dns>

Specify at most two Domain Name Servers to be used.

<dns>

<hostname>

Specify host name.

<domain />

Specify domain name.

<vlan>

<enable>

Virtual LAN enabled if set to true

<id>

VLAN ID.

<std_prio_map>

<sip_priority>

<media_priority>

<ether_8021x>

<enable>

<username />

<eap_md5>

<enable>

PROVISIONING – UPGRADE AND CONFIGURATION

```
        <password>
    <eap_tls>
        <enable>
        <password>

<qos>
    <dscp_sip>
    <dscp_media>

<time>
    <ntp>
    <timezone>
    <daylight_save>
    <ntps>
```

<sip>

<udp_transport>	Specify if UDP shall be used as transport.
<udp_port>	Specify the UDP port to listen to.
<tcp_transport>	Specify if TCP shall be used as transport.
<tcp_port>	Specify the TCP port to listen to.
<tls_transport>	Specify if TLS shall be used as transport.
<sips_transport>	Specify if SIPS shall be used as transport.
<tls_port>	Specify the TLS port to listen to.
<rtp_port>	Specify the start port for RTP traffic.
<outbound_proxy />	Specify the URL of outbound proxies to visit for all outgoing requests. The outbound proxies will be used for all accounts and will be used to build the route set for outgoing requests. The final route set for outgoing requests will consist of the outbound proxies and the proxy configured in the account.
<use_stun>	Use Simple Traversal of UDP through NATs (STUN) for NAT traversal. Default is no.
<stun_domain />	Specify domain name to be resolved with DNS SRV resolution to get the address of the STUN servers. Alternatively application may specify stun_host and stun_relay_host instead.
<stun_host />	Specify STUN server to be used in “HOST[:PORT]” format. If port is not specified, default port 3478 will be used.
<use_turn>	Use Traversal Using Relay NAT (TURN) for NAT traversal. Default is no.
<turn_host />	Specify TURN relay server to be used.
<turn_tcp>	Use TCP connection to TURN server. Default is false.
<turn_user />	TURN username.
<turn_passwd />	TURN password.
<nat_type_in_sdp>	Support for adding and parsing NAT type in the SDP to assist troubleshooting. The valid values are: 0: no information will be added in SDP and parsing is disabled 1: only the NAT type number is added 2: add both NAT type number and name

PROVISIONING – UPGRADE AND CONFIGURATION

<require_100rel>	Specify whether support for reliable provisional response (100rel and PRACK) should be required by default. Note that this setting can be further customized in account configuration.
<use_srtp>	Specify default value of secure media transport usage. Note that this setting can be further customized in account configuration. 0: SRTP will be disabled, and the transport will reject RTP/SAVP offer. 1: SRTP will be advertised as optional and incoming SRTP offer will be accepted. 2: The transport will require that RTP/SAVP media shall be used.
<srtp_secure_signaling>	Specify whether SRTP requires secure signalling. This option is only used when use_srtp option above is non-zero. Note that this setting can be further customized in account configuration. 0: SRTP does not require secure signalling 1: SRTP requires secure transport such as TLS 2: SRTP requires secure end-to-end transport (SIPS)
<codec>	
<type>	Codec type
<name>	Codec name
<prio>	Codec priority (0-4)
<dtmf>	DTMF signalling. Default is 2. 0: In-band 1: SIP message 2: RTP message
<no_vad>	Disable VAD. Default is VAD enabled.
<ec_tail>	Echo canceller tail length, in milliseconds.
<enable_ice>	Enable ICE?
<enable_relay>	Enable ICE relay?
<enable_presence>	Enable the use of presence signalling.
<tls>	
<tls_password />	Password for the private key
<tls_method>	TLS protocol method from pjsip_ssl_method, which can be: 0: TLS v1.0 1: TLS v1.1 2: TLS v1.2 (Default)
<tls_verify_server>	Verify server certificate.
<tls_verify_client>	Verify client certificate.
<tls_require_client_cert>	Require client certificate.
<tls_neg_timeout>	TLS negotiation timeout in seconds to be applied for both outgoing and incoming connections. If zero, no timeout is used.
<account>	
<valid>	If this account information is valid or not.
<name>	User defined name of the account
<id>	The full SIP URL for the account.

PROVISIONING – UPGRADE AND CONFIGURATION

<registrar>	This is the URL to be put in the request URI for the registration.
<publish_enabled>	If this flag is set, the presence information of this account will be published to the server where the account belongs.
<initial_auth>	If this flag is set, the authentication client framework will send an empty Authorization header in each initial request.
<initial_algo />	Specify the algorithm to use when empty Authorization header is to be sent for each initial request (see above).
<pidf_tuple_id />	Optional PIDF tuple ID for outgoing PUBLISH and NOTIFY. If this value is not specified, a random string will be used.
<force_contact />	Optional URI to be put as Contact for this account. It is recommended that this field is left empty, so that the value will be calculated automatically based on the transport address.
<require_100rel>	Specify whether support for reliable provisional response (100rel and PRACK) should be required for all sessions of this account.
<proxy_uri />	Optional URI of the proxies to be visited for all outgoing requests that are using this account (REGISTER, INVITE, etc).
<reg_timeout>	Optional interval for registration, in seconds. If the value is zero, default interval will be used.
<cred>	Array of credentials. Normally, if registration is required, at least one credential should be specified to successfully authenticate the service provider. More credentials can be specified, for example when it is expected that requests will be challenged by the proxies in the route set.
<realm>	Realm. Use "*" to make a credential that can be used to authenticate any challenges.
<scheme />	Scheme (e.g. "digest").
<username>	Authentication name
<cred_data_type>	Type of data (0 for plaintext password).
<cred_data>	The data, which can be a plaintext password or a hashed digest.
<auto_update_nat>	This option is useful for keeping the UDP transport address up to date with the NAT public mapped address. When this option is enabled and STUN is configured, the library will keep track of the public IP address from the response of REGISTER request. Once it detects that the address has changed, it will unregister current Contact, update the UDP transport address and register a new Contact to the registrar.
<ka_interval>	Set the interval for periodic keep-alive transmission for this account. If this value is zero, keep-alive will be disabled for this account. The keep-alive transmission will be sent to the registrar's address after successful registration.
<ka_data />	Specify the data to be transmitted as keep-alive packets. Default: CR-LF.
<use_srtp>	Specify whether secure media transport should be used for this account. 0: SRTP will be disabled and the transport will reject RTP/SAVP offer. 1: SRTP will be advertised as optional and incoming SRTP offer will be accepted. 2: The transport will require that RTP/SAVP media is used.

PROVISIONING – UPGRADE AND CONFIGURATION

<srtp_secure_signaling> Specify whether SRTP requires secure signalling. This option is only used when use_srtp option above is non-zero.
0: SRTP does not require secure signalling
1: SRTP requires secure transport such as TLS
2: SRTP requires secure end-to-end transport (SIPS)

<account>

Same as above for account 2

<provisioning>

<upgrade>
<url> Place to find software upgrades. The supported URL types are: HTTP, FTP, and TFTP.

<dev_mngt>
<enable> Device management enabled, true or false.
<use_dhcp_option> Use DHCP option for DM server address.
<dhcp_option> Specification of which DHCP option to use.
<file_server_address> DM server address if not provided by DHCP option.
<pagename /> Base name of configuration files to download
<type /> Configuration file type specification
<update_interval> Timing for downloading files. Shall be entered in crontab format:
* * * * * where the * stands for minute (0–59), hour (0–23), day of month (1–30), month (1–12), day of week (0–7) (Sunday =0 or 7)
Example:
0 6 * * * = the files are downloaded daily at 6:00.

<https_check_srv_cert> Controls server certificate, true or false.
<https_protocol> Possibility to set https protocol if open-ssl auto detection fails.

<www>

<enable_https> Secure communication to the KX-HDV800 web server. Default is false.

<ldap>

<enable> LDAP enabled, true or false.
<name_filter> NAME filter according to RFC2254
<server_url> LDAP server address
<search_base> The DN (distinguished name) of the search base
<username />
<password />
<max_hits>
<country_code>
<area_code>
<external_prefix />
<min_length_for_ext_prefix />
<exact_length_for_no_ext_prefix />
<number_prefix_for_no_ext_prefix />

<number_attributes>

<display_name>

<sort_results>

Export configuration

- ⇒ Select **Settings > Provisioning**.
- ⇒ Click on the **Export** button under **Configuration**.
The configuration file is shown in the web browser.
- ⇒ Choose to save the page as an xml file.
The xml file is as default saved in your folder for downloaded files.
- ⇒ If necessary, edit the xml file in a suitable editor.

Import configuration

- ⇒ Click on the **Browse...** button under **Configuration**.
- ⇒ Select the xml file and choose to open it.
- ⇒ Click on the **Import** button.

USING A DEVICE MANAGEMENT SERVER

Using Device management facilitates the upgrading and configuration of multiple conference phones. To use this feature, the Device management needs to be enabled

PROVISIONING – UPGRADE AND CONFIGURATION

(default) and configured and the appropriate files must be located on a server reachable from all phones, here called a device management server.

The configuration and firmware download are controlled with a configurable frequency. The default value is once every 30 minutes. (Note: The interval can only be edited directly in the configuration file.)

Configuration priorities

Because the same configuration parameters can be entered in multiple locations, there is a need for priorities. The local configuration files have the highest priority followed by the global configuration file. Configuration entered on the unit itself, via the web interface or directly on the phone, is overridden the next time the configuration files are downloaded.

① Note one exception. Phone language entered on the unit will take precedence.

Files on the device management server

Global configuration file

The global configuration file contains the basic configuration – all settings that are common for all conference phones on your location. The easiest way to create this file is simply to configure one phone and export the configuration file or use the built in configuration file creator.

The default name for this file is HDV800.xml, but it is possible to create a custom name by using the pagename element in the configuration file. It is also possible to refer to a cgi, php, asp, js or jsp file, instead of the xml file, if this is declared using the type element in the configuration file.

KX-HDV800 searches for configuration files in the following order:

	Type parameter value	Result
1	<nothing>	<pagename>.xml
2	cgi	<pagename>.cgi?phone_model=HDV800>
3	%""%	<pagename>.php?phone_model=HDV800>
4	asp	<pagename>.asp?phone_model=HDV800>
5	E	<pagename>.js?phone_model=HDV800>
6	E %	<pagename>.jsp?phone_model=HDV800>
:	<any name>	<pagename>.<any name>? phone_model=HDV800
=	auto	1, 2, 3, 4, 5 and 6 will be tried in that order

PROVISIONING – UPGRADE AND CONFIGURATION

Local configuration file

The local configuration file contains configuration parameters that are unique for every conference phone. The settings in this file takes precedence over the settings in the global configuration file.

The default name for this file is HDV800-**<MAC>**.xml, where **<MAC>** is the MAC address of the specific conference phone. The MAC address should be written without colons.

It is possible to create a custom name by using the pagename element in the configuration file. It is also possible to refer to a cgi, php, asp, js or jsp file, instead of the xml file, if this is declared using the type element in the configuration file.

KX-HDV800 searches for configuration files in the following order:

Type parameter value	Result
1 <nothing>	<pagename>-<MAC>.xml
2 cgi	<pagename>.cgi? phone_model=HDV800ð=<MAC>
3 %""%	<pagename>.php? phone_model=HDV800ð=<MAC>
4 asp	<pagename>.asp? phone_model=HDV800ð=<MAC>
5 E	<pagename>.js? phone_model=HDV800ð=<MAC>
6 E %	<pagename>.jsp? phone_model=HDV800ð=<MAC>
: <any name>	<pagename>.<any name>? phone_model=HDV800ð=<MAC>
= auto	1, 2, 3, 4, 5 and 6 will be tried in that order

Firmware binary

Contains the firmware binary that will be downloaded and installed by KX-HDV800 if the metadata file shows that this is a newer version than the present installed. The binary file can be downloaded from **<https://panasonic.net/cns/pcc/support/sipphone/>**.

Firmware metadata file

A metadata file in xml format with information of the firmware version in the binary file. The file is used to check if the binary file should be downloaded to the phone or not.

The name of this file shall be HDV800_fw_version.xml. The file shall contain the following elements in xml format.

```
<firmware_version>
<version>X.X.X </version>   Eg. 2.0.3
<filename>xxxx </filename>  Eg. HDV800_v2.0.3.kt
<checksum>XXXX </checksum> MD5 checksum of the firmware binary
</firmware_version>
```

Device management configuration in KX-HDV800

⇒ Select **Settings** > **Provisioning**.

KX-HDV800

You are logged in as ADMIN
[Logout](#)

StatusPhone bookCall listSettings

BasicSIPNetworkMediaLDAPLLDPWeb interfaceTime & RegionProvisioningSystemConference Application

Firmware upgrade

Current version:2.5.48

File

Choose file

No file chosen

Upgrade

Configuration

File

Choose file

No file chosen

Import

Export

Export

Passwords will not be exported

Device management

Enable

☒ On☐ Off

Use DHCP option

☒ On☐ Off

DHCP option

43: Vendor specific

File server address

HTTPS protocol

TLSv1

Check server cert.

☒ On☐ Off

Certificate

Choose file

No file chosen

Root certificate

Choose file

No file chosen

Private key

Choose file

No file chosen

Save

Device management

- Enable

On enables Device management.
- Use DHCP option

Set to on if you want to use DHCP option for DM server address.
- DHCP option

Select the DHCP option used for the DM server address.
43: Vendor specific
56: DHCP message
60: Class Id
61: Client Id
66: Server-name
67: Bootfile-name
- File server address

DM server address if not provided by DHCP option.
- HTTPS protocol

Default is auto, but can be set to SSLv2 or SSLv3 if open-ssl auto detection fails.
- Check server cert.

Enable authentication with certificate.
- Certificate

Here you can upload a certificate to the KX-HDV800 to be used for authentication when using Device management.
- Root certificate

The public key in the root certificate is used to verify other certificates when using Device management.
- Private key

Here you can upload a private key to the KX-HDV800 to be used for authentication when using Device management.

 Read more about certificates on page 24.

Setting up a Device management server

This is a description of a manual method to create the configuration files.

- ⇒ Select **Settings > Provisioning**.
- ⇒ Enable Device management and enter the server information.

Creating a global configuration file

- ⇒ Configure one phone with the basic configuration.
- ⇒ Click on **Export** to create a configuratuion file.
- ⇒ If necessary, edit the xml file in a suitable editor.
- ① Some parameters can't be entered via the web interface (update frequency, page-name, and filetype).
- ① To avoid confusion, it may be wise to delete the local information from the file (eg. account information).
- ⇒ Save the file with the name **HDV800.xml** on the File server address specified above.

Creating local configuration files

- ⇒ Save a copy of the configuration file for each conference phone on your location with content only in the elements that shall be unique for each conference phone (eg. account information).

The default name for each file is HDV800-<MAC>.xml, where <MAC> is the MAC address of the specific conference phone.

- ⇒ Place the configuration files on the File server address specified above.

Firmware binary

- ⇒ Place the firmware binary file on the Provisioning server.
- ⇒ Create a Firmware metadata file according to page 47 and place it on the File server address specified above.
- ① Depending on the server used, and the security settings, there might be necessary to add the file type .kt to the MIME settings on the server. This is easily checked by trying to download the kt file from a web browser.


IMPORTING AND EXPORTING CONTACTS

You can import contacts from a comma separated values (CSV) file. One way of creating a CSV file is using Microsoft® Excel® and saving the file in CSV format.

Enter the names of the contacts in the first column and their phone numbers or URIs in the second. Do not use hyphens or spaces in the number. Note that Excel ignores zeros at the beginning of numbers. The cells must therefore be formatted as text.

	A	B	C	D	E	F
1	Name	Telephone				
2	Allen, Jerry	+81921234567				
3	Anderson, Justin	+81921234567				
4	Andrews, Fanny	+81921234567				
5	Berg, David	+81921234567				
6	Berlin office	+81921234567				
7	Bewers, Darren	+81921234567				
8	Bjork, Markus	+81921234567				
9	Branshaw, Liw	+81921234567				
10	Carling, Richard	+81921234567				
11	Carlsson, Julia	+81921234567				
12	Claesson, Nicole	+81921234567				
13	Collins, David	+81921234567				
14	Cordin, Justin	+81921234567				
15	Crown, Juanito	+81921234567				
16	Evalders, Julie	+81921234567				
17	Gardelius, Stefan	+81921234567				
18	Hellberg, Mark	+81921234567				
19	Konrads, Ray	+81921234567				
20	Langdon, Steve	+81921234567				
21	Leander, Adam	+81921234567				
22	Lowendahl, Roger	+81921234567				
23	Luong, Xi	+81921234567				
24	Magret, Robin	+81921234567				
25	Mowat, Leo	+81921234567				
26	Mowji, Al	+81921234567				
27	Nelson, Mike	+81921234567				
28	Nyberg, Paul	+81921234567				

 It is normally possible to export contact books stored in your PC in CSV format.

 The way the number can be written may depend on the SIP PBX being used, but normally you can use:

- Complete phone number, including country code
- Phone number, including area code
- Local phone number only
- Internal speed dial number (with company's own PBX)
- URI, e.g. **sip:user@company.com**
- URI with IP address, e.g. **sip:10.10.1.100** (within a local network)

Importing contacts

- ⇒ Select **Phone Book**.
- ⇒ Click on the **Scroll...** button under the heading Import in the web window.
- ⇒ Open your CSV file.
- ⇒ Click on **Import**.
- ① The name is limited to 15 characters, since the KX-HDV800 screen cannot display more than 15 characters.

Exporting contacts

You can export your contacts as a CSV document in order to import them into another phone.

- ⇒ Click on **Export**.
- ⇒ Save the document.

IMPORTING AND EXPORTING CONFERENCE GROUPS

The conference groups can be imported and exported in the same way as the contacts in the phone book, but use a three column csv instead of a two column csv.

	A	B	C	D	E	F	G
1	Group	Name	Number				
2	Sales	Carlsson, Julia	+81921234567				
3	Sales	Berg, David	+81921234567				
4	Sales	Berlin office	+81921234567				
5	Sales	UK office	+81921234567				
6	Development	Bjork, Markus	+81921234567				
7	Development	Branshaw, Liw	+81921234567				
8	Development	Luong, Xi	+81921234567				
9	Development	Lowendahl, Roger	+81921234567				
10							
11							
12							
13							
14							

CHECKING STATUS AND LOGS

The tabs under Status show the settings on corresponding tabs plus device info and logs.

DEVICE

⇒ Select **Status > Device**.

KX-HDV800

You are logged in as ADMIN
[Logout](#)

Status

Phone book

Call list

Settings

Device

Network

Time & Region

SIP

Media

Log

Hardware

Product name

KX-HDV800

ID

93212548

MAC address

00:17:7D:12:0A:36

Bluetooth address

C4:64:E3:B3:A7:66

Software

Application

1.3.2

The Device tab shows phone information including ID, network port and current software version.

On phone: ⚙ (MENU) > **STATUS > DEVICE** (8,6).

NETWORK

⇒ Select **Status > Network**.

KX-HDV800

Status

Phone book

Call list

Settings

Device

Network

Time & Region

SIP

Media

Log

Licenses

Network

DHCP

☒ On

☐ Off

IP address

192.168.0.55

Hostname

KX-HDV800

Netmask

255.255.255.0

Domain

Gateway

Primary DNS

Secondary DNS

Quality of Service

SIP DiffServ

0

Media DiffServ

0

VLAN

☐ On

☒ Off

VLAN ID

1

VLAN map enable

☐ On

☒ Off

VLAN prio SIP

0 - Best Effort

VLAN prio media

0 - Best Effort

On phone: ⚙ (MENU) > **STATUS > NETWORK** (8,2).

CHECKING STATUS AND LOGS

TIME & REGION

⇒ Select **Status > Time & Region**.

KX-HDV800You are logged in as ADMIN
[Logout](#)

StatusPhone bookCall listSettings

DeviceNetwork**Time & Region**SIPMediaLog

Time

Enable NTP☒ On ☐ Off


Time11:02:37Date2010-06-09

TimezoneUTC+01:00Daylight saving☒ Yes ☐ No

NTP Serverpool.ntp.org

Region

CountrySweden (SWE)

On phone:  (MENU) > **STATUS > TIME** (8,5).

SIP

⇒ Select **Status > SIP**.

KX-HDV800

StatusPhone bookCall listSettings

DeviceNetworkTime & Region**SIP**MediaLogLicenses

Account 1

StatusREGISTERED

Account name169Realm*

User169Authentication name169

Registrar192.168.0.101Password*****

ProxyRegistration interval1800

Enable keep-alive☒ Yes ☐ No

Account 2

StatusDISABLED

Account nameRealm*

UserAuthentication name

RegistrarPassword

ProxyRegistration interval1800

Enable keep-alive☒ Yes ☐ No

NAT Traversal

STUN☐ On ☒ OffSTUN host

Offer ICE☐ Yes ☒ No

TURN☐ On ☒ OffTURN user

TURN hostPassword

Advanced

CHECKING STATUS AND LOGS

Account 1 and Account 2

On phone: ⚙️ (MENU) > STATUS > ACCOUNTS (8,1,1 and 8,1,2).

NAT traversal

On phone: ⚙️ (MENU) > STATUS > NAT TRAVERSAL (8,3).

Transport

On phone: ⚙️ (MENU) > STATUS > ACCOUNTS > TRANSPORT (8,1,3).

MEDIA

⇒ Select **Status > Media**.

KX-HDV800

You are logged in as ADMIN
[Logout](#)

StatusPhone bookCall listSettings

DeviceNetworkTime & RegionSIPMediaLog

Codec

	Priority
G722	4
G711 Alaw	3
G711 Ulaw	4
G729	1

Security

S RTP

☒ Disabled☐ Optional☐ Mandatory

Secure signalling

☐ No☒ TLS☐ SIPS

DTMF

DTMF Signalling

☒ RFC 2833☐ SIP Info☐ Inband

On phone: ⚙️ (MENU) > STATUS > MEDIA (8,4).

CHECKING STATUS AND LOGS

LOG

⇒ Select **Status > Log**.

The screenshot shows the KX-HDV800 web interface. At the top, it says "KX-HDV800" and "You are logged in as ADMIN Logout". Below this is a navigation bar with tabs: Status, Phone book, Call list, Settings, Device, Network, Time & Region, SIP, Media, and Log. The Log tab is selected. Below the navigation bar, there is a section for "Application log". It includes a dropdown menu for "Application", a "Change" button, and a "Refresh" button. Below this, there is a "Log level" section with a dropdown menu set to "Info", a "Set" button, and a "Clear Log" button. The main area displays a list of log messages, including SIP manager settings, registration success messages, and account registration messages.

```
Jun 9 07:03:18: INF: sip_manager: ua_cfg.nameserver[1] = 10.10.1.18
Jun 9 07:03:18: INF: sip_manager: ua_cfg.outbound_proxy_cnt = 0
Jun 9 07:03:18: INF: pjsua version 1.0-trunk for arm-926-linux-gnu initialized
Jun 9 07:03:19: INF: Registration sent
Jun 9 07:03:19: INF: sip_manager: Setting codec G722, prio 4
Jun 9 07:03:19: INF: sip_manager: Setting codec PCMA, prio 3
Jun 9 07:03:19: INF: sip_manager: Setting codec PCMU, prio 2
Jun 9 07:03:19: INF: sip_manager: Setting codec G729, prio 1
Jun 9 07:03:19: INF: <sip:300@10.10.1.32;transport=udp>: registration success, status=200 (OK),
will re-register in 300 seconds
Jun 9 07:03:21: INF: mmi: Account '300' registered
Jun 9 07:08:14: INF: <sip:300@10.10.1.32;transport=udp>: registration success, status=200 (OK),
will re-register in 300 seconds
Jun 9 07:08:14: INF: mmi: Account '300' registered
Jun 9 07:13:09: INF: <sip:300@10.10.1.32;transport=udp>: registration success, status=200 (OK),
will re-register in 300 seconds
Jun 9 07:13:09: INF: mmi: Account '300' registered
Jun 9 07:18:04: INF: <sip:300@10.10.1.32;transport=udp>: registration success, status=200 (OK),
will re-register in 300 seconds
Jun 9 07:18:04: INF: mmi: Account '300' registered
Jun 9 07:22:59: INF: <sip:300@10.10.1.32;transport=udp>: registration success, status=200 (OK),
```

The Log tab contains five types of log messages and can be useful for trouble shooting.

⇒ Select the log you want to review and click on the **Change** button.

① The **Refresh** button adds all new messages sent since the present log was chosen.

Application log

This shows the phone application messages. The log can be filtered from “Fatal” (only the fatal error messages) to “Trace” (all messages).

The **Clear log** button erases all content in the log.

SIP Trace

The SIP Trace logs the communication between the phone and the SIP PBX.

The **Clear log** button erases all content in the log.

It is possible to disable the SIP trace log

⇒ Select SIP logging **Off** and click on the **Set** button.

CHECKING STATUS AND LOGS

System log

Shows the phone system messages.

Device management log

Logs the device management activities.

Upgrade log

Logs the upgrade procedure.

SPECIFICATIONS

Dimensions

(Width x Depth x Height)	275 mm x 240 mm x 77 mm
Weight	1 kg
Colour	Liquorice black
Display screen	Illuminated graphics (LCD), 128 x 64 px
Keypad	Alphanumerical 0–9, *, on, off, mute, hold, volume up, volume down, 5 buttons for menu navigation, line mode, conference guide
Anti-theft protection	Kensington security slot
Memory	Support for SD and SDHC memory cards (Recording capacity 35 h/GB)
PoE/AC Adapter	3.2 W (Standby) 5.5 W (Talking)

Bluetooth® Specification

Frequency Band	2.402 GHz to 2.480 GHz
Maximum Power Output	0.01 W

Connectivity

Network connection	Modular 8P8C (RJ45), Ethernet 10/100 Base T
USB connection	USB 2.0 Mini B.
Bluetooth	Bluetooth v4. Support for Bluetooth Low Energy Profiles, GAP and GATT, Class 1.
NFC	Support for simplified Bluetooth pairing and connection using NFC (near-field communications). NFC Forum Type 4 and ISO/IEC 14443 Type A support.
Power supply	IEEE 802.3af Power over Ethernet, Class III. Optional: AC adapter 100 V–240 V AC/12 V DC
Extra microphones	2 modular 4P4C (RJ11)
Auxiliary	Modular 4P4C (RJ11) for wireless headset

Network and communication

IP stack	IPv4
Network addressing	DHCP and static IP
NAT traversal	STUN, ICE and TURN
Connection protocol	SIP 2.0 (RFC 3261 and companion RFCs)
Transport	UDP, TCP, TLS and SIPS

SPECIFICATIONS

Security	SRTP and TLS (TLS v1.0, TLS v1.1, TLS v1.2)
Quality of Service	DiffServ, VLAN
Audio support	Codecs: G722, G711 A-law, G711 μ -law, G729ab
DTMF tone generation	RFC2833, SIP INFO, In-band
Time servers	NTP and SNTP
Daylight saving	Configurable for automatic adjustments.
Configuration	Via integrated web server

Configuration and provisioning

Configuration	Via integrated web server, HTTP or HTTPS Separate user and administrator login for secure configuration.
Device management	Support for device management for easy configuration and updating of multiple conference phones.

Directory

Internal phone book	1,000 entries per profile (4 password protected profiles) Export/import of directory Call list
External directory	Support for LDAP

Sound

Microphone	Omnidirectional, 360°
Reception area	Up to 30 m ² , >10 people
Speaker	Frequency band 200 Hz–7000 Hz
Volume	90 dB SPL 0.5 m
Equalizer	Three pitches: soft, neutral, bright

Environment

Temperature:	0 °C–40 °C
Relative humidity:	20 %–80 % condensation free
Recommended acoustic conditions:	Reverberation period: 0.5 S Rt 60 Background noise: 45 dBA

Panasonic Corporation

1006, Oaza Kadoma, Kadoma-shi, Osaka 571-8501, Japan

These materials have been reproduced by Panasonic with the permission of Konftel Inc. COPYRIGHT © Konftel Aktiebolag. ALL RIGHTS RESERVED.

PNQX8911ZA PP0619MK0