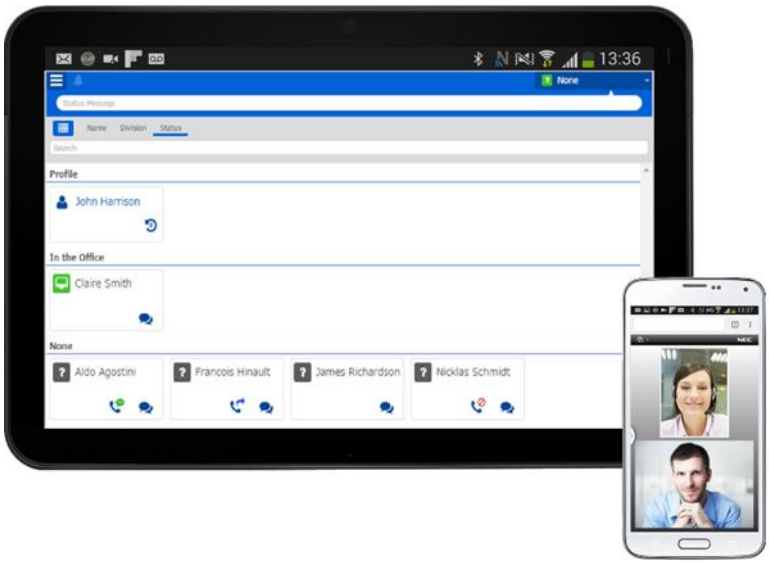
SV9100 InUC Installation Guide



Please read this manual carefully before operating this product and save this manual for future use.

What is InUC?

The InUC Web Client is a browser based client hosted on the SV9100 CPU that provides a Buddy List, BLF status, Call Control, Call History, Function Key Status and Access, Presence Status, group or individual Email Messaging, group and individual Instant Messaging, Service Access for Call Forward and Do Not Disturb, Speed Dial List, Status Messages, and Video Conferencing. Each of these features is described in more detail below.

Buddy List

Each user can define a list of buddies that will show up on their Home page. Each buddy entry shows the following information:

• Online or Offline
• BLF Status – Shows Busy, Call Forward, and DND icons
• IM Icon – Initiate an IM to a buddy
• Presence Status – Shows if buddy's presence status is set for In the Office, On Vacation, Business Travel, In a Meeting, Out to Lunch, Sick, Gone for the Day, Out of the Office, or Unavailable. Up to 5 custom presence states can be defined. PRG 20-70 is used to assign an icon, colour, and name to the custom presence state.
• Status Message – Shows the buddy's Status Message if one is set.

Buddy lists are initially sorted by name. Buddy Lists can also be sorted by a Division/Department defined in system programming or sorted by Presence Status.

Call Control

The InUC Web Client can control a user's physical terminal giving them the ability to make and receive internal and outside calls. InUC Web Client can perform the following Call Control functions:

• Call
• Answer
• Hold
• UnHold
• Transfer
• Conference

Web Browser Softphone

The InUC Web Client can register as a web browser softphone giving users the ability to make and receive internal and outside calls with the feature set of a standard SIP terminal. InUC Web Client can perform the following softphone functions:

• Call
• Answer
• Hold
• Resume or UnHold
• Transfer
• Video Calling between InUC Softphone users

Call History

When the InUC Web Client is run in desktop phone mode, the client will show the call history of the controlled desktop phone. Users can make a call to a number in the Call History list.

Function Key Status

When the InUC Web Client is run in desktop phone mode, the client can show the status of function keys that are programmed on the controlled desktop phone. Some functions can be accessed from the programmed function keys.

Email Messaging

Users can initiate an Email to one or more InUC Web Client users. If the InUC Web Client user has an Email address defined in Program 20-57, other InUC Web Client users can select them from a list within InUC Web Client. This will open the new Email form in their default mail client with the selected users Email address already populated in the To: field.

Instant Messaging

Users can send an instant message to one or more InUC Web Client users. Instant messages can be sent from the buddy list or in a multicast message. Instant Messages show date and time stamp. When a user logs out of the InUC Web Client, the messages are not automatically saved, but a user can manually save them to a text file.

Service Access

Under the Service Access feature, the InUC Web Client can Set and Cancel Call Forwarding (immediate, both, busy, busy/no answer, and no answer) and Do not Disturb. Service Access also provides a link to open Web Programming.

Speed Dial

The InUC Web Client lists the Speed Dial names and numbers defined in Program 13-04 in system programming. Users can make calls to the numbers in the Speed Dial list when logged in with Call Control mode. The Speed Dial list can be sorted alphabetically or by the Speed Dial index.

Video Conferencing

The InUC Client Web Conference gives you the ability to have a video conference with a maximum of seven other users. The SV9100 supports a total of four Web Conferences with a maximum of eight parties each.

ST500 Mode (SV9100 CP20 Only)

ST500 mode is an added mode that allows for an ST500 client user on an Android or iOS device to access the above features of InUC.

Contents

System Requirements

SV9100 CP10 (v9.00)

Ethernet connection to either CCPU or VoIPDB (GPZ-IPLE is required for Web Browser Phone Mode)

SV9100 CP20 (v10.00)

Ethernet connection to either CCPU or VoIPDB (GPZ-IPLE is required for Web Browser Phone Mode and ST500 Mode)

Hardware, Operating System and Browser Support

Windows PC

Recommended Minimum Specification
- Intel Core i5 running at 2.7 GHz or greater
- 4GB RAM of more

Supported OS
- Windows 7/8.1/10 32bit or 64bit

Web Browser
- Google Chrome v69 or later
- Microsoft Internet Explorer 11

MAC

Recommended Minimum Specification
- Intel Core i5 running at 2.7 GHz or greater
- 4GB RAM of more

Supported OS
- MAC OS X v10.10 or later

Web Browser
- Google Chrome v69 or later

Android Smartphone/Tablet

Supported OS
- Android v4.4.2 or later

Web Browser
- Google Chrome v69 or later

iOS Smartphone/Tablet

Supported OS
- iOS v11.4 or later

Web Browser
- Safari v11.0 or later

		Windows		Android	iOS
		Chrome	IE11	Chrome	Safari
InUC Client	InUC User Client	Yes	Yes	Yes	-
	Web Video Conference	Yes	Yes[1]	Yes	-
	Screensharing	Yes[2]	-	-	-
	View Screensharing	Yes	Yes	Yes	-
	InUC Call Control	Yes	Yes	Yes	-
	InUC Browser Phone	Yes[3]	-	-	-
	InUC ST500 Mode			Yes	Yes

[1] Temasys WebRTC Plugin Required

[2] NEC Screen Sharing Plugin required

[3] Browser Phone mode only works on Windows and Google Chrome v59 or higher.

Note: Feature set is dependent on device and operating system.

Terminal Support

InUC Desktop Phone mode is supported with the DT300/DT400/DT500/DT700/DT800/DT900 terminals.

ST500 Mode is available using ST500 for Android v3.1 or later and ST500 for iOS v11.4 or later with the SV9100 CP20 CPU.

Desktop Phone Mode call control feature support is outlined in the below table.

Function		MLT	SLT
Call Function	**Display Call Status**	Yes	Yes
	Call	Yes	Yes
	Answer	Yes	-
	Hold	Yes	-
	Resume	Yes	-
	Transfer	Yes	-
	Add to group call	Yes	-
	End a call	Yes	-
Call History		Yes	-
Function Key		Yes	-

SV9100 Licenses

Order Code	License Name	License Description	Maximum Values
BE116985	SV9100 InUC Web Client License (0081)	Required for a user to access the InUC Web Client feature	Max 255
BE117606	SV9100 InUC Web 1st Party CTI License (0082)	Required for Desktop Phone Mode	Max 128
BE118383	SV9100 InUC Web Browser Phone License (0084)	Required for Browser Phone Mode	Max 255
BE115845	SV9100 Web Video Conference License (0080)	Required for Video Conferencing (4 free with SV9100)	Max 32
BE114068	SV9100 Encryption License (0030)	Required for Browser Phone Mode	Max 1 (System License)
BE118381	SV9100 R9 Feature License	Required for Browser Phone Mode	Max 1 (System License)
BE119589	SV9100 CP20 R10 Feature License	Required for ST500 Mode	Max 1 (System License)
BE114042	SV9100 System Port Capacity License	Required when number of ports on the system exceeds 64. 1 license per extra port is required. Prophix will automatically add this license when InUC Browser phones are configured past 64 ports.	1 per port over 64.

NOTE: Browser Phone mode is not available in a Netlink environment.

Network Considerations

NEC recommends that you have prior knowledge on the following:

- Domain Name System (DNS)
- Network Address Translation (NAT)
- Traversal Using Relays around NAT (TURN)
- Session Traversal Utilities for NAT (STUN)

SV9100 Site Recommendations

- A static Public IP address required on the WAN interface.
- Use split DNS with an internal DNS record for SV9100 FQDN resolvable to the SV9100 IPL IP address (PRG10-12-09). And use an external DNS record for SV9100 FQDN resolvable to the static Public IP Address.
- A NAT router is required in a typical deployment. Most business grade SOHO routers and above include this function.
- TCP port 443 by default or custom port number configured in PRG10-20-08 UC Web Application, opened on Firewall from the public internet and forwarded to the SV9100 IPL IP Address (PRG10-12-09).
- The use of a Public STUN/TURN server or a locally deployed STUN/TURN Server for the use of WebRTC remotely is required. In this document reference is given to using a Public TURN Server offering.
- TLS configuration is recommended when utilising InUC off net.
- You will need administrative access to the WAN router/firewall device. NEC will not provide support in configuration of this device.
- A NAT router is required in a typical deployment. Most business grade SOHO routers and above include this function.
- If utilising a locally deployed STUN/TURN server, TCP and UDP Port 3478 (STUN/TURN requests) by default, or custom port depending on service used, must be opened on the Firewall.
- If utilising a Public STUN/TURN server no ports are required to be opened on the firewall for this.
- If the WAN router/firewall has a built in SIP proxy of SIP Application Layer Gateway (ALG). These should be disabled.
- If Browser phone is being used publically, registration port set for the Browser Phone must be opened on the firewall.

WAN Router/Firewall

Default ports that should be opened are described in the table below. Custom port numbers used, will need to be adjusted and opened accordingly within the WAN router/firewall device.

Application	Port Number(s)	Transport Protocol	WAN Router/Firewall Location
HTTPs	443 (default)	TCP	SV9100 Side InUC
STUN/TURN*	3478	UDP	Client Side

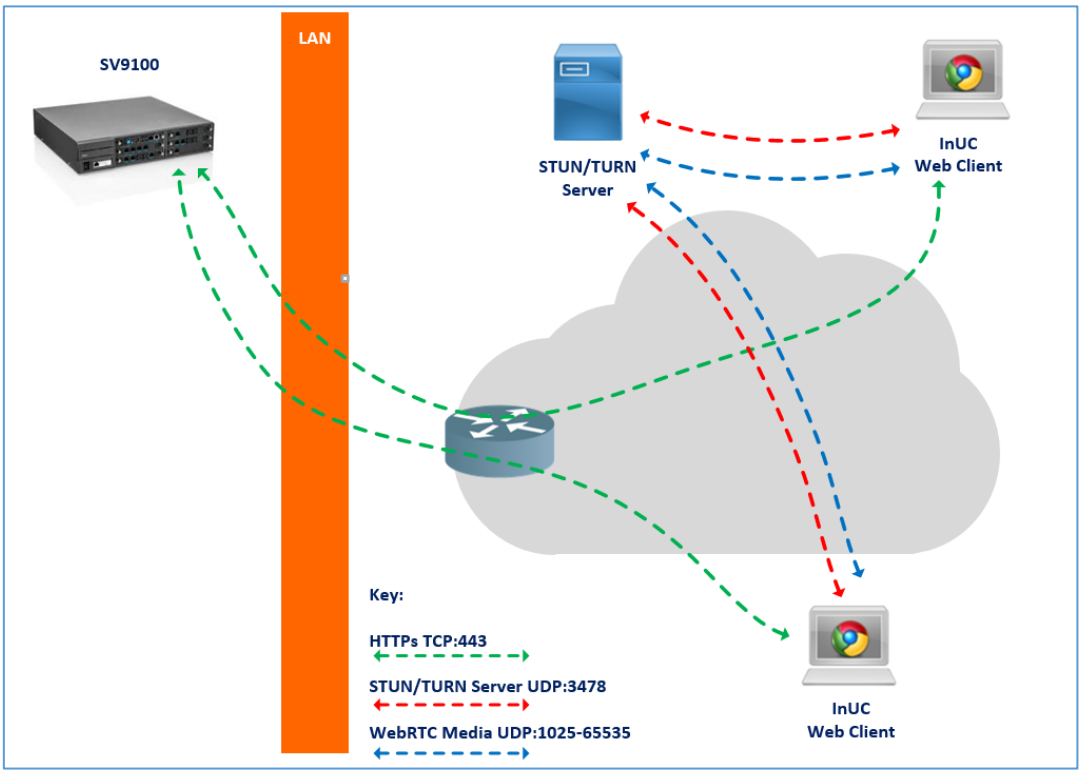
* If utilising a loally deployed STUN/TURN server.

STUN Server

WebRTC video conferencing is designed to work peer-to-peer, so users can connect by the most direct route possible. However, WebRTC is built to cope with real-world networking: client applications need to traverse NAT gateways and firewalls, and peer to peer networking needs fallbacks in case a direct connection fails. As part of this process, WebRTC uses STUN servers to get the IP address of your computer, and TURN servers to function as relay servers in case peer-to-peer communication fails.

TURN Server

TURN stands for Traversal Using Relays around NAT. It is a standard method of NAT traversal used in **WebRTC**. It is defined in IETF RFC 5766. **TURN** is used to relay media via a **TURN server** when the use of STUN isn't possible.



Using DNS for InUC access

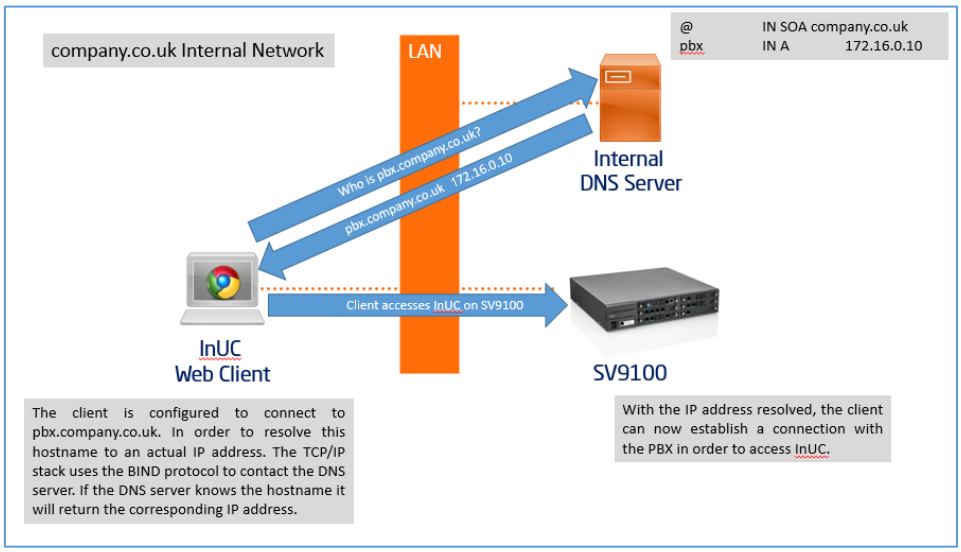
Split DNS is a useful installation method that allows for a single hostname (e.g. sv9100.nec.co.uk) to be used and resolved to a private IP address when on the internal LAN network and to a different public WAN IP address when located externally for getting the most consistent experience when using InUC internally and externally.

Many client applications commonly use a hostname or FQDN (Fully Qualified Domain Name) to connect to an application server (i.e. the SV9100). For the SV9100 this could be used in various ways but some examples could include IP phones connecting to the PBX or user access to on-board applications such as InUC.

The means of accommodating this varies depending on an organization's DNS infrastructure but a typical example is illustrated below.

Internal DNS

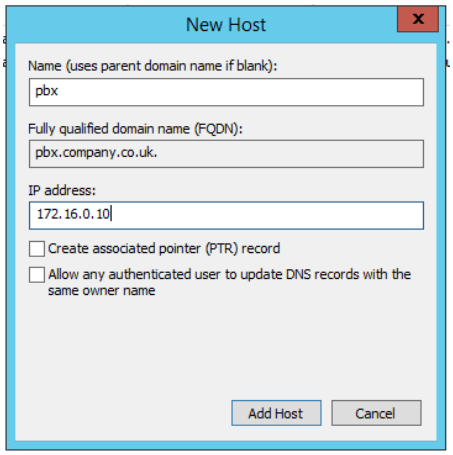
The resolution of the DNS address pbx.company.co.uk to the IP address 172.16.0.10 and the subsequent connection between the InUC client and the PBX will be accomplished as follows.



Create an Internal DNS host record

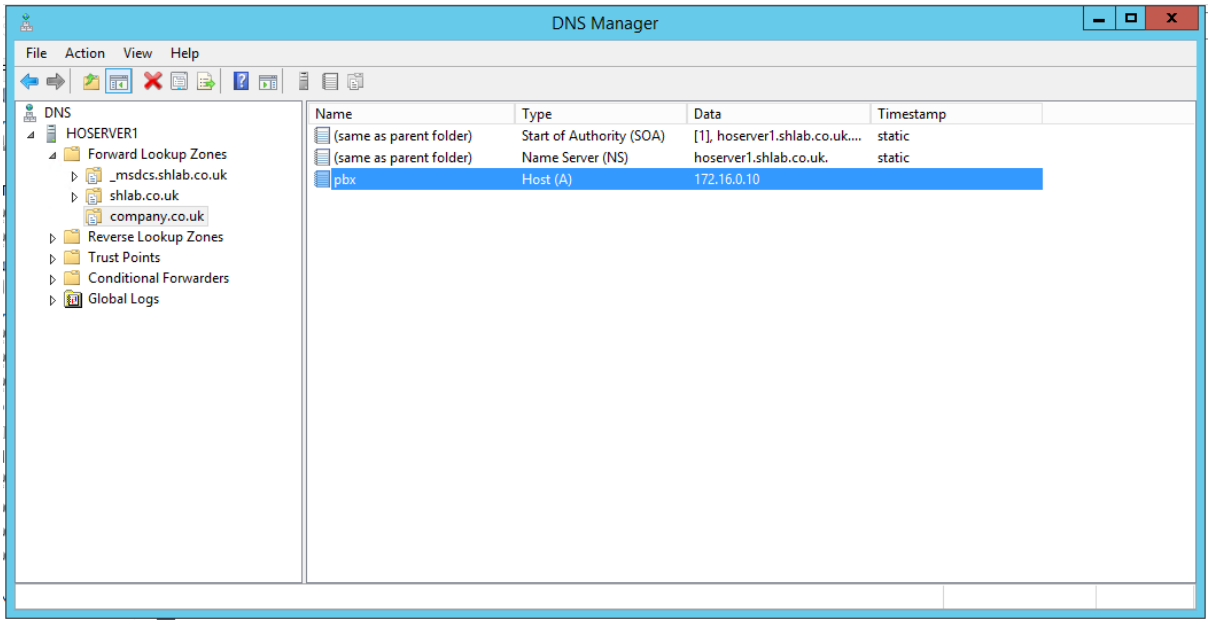
From the Server Manager application:

1. Right click on the zone for your hosts domain (for example company.co.uk) and select **"New Host (A or AAAA)…"**



2. Enter the hosts Name (for example pbx)
3. In the IP Address field enter the local IP address of the SV9100.

4. Click **"Add Host"**. A dialog will appear confirming that the record was added and you should now see a new entry as below under the domain lookup zone.



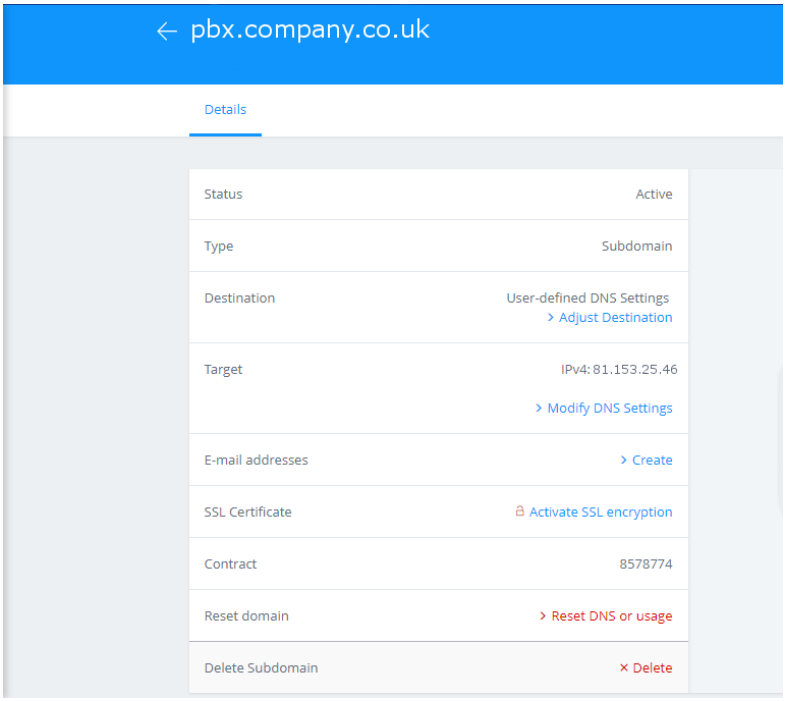
Test your DNS Entry

To make sure that your DNS Server resolves your FQDN to the correct IP Address do the following:

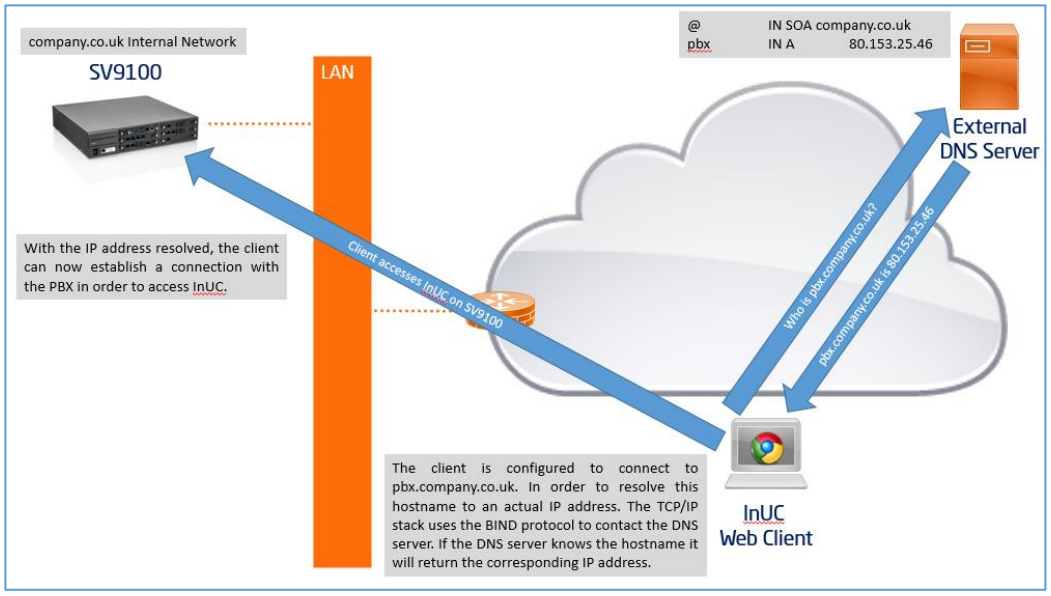
1. Open a command prompt window on a computer in your organisations network.
2. Type in nslookup followed by your domain name – Example nslookup pbx.company.co.uk
3. You should get as a result the IP Address of the host – in this example: 172.16.0.10

External DNS

When access is required from a remote location, the connection can no longer be established directly to the PBX's internal IP address. Instead, the DNS address pbx.company.co.uk should now resolve to the Public IP address of the WAN router/firewall connected to the PBX LAN network. This requires that the external Domain Name Server resolves pbx.company.co.uk to the relevant Public IP address.



Since the InUC client and PBX are no longer on the same network the connection is established through the WAN Router/Firewall, which must be configured to allow access for the client to connect using HTTPs with the PBX.



License Requirements

BE116985 SV9100 InUC Web Client License – required for a user to access the InUC Web Client feature
BE117606 SV9100 InUC Web 1st Party CTI License – required for Desktop Phone Mode
BE115845 SV9100 Web Video Conference License – required for 5 – 32 channels, 4 are available on the CPU.
BE118383 SV9100 InUC Web Phone License – required for Browser Phone Mode
BE114068 SV9100 Encryption LIC (system license) - required for Browser Phone Mode
BE118381 SV9100 CP10 R9 Version Feature License
BE119589 SV9100 CP20 R10 Version Feature License
BE114042 SV9100 System Port Capacity License**

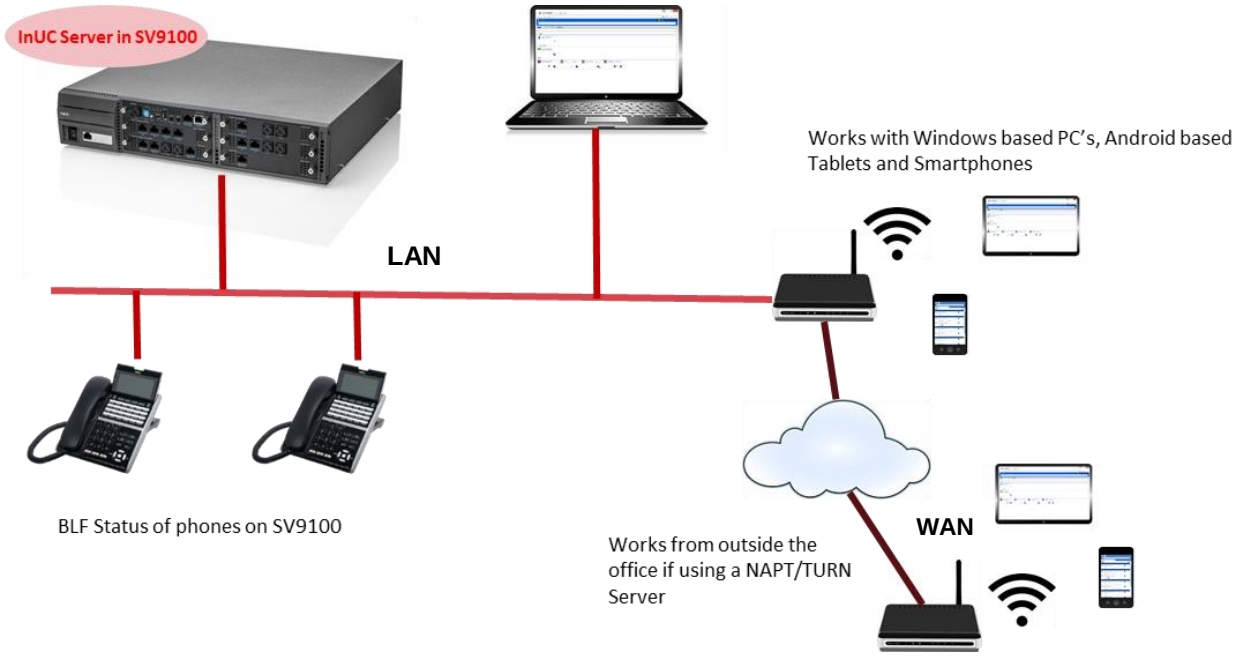
InUC User	**InUC User + Web Conference**	**InUC User + Desktop Phone Mode**	**InUC User + Browser Phone Mode**	**InUC User + ST500 Mode***
InUC Web Client License	InUC Web Client License Web Video Conference License	InUC Web Client License InUC Web 1st Party CTI License R7 Feature License	InUC Web Client License InUC Web Phone License Encryption License R9 Feature License System Port Capacity License**	InUC Web Client License SV9100 CP20 R10 Feature License

*ST500 Mode only supported with SV9100 CP20

** Required when number of ports on the system exceeds 64. 1 license per extra port is required. Prophix will automatically add this license when InUC Browser phones are configured past 64 ports.

Installation

Installation Environment



Connect to the SV9100 using PC Pro

This installation guide will cover the most frequently used configuration options. For advanced configuration please refer to the SV9100 Features and Specifications manual for further information.

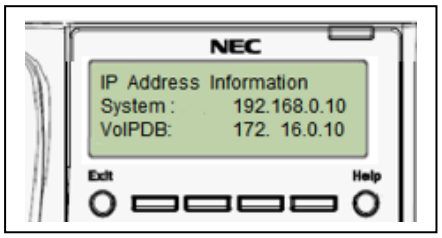
You must have SV9100 PCPro installed to your laptop/PC. This can be downloaded from BusinessNet.

The SV9100 can also be configured via an SV9100 system phone or via a Web Pro interface, these are not covered within this guide.

Connecting PCPro to the SV9100

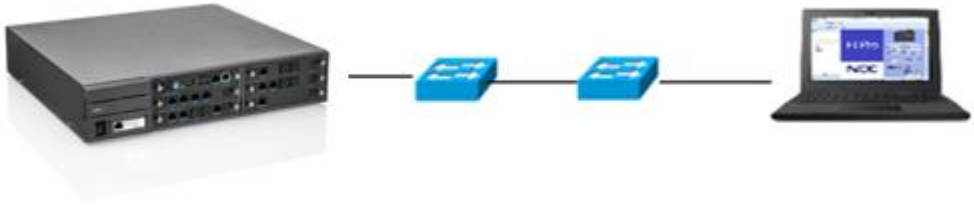
Connection default IP Address:
172.16.0.10 / 255.255.0.0

You can check the IP address at any SV9100 system phone:
Press the centre Navigation Key and dial 841



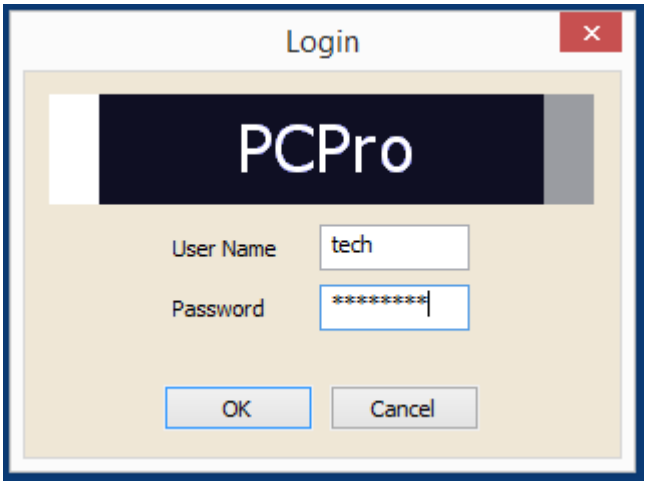
Direct to Ethernet connector on the SV9100 CPU card.

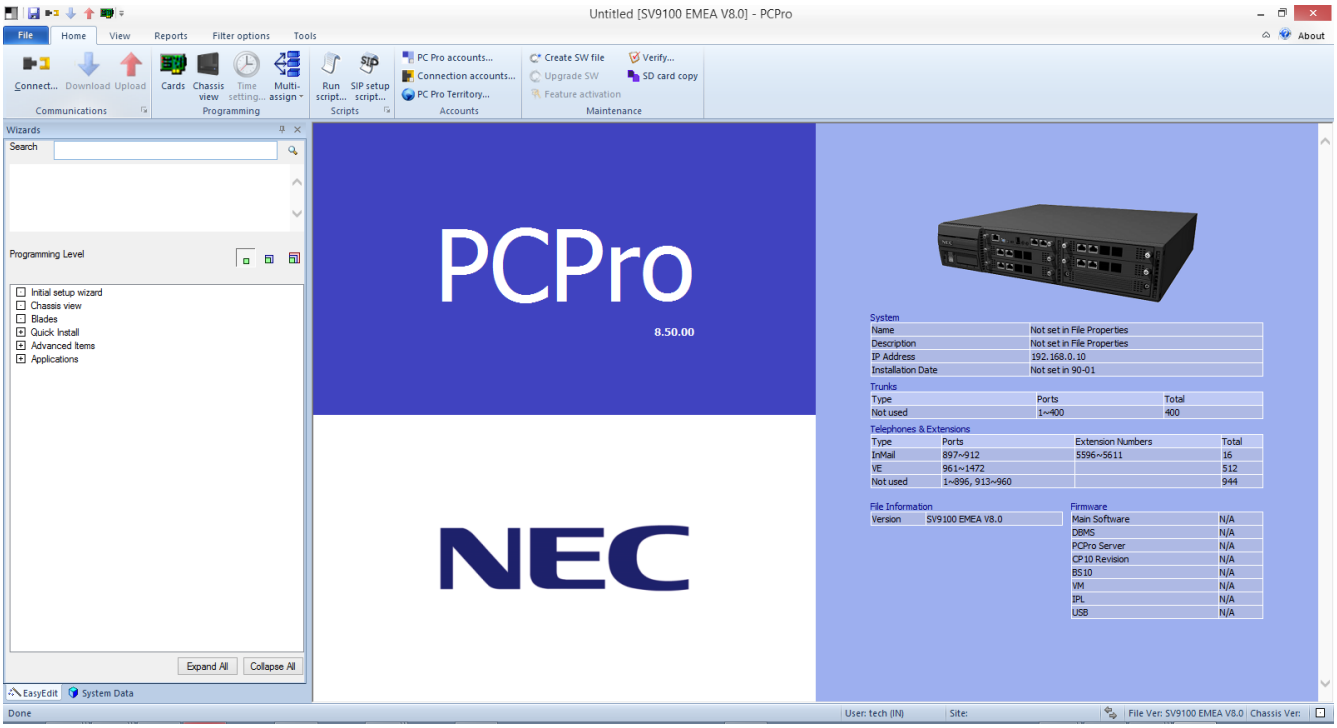
Via the customer's LAN.



SV9100 PCPro

Installer level access:
User Name: tech
Password: 12345678

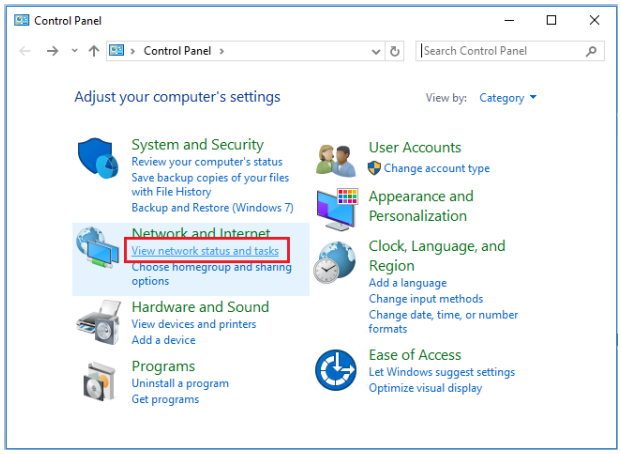




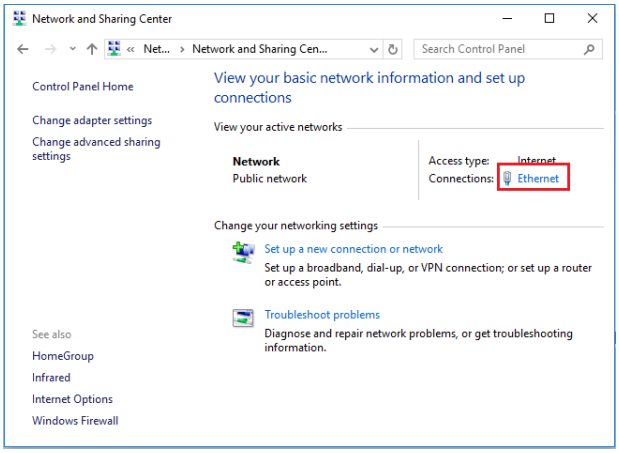
Change your PC IP Address

You may need to reconfigure your PC to have an IP address in the same subnet as the SV9100 during system configuration.

Your IP Address is adjusted in Windows Control Panel, select 'View network status and tasks'

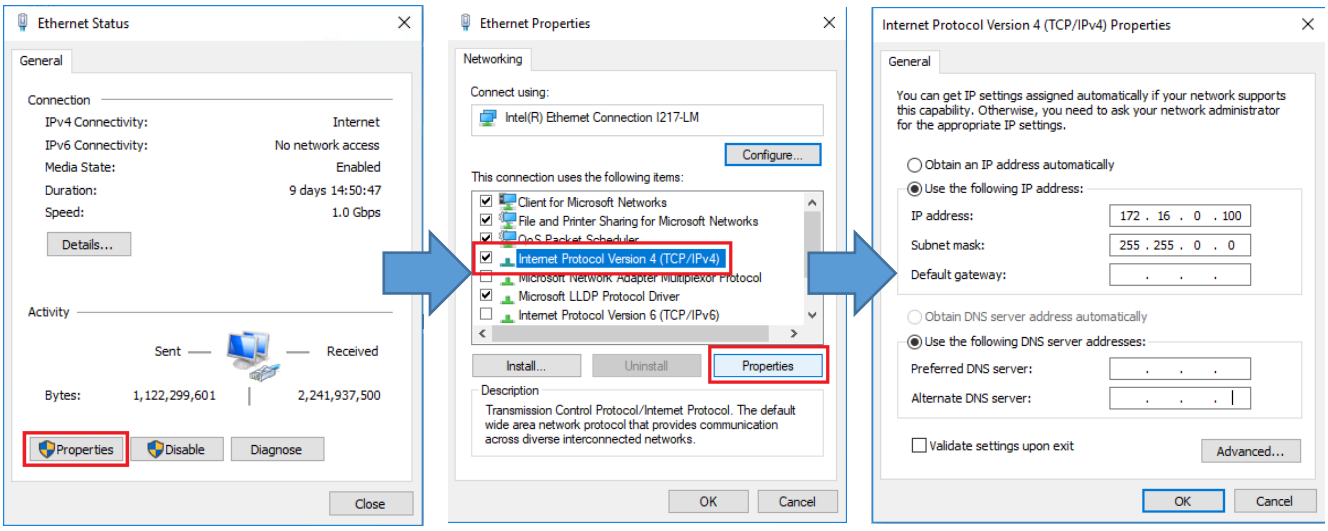


Edit the properties of your Ethernet adaptor



You will need to define an IP address in the same network as the SV9100. Recommended values are 172.16.0.100 / 255.255.0.0

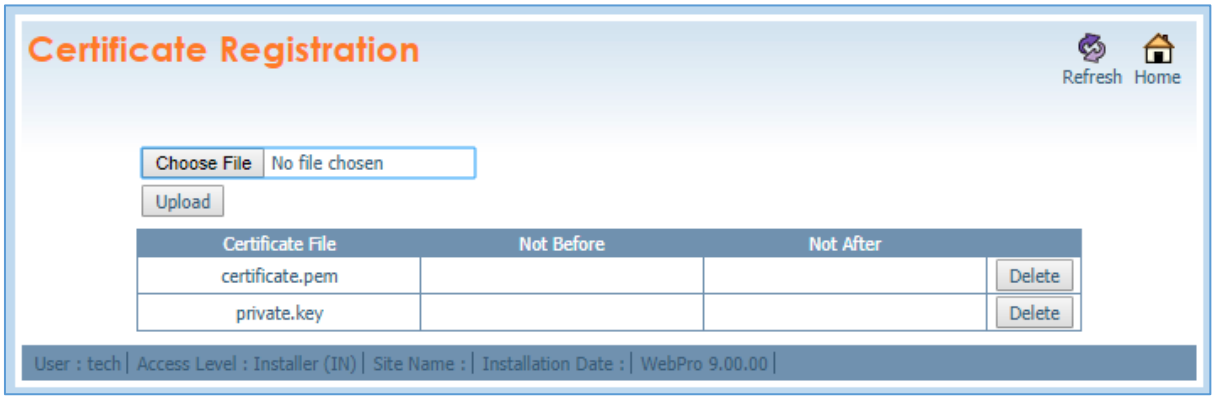
Gateway and DNS addresses are not necessary. Once commissioning of the SV9100 is completed you can return to this area and reconfigure your network adaptor to the previous values.



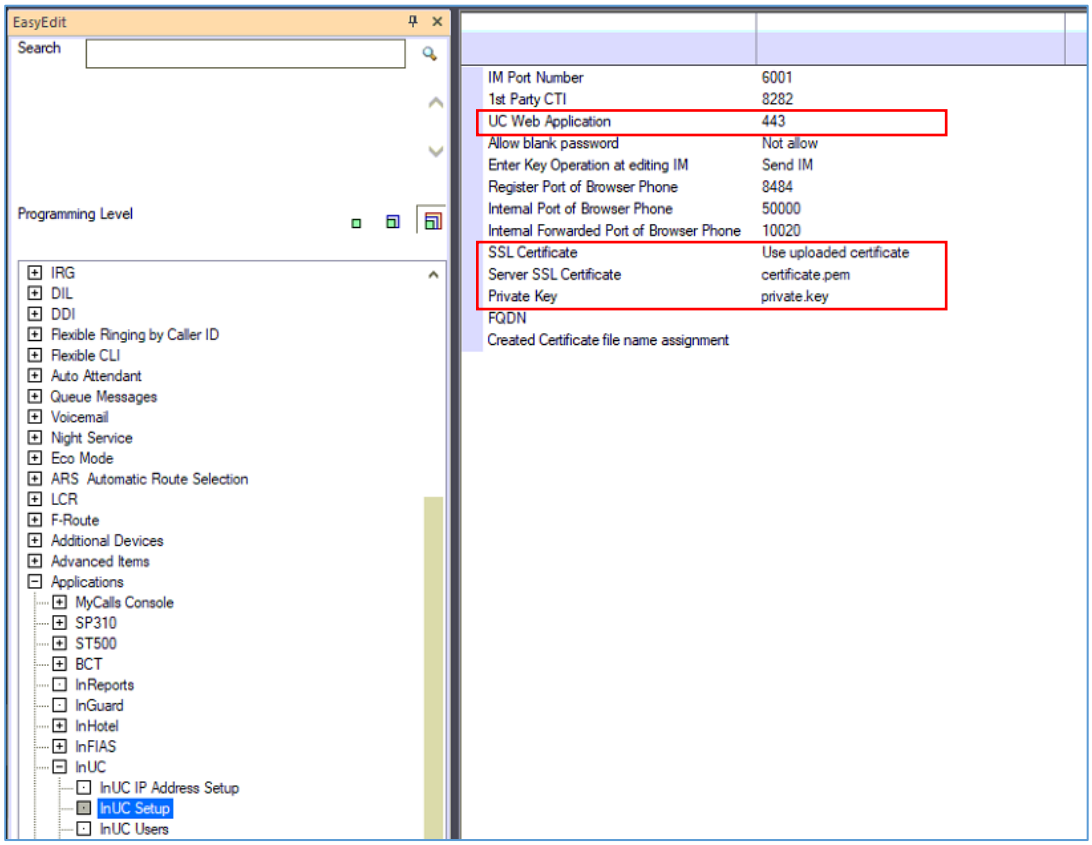
Configuring the SV9100 for TLS

Certificates are required when encrypting traffic in and out of the SV9100. In order to do so, certificates can be purchased from a Public Certificate Authority or Self Signed Privately in accordance with current certificate requirements.

Once the certificate and associated files are ready, the server certificate and private key file are uploaded into the system using WebPro:



Once uploaded to the system the server certificate and private key file are added into the system in programming, as well as setting the SV9100 to use the newly uploaded certificates. Finally, the connection port for InUC can be set, for example to port 443. A reboot is required after the upload and setting of the below configuration items.



Configure the SV9100 for using InUC

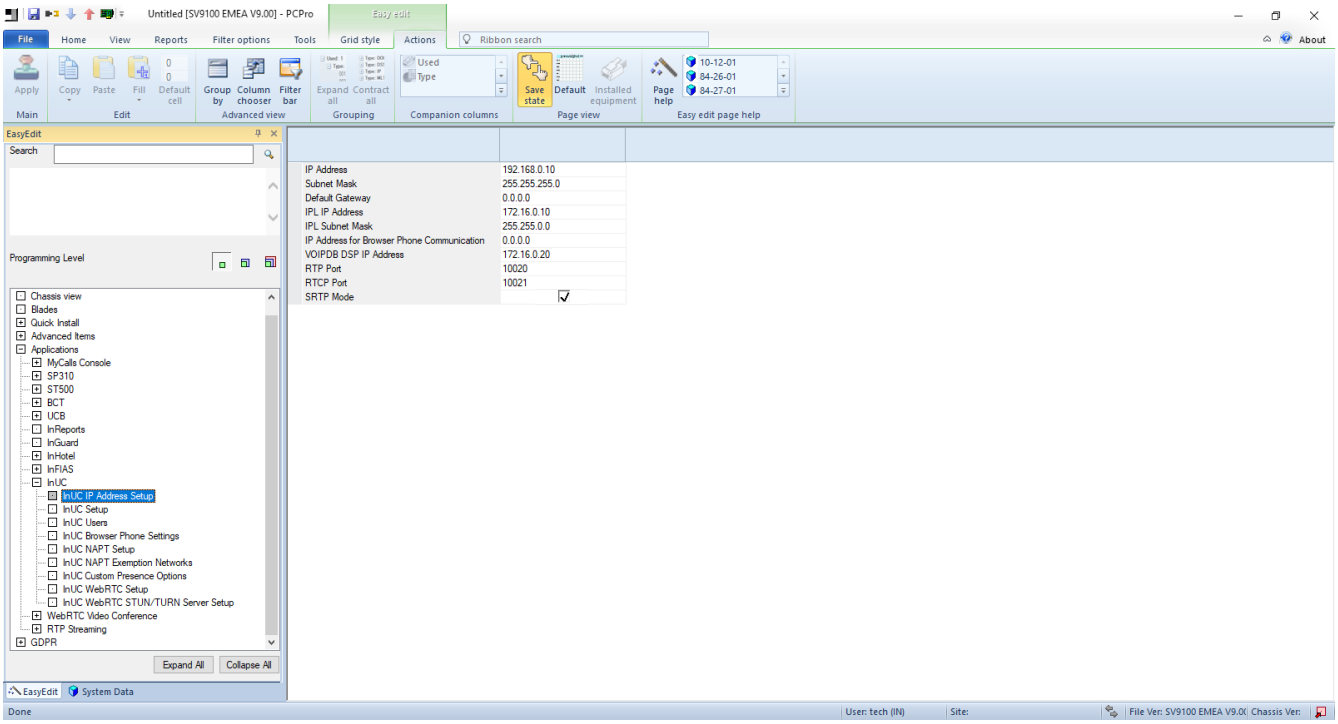
IP Configuration

From the **IP Configuration** screen you can check the IP configuration details of your SV9100 are correctly setup for use with the InUC application.

If you're connecting the SV9100 to a network using the CCPU Ethernet port then the **IP Address**, **Subnet Mask**, and **Default Gateway** fields are configured.

If you're connecting the SV9100 using the VoIPDB card Ethernet port then the **VoIP IP Address**, **VoIP Subnet Mask**, and **Default Gateway** fields are used.

- Easy Edit > Applications > InUC > InUC IP Address Setup



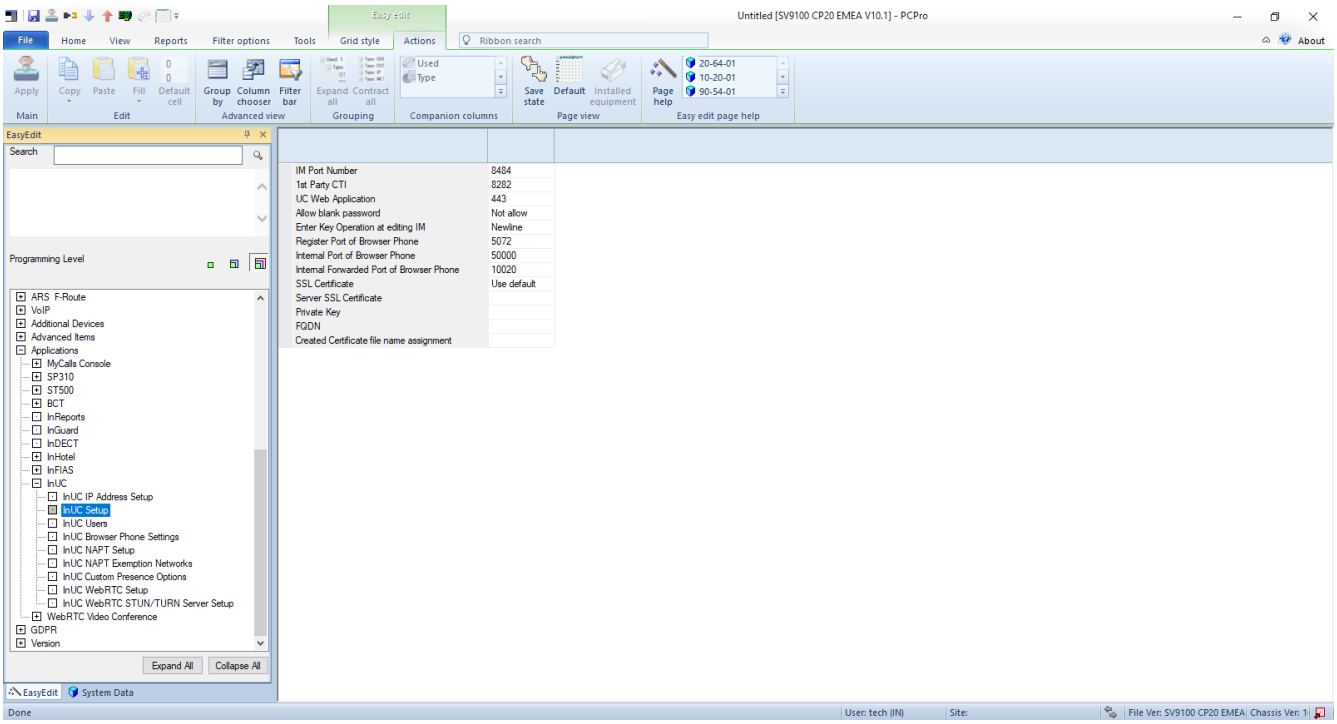
System Data Item	Item name	Input Data	Default Value
10-12-01	IP Address CCPU Ethernet interface IP address. Cannot be configured with an IP address in the same network subnet address range as the IPL interface.	0-9 (000.000.000.000)	192.168.0.10
10-12-02	Subnet Mask CCPU Ethernet interface Subnet Mask	0-9 (000.000.000.000)	255.255.255.0
10-12-03	Default Gateway Default Gateway can be used by CCPU or IPL interface. Which network subnet address range it is configured for determines which interface can use it.	0-9 (000.000.000.000)	0.0.0.0
10-12-09	IPL IP Address IPL Ethernet interface IP address. Cannot be configured with an IP address in the same network subnet address range as the IP interface in PRG10-12-01.	0-9 (000.000.000.000)	172.16.0.10

10-12-10	IPL Subnet Mask IPL Ethernet interface Subnet Mask	0-9 (000.000.000.000)	255.255.0.0
84-26-15	IP Address for Browser Phone Communication This is IP address is used for browser phone communication and should be configured in the same network address range as PRG10-12-09.	0-9 (000.000.000.000)	0.0.0.0
84-26-01	VoIPDB DSP IP Address VoIPDB Media Gateway interface IP address. Should be in the same network subnet address range as the IP interface in PRG10-12-09.	0-9 (000.000.000.000)	172.16.0.20
84-26-02	RTP Port Sets the first port used by the Media Gateway DSP channels for audio (RTP) communication.	0-65534	10020
84-26-03	RTCP Port Sets the first port used by the Media Gateway DSP channels for RTCP feedback of basic network conditions such as delay, jitter, and packet loss.	0-65534	10021
84-27-03	sRTP Mode Sets whether the VoIPDB can support sRTP for encryption of the RTP audio packets. If Browser phone is being used this MUST be enabled.	0:Disabled 1:Enabled	0:Disabled

InUC Setup

The **InUC Setup** screen is used for the configuration of common items used by the InUC application.

- Easy Edit > Applications > InUC > InUC Setup



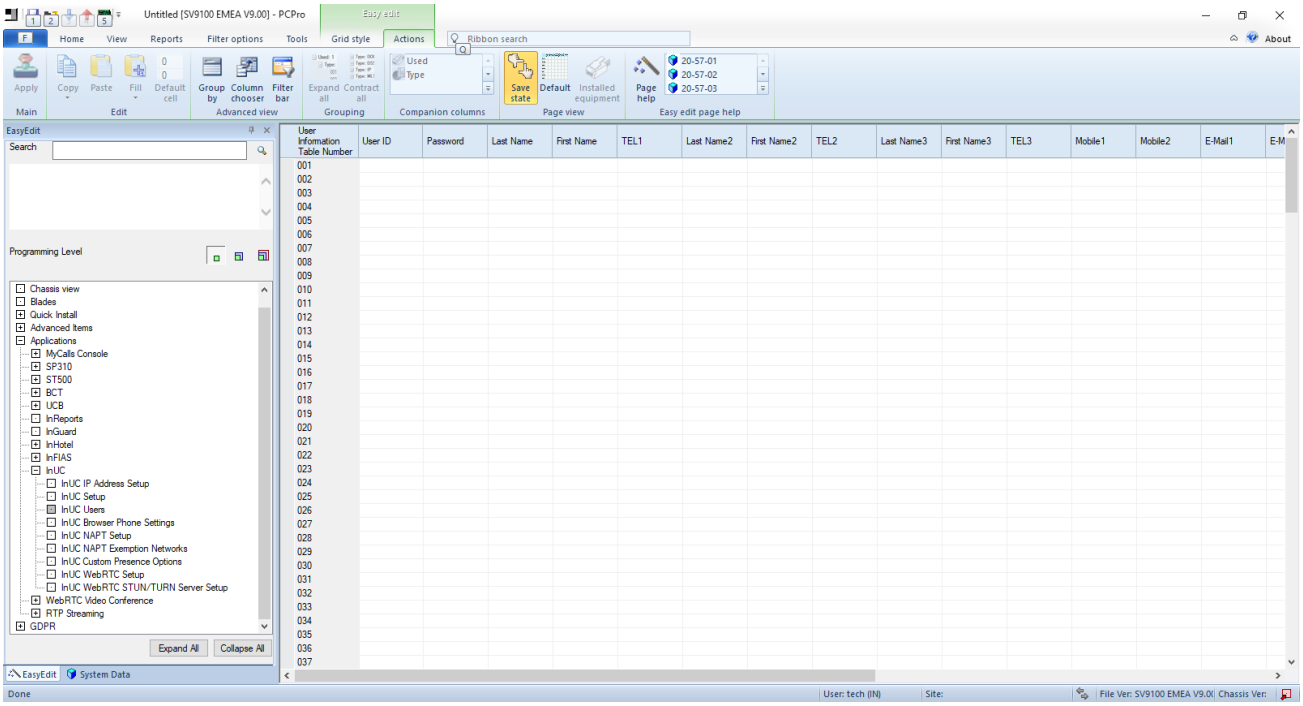
System Data Item	Item name	Input Data	Default Value	Recommended Value
20-64-03	IM Port Number Assign the port to use for the IM Port Number. This is the port number which is used when using an instant message (IM) communication by UC Web application.	0-65535	0	8484
10-20-01 Device ID 9	1st Party CTI Set to 8282. Used by CTI applications for 1st party control of an assigned extension number.	0-65535	0	8282
10-20-01 Device ID 8	UC Web Application Set to 443. Used by the PBX for incoming HTTPs connections. Only InUC is accessible from this port if configured. If assigned, PRG90-54-03 must be changed to another value (8443) and the PBX will need to also be restarted before it is usable.	0-65535	0	443
20-64-04	Allow Blank Password Set whether a blank password is allowed at the time of login of UC Web application and Video Conference.	0: Not Allow 1: Allow	0: Not Allow	
20-64-05	Enter Key Operation at Editing IM When it is set to 0: Newline, the Enter key moves the cursor to a newline, and Ctrl + Enter sends an IM message. When it is set to 1: Send IM, Enter key sends an IM message, and Ctrl + Enter moves the cursor to a newline.	0: Newline 1: Send IM	0: Newline	

20-64-06	Register Port of Browser Phone This is the register port used by the browser phone. If set to 0 the InUC web client cannot use browser phone mode.	0-65535	0	5072
20-64-07	Internal Port of Browser Phone This is an internal port used by the browser phone. If set to 0 the InUC web client cannot use browser phone mode but when not 0 it will reserve 512 ports from the port set here. For example if configured as 50000, 50000 – 50511 are reserved.	0-65535	0	50000
20-64-08	Internal Forwarded Port of Browser Phone This is an internal forwarded port used by the browser phone. If set to 0 the InUC web client cannot use browser phone mode but when not 0 it will reserve 460 ports from the port set here. For example if configured as 10020, 10020 – 10479 are reserved. This can be set to the same port number configured in PRG84-26-02.	0-65535	0	10020
90-54-04	SSL Certificate The server certificate used for HTTPS Web Programming and UC Web Application connections. When set to '0: Use default', the system uses its built-in default self-signed certificate. When set to '1: Use uploaded certificate', the system uses an uploaded certificate set in PRG 10-72-01/02.	0: Use default 1: Use uploaded certificate	0: Use default	
10-72-01	Server SSL Certificate Defines the Server Certificate name uploaded through WebPro for SSL connection usage when the SV9100 receives a SSL request.	Up to 32 characters	Blank	
10-72-02	Private Key Defines the Server Certificate Key name uploaded through WebPro for SSL connection usage when the SV9100 receives a SSL request.	Up to 32 characters	Blank	
10-72-03	FQDN Sets the Fully Qualified Domain Name that can be used for generating a self-signed certificate that can be used by the SV9100 for HTTPs connections.	Up to 128 characters	Blank	
10-72-04	Created certificate file name assignment Sets the file name of the generated self-signed certificate. This must end with the file extension .pem	Up to 64 characters	Blank	

InUC Users

The **InUC Users** screen is used for configuring the application user details. Up to 255 InUC users can be configured.

- Easy Edit > Applications > InUC > InUC Users



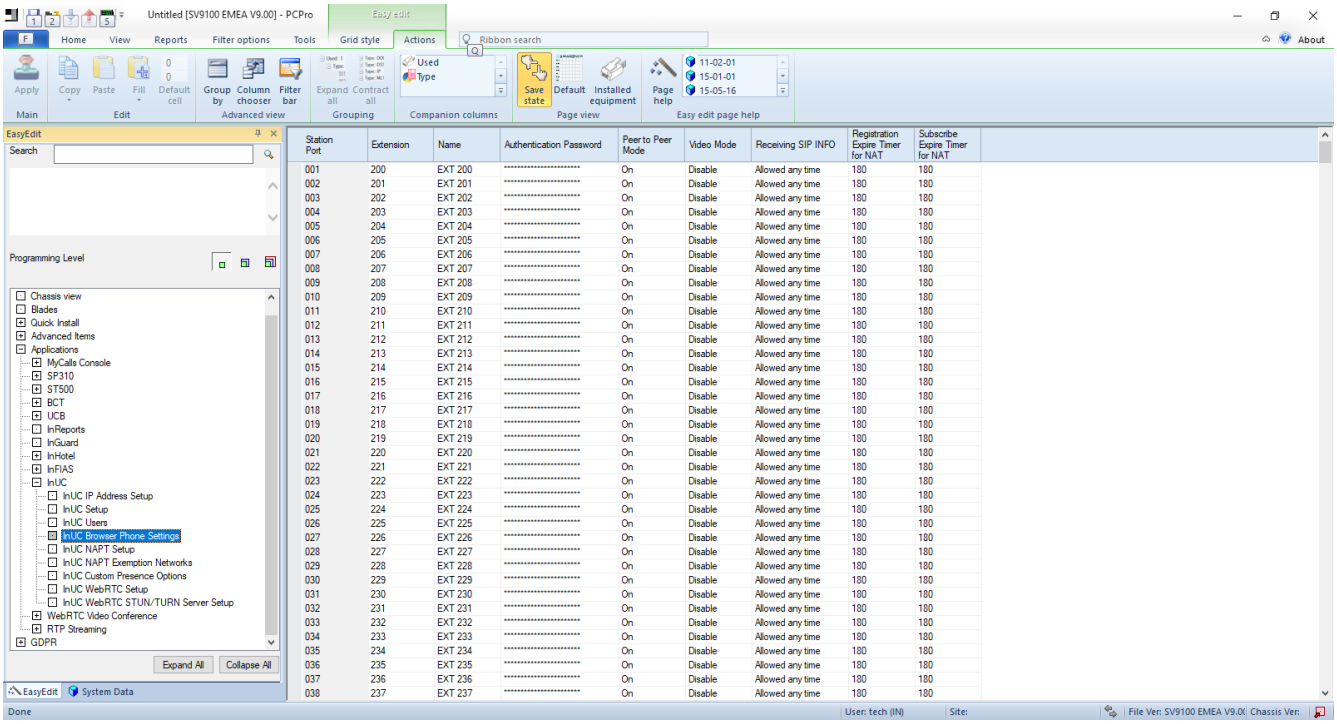
System Data Item	Item name	Input Data	Default Value
20-57-01	User ID User ID to logon with	Up to 16 characters.	Blank
20-57-02	Password Password required to logon with.	Up to 16 characters.	Blank
20-57-03	Last Name Last Name used for Display.	Up to 20 characters.	Blank
20-57-04	First Name First Name used for Display.	Up to 20 characters.	Blank
20-57-07	TEL1 Telephone number to display.	0-9,*,#,@,P,R	Blank
20-57-08	Last Name 2 Last Name used for Display.	Up to 20 characters.	Blank
20-57-09	First Name 2 First Name used for Display.	Up to 20 characters.	Blank
20-57-10	TEL2 Telephone number to display.	0-9,*,#,@,P,R	Blank
20-57-11	Last Name 3 Last Name used for Display.	Up to 20 characters.	Blank
20-57-12	First Name 3 First Name used for Display.	Up to 20 characters.	Blank
20-57-13	TEL3 Telephone number to display.	0-9,*,#,@,P,R	Blank
20-57-14	Mobile 1 Mobile telephone number to display.	0-9,*,#,@,P,R	Blank
20-57-15	Mobile 2 Mobile telephone number to display.	0-9,*,#,@,P,R	Blank

20-57-16	E-Mail 1 E-mail address to display and use.	Up to 128 characters.	Blank
20-57-17	E-Mail 2 E-mail address to display and use.	Up to 128 characters.	Blank
20-57-18	Company Company name to display	Up to 128 characters.	Blank
20-57-19	Department/Division Department/Division to display.	Up to 128 characters.	Blank
20-57-20	City City to display.	Up to 64 characters.	Blank
20-57-21	State/Prov State/Province to display.	Up to 32 characters.	Blank
20-57-22	Zip/Postal Zip/Postal area to display.	Up to 128 characters.	Blank
20-57-23	Country Country to display.	Up to 128 characters.	Blank
20-57-24	Profile Note Profile Note to display.	Up to 256 characters.	Blank
20-57-41	UC-Extension Number Extension number to use for desktop phone mode CTI control.	0-9 Up to 8 digits.	Blank
20-57-43	Extension Number of Browser Phone Extension number to use for browser softphone mode.	0-9 Up to 8 digits.	Blank
20-57-42	Language	0:English 1:German 2:French 3:Italian 4:Spanish 5:Dutch 6:Portuguese 7:Norwegian 8:Danish 9:Swedish 10:Turkish 11:Romanian 12:Polish 13:Russian 14:Simplified Chinese 15:Traditional Chinese 16:Thai 17:Vietnamese 18:Bahasa Indonesia 19:Language 20 20:Language 21 21:Language 22 22:Language 23 23:Language 24 24:Language 25 25:Language 26 26:Language 27 27:Language 28 28:Language 29 29:Language 30	English

InUC Browser Phone Settings

The **InUC Browser Phone Settings** screen is used for configuring the application user details that will be using the browser phone softphone integration.

- Easy Edit > Applications > InUC > InUC Browser Phone Settings



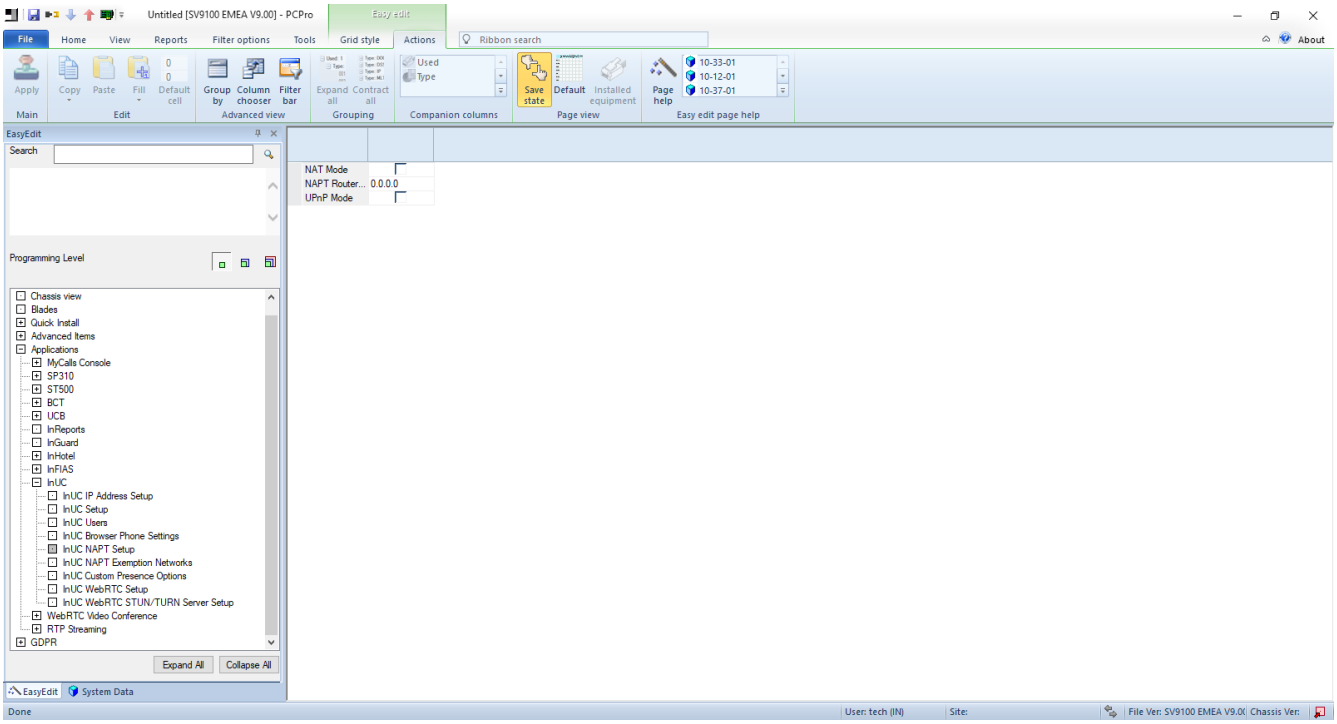
System Data Item	Item name	Input Data	Default Value
11-02-01	Extension Extension Number	8 digits (0-9)	-
15-01-01	Name Extension name	12 Characters	-
15-05-16	Authentication Password Enable authentication password used for securing access by IP devices to the SV9100. Enter a password here and enter in the IP device to ensure authentication is successful.	24 Characters	-
15-05-50	Peer to Peer Mode Enable sending of RTP directly between IP devices. When disabled RTP is handled between the devices and VoIPDB card using additional channel resources.	0:Disabled 1:Enabled	1:Enabled
15-05-43	Video Mode Enable video support for calling between peer to peer extensions.	0:Disabled 1:Enabled	0:Disabled
15-05-49	Receiving SIP INFO Select whether or not the system can receive SIP INFO DTMF message from a SIP IP terminal. There are two modes available for receiving the SIP INFO DTMF message. 'Allowed any time' can receive a SIP INFO message as a dialled digit information any time during signalling or conversation. 'Allowed while RTP is	0:Disabled 1: Allowed any time 2: Allowed while RTP is not available	1:Allowed any time

	not available' can only receive a SIP INFO message before an RTP connection is established during the signalling.		
15-05-47	Registration Expire Timer for NAT When the Expire timer value of the REGISTER message received from the IP MLT terminal is outside the useful range or there is no Expire timer value in the REGISTER message, the system sends this value to a terminal as an Expire timer value. It also acts as a monitoring time of whether the IP MLT terminal is connected. This setup is applied to a IP MLT terminal connected via NAT. However, when this value is 0, the value of PRG84-23-01 is applied even if the IP MLT is connected via NAT.	0-65535	180
15-05-48	Subscribe Expire Timer for NAT When the Expire timer value of the REGISTER message received from the IP MLT terminal is outside the useful range or there is no Expire timer value in the REGISTER message, the system sends this value to a terminal as an Expire timer value. It also acts as a monitoring time of whether the IP MLT terminal is connected. This setup is applied to a IP MLT terminal connected via NAT. However, when this value is 0, the value of PRG84-23-01 is applied even if the IP MLT is connected via NAT	0-65535	180

InUC NAPT Setup

The **InUC NAPT Settings** screen is used for configuring the network details required for using InUC Browser Phone clients at remote locations to the SV9100.

- Easy Edit > Applications > InUC > InUC NAPT Setup

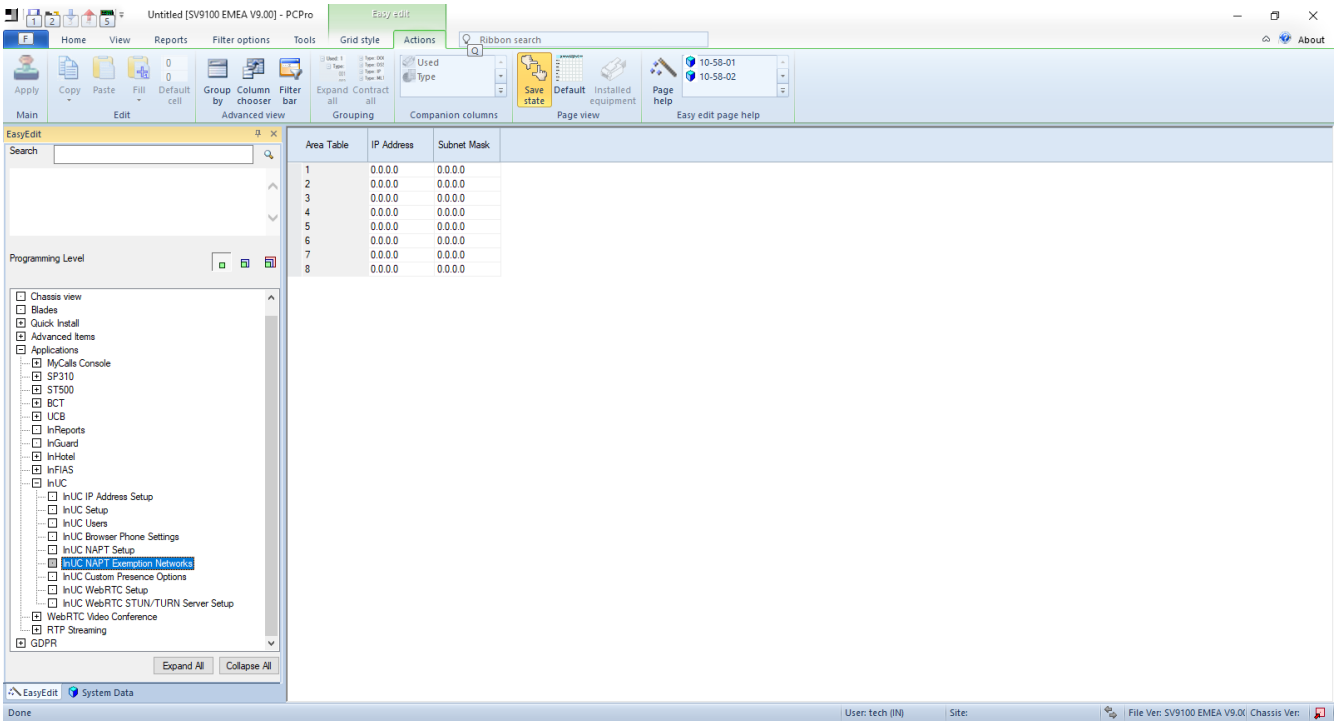


System Data Item	Item name	Input Data	Default Value
10-33-01	NAT Mode Enables NAT mode for standard SIP devices	0:Disabled 1:Enabled	0:Disabled
10-12-07	NAPT Router IP Address The Public IP address of the router connected to the SV9100 network.	0-9 (000.000.000.000)	0.0.0.0
10-37-01	UPnP Mode If the router supports UPnP this can be enabled to automatically learn the Public IP address of the router.	0:Disabled 1:Enabled	0:Disabled

InUC NAPT Exemption Networks

The **InUC NAPT Exemption Networks** screen is used for configuring the network details required for using InUC Browser Phone clients on local networks to the SV9100.

- Easy Edit > Applications > InUC > InUC NAPT Exemption Networks

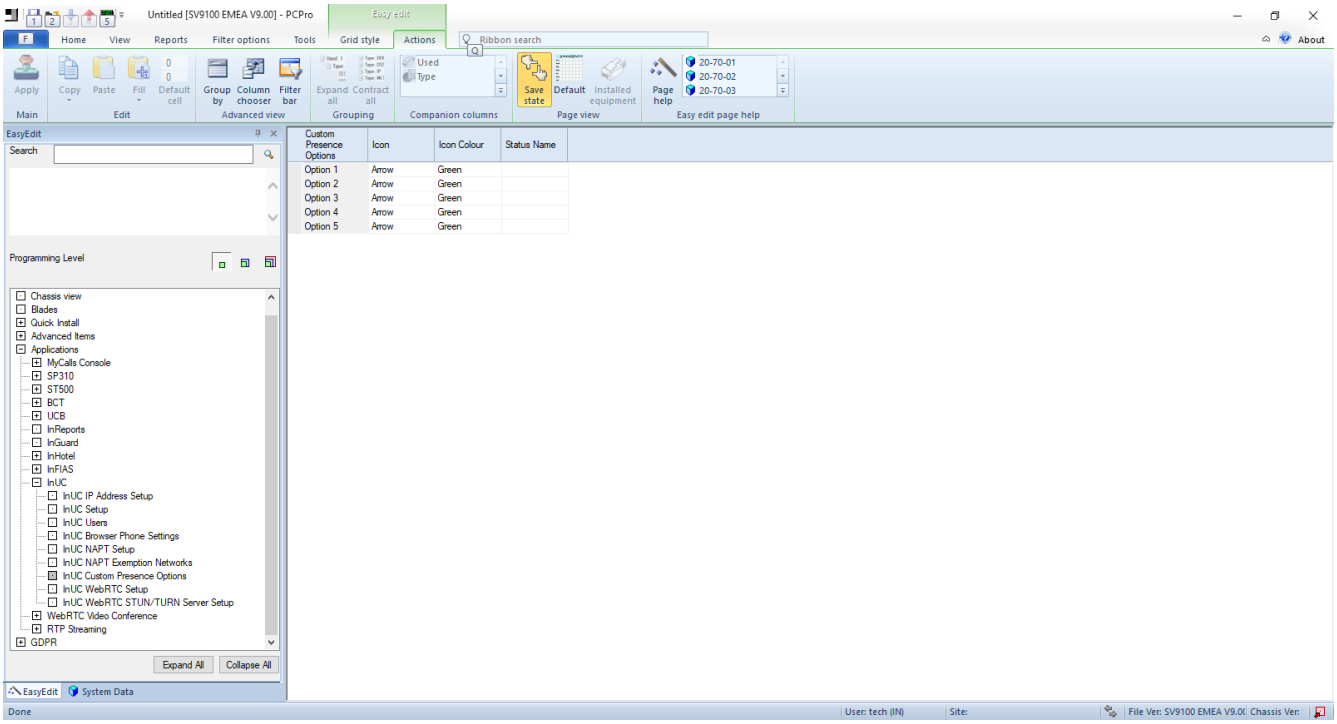


System Data Item	Item name	Input Data	Default Value
10-58-01	IP Address Enables NAT mode for standard SIP devices	0-9 (000.000.000.000)	0.0.0.0
10-58-02	Subnet Mask The Public IP address of the router connected to the SV9100 network.	0-9 (000.000.000.000)	0.0.0.0

InUC Custom Presence Options

There are 10 standard Status Messages available by default for presence indication. Using this screen you can define up to 5 custom Status Messages for your individual organisation's needs.

Easy Edit > Applications > InUC > InUC Custom Presence Options

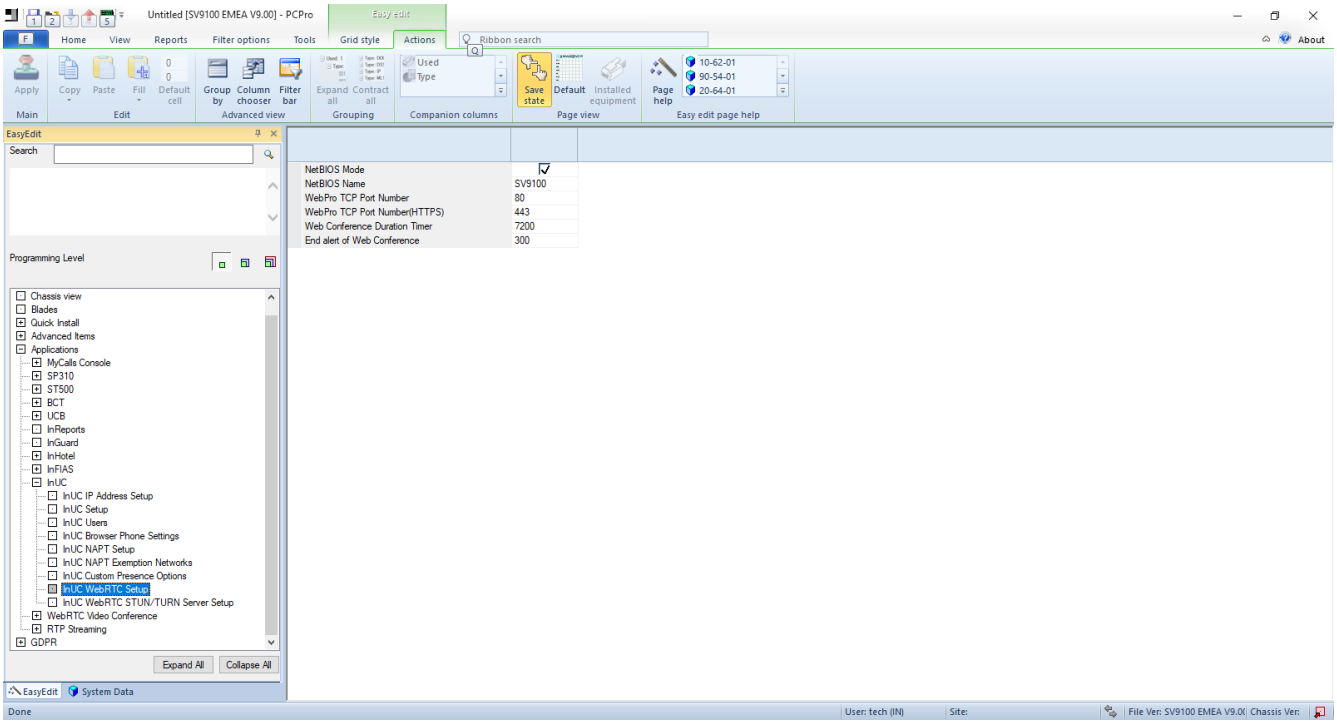


Program Data	Name	Input Data	Description	Default Value
20-70-01	Icon	0:Arrow 1: Asterisk 2: At 3: Bed 4: Coffee 5: Book 6: Building 7: Lock 8: Mobile 9: Subway	Defines the presence icon for the custom presence item.	
20-70-02	Icon Colour	0: Green 1: Orange 2: Red	Defines the colour of the selected presence icon.	
20-70-03	Status Name	Up to 16 characters	Defines the name used for the custom presence item.	

InUC WebRTC Setup

The **InUC WebRTC Setup** screen is used for configuring common settings for using the WebRTC video conference feature of the InUC application.

Easy Edit > Applications > InUC > InUC WebRTC Setup



Program Data	Name	Input Data	Description	Default Value
10-62-01	NetBIOS Mode	0: Disabled 1: Enabled	Defines	1: Enabled
10-62-02	NetBIOS Name	Up to 15 characters	Defines the NETBIOS name used by the system.	SV9100
90-54-01	WebPro TCP Port Number		Defines the TCP port used for HTTP WebPro access.	80
90-54-03	WebPro TCP Port Number (HTTPS)		Defines the TCP port used for HTTPs WebPro access. Change if 443 is being used as the InUC access port.	443
20-64-01	Web Conference Duration Timer	0 ~ 64800	Defines a timer used for the maximum WebRTC video conference time. When the timer expires the conference is automatically ended.	7200
20-64-02	End Alert of Web Conference	0 ~ 64800	Defines a timer used for warning the WebRTC video conference users that the conference is going to end.	300

InUC WebRTC STUN/TURN Server Setup

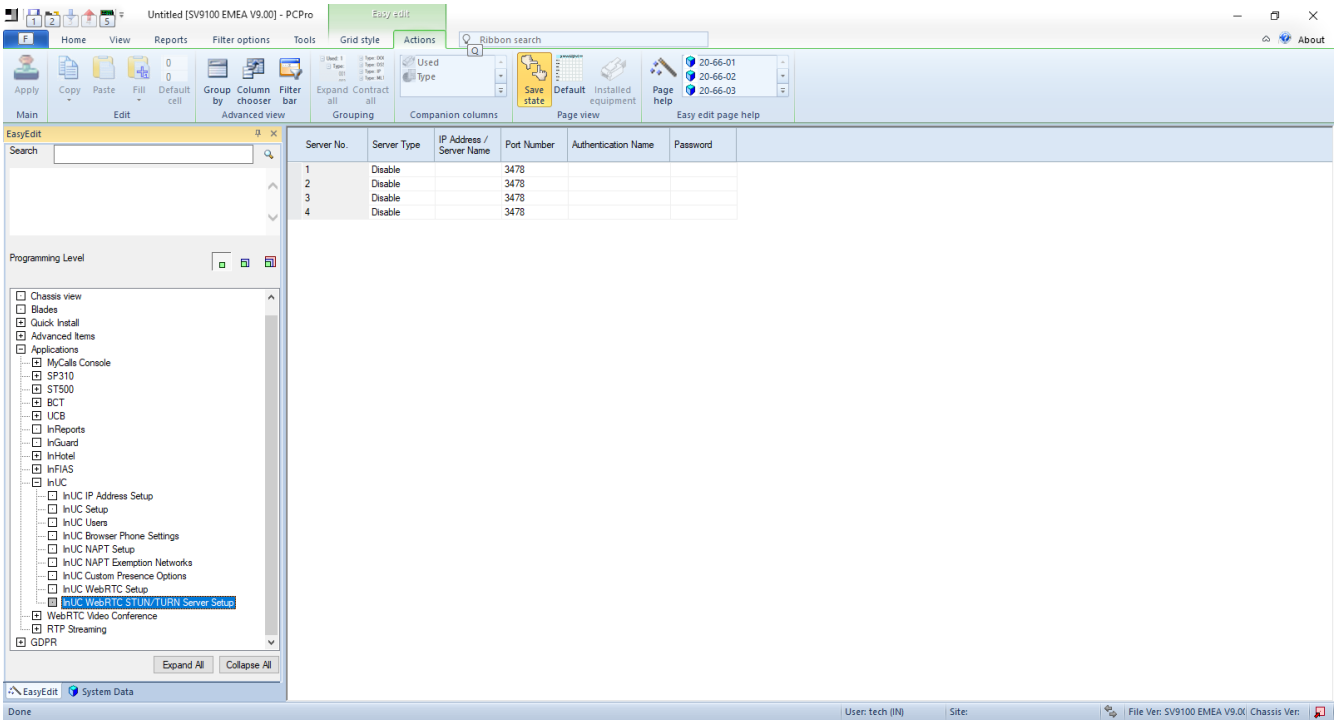
The **InUC WebRTC STUN/TURN Server Setup** screen is used for configuring STUN/TURN server settings for allowing InUC clients to automatically learn their Public IP address details.

If a locally deployed STUN/TURN Server is NOT to be used then NEC recommends the use of a third party STUN/TURN server. Details of which are:

Server Type: TURN
IP Address/Server Name: numb.viagenie.ca
Port Number: 3478
Authentication Name: xxxxxxxx
Password: xxxxxxxx

The Server Name, Authentication Name and Password can be obtained/configured by creating a FREE account at http://numb.viagenie.ca/

Easy Edit > Applications > InUC > InUC WebRTC STUN/TURN Server Setup



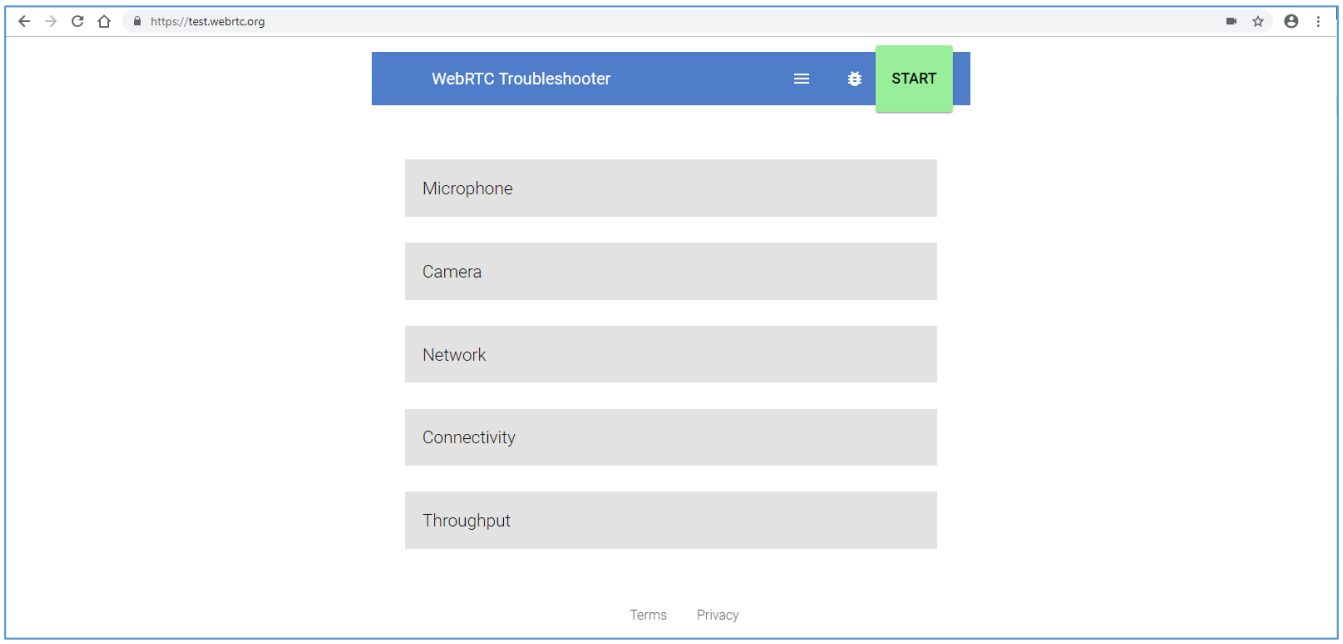
Program Data	Name	Input Data	Description	Default Value
20-66-01	Server Type	0: Disable 1: STUN Server 2: TURN Server	Enable the usage of STUN or TURN server settings.	0:Disable
20-66-02	IP Address / Server Name		Enter the IP address or FQDN of a valid STUN or TURN server.	Blank
20-66-03	Port Number		Enter the port number used by the STUN or TURN server	3478
20-66-04	Authentication Name		If required enter an authentication name	Blank
20-66-05	Password		If required enter an authentication password.	Blank

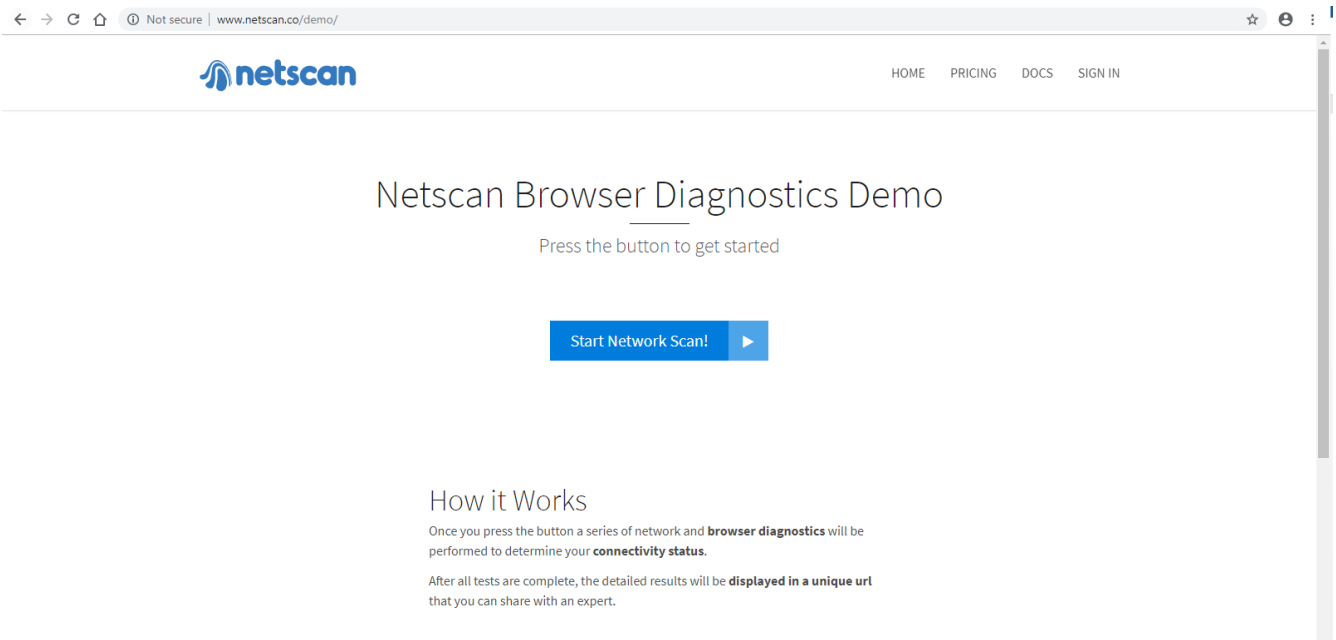
Troubleshooting

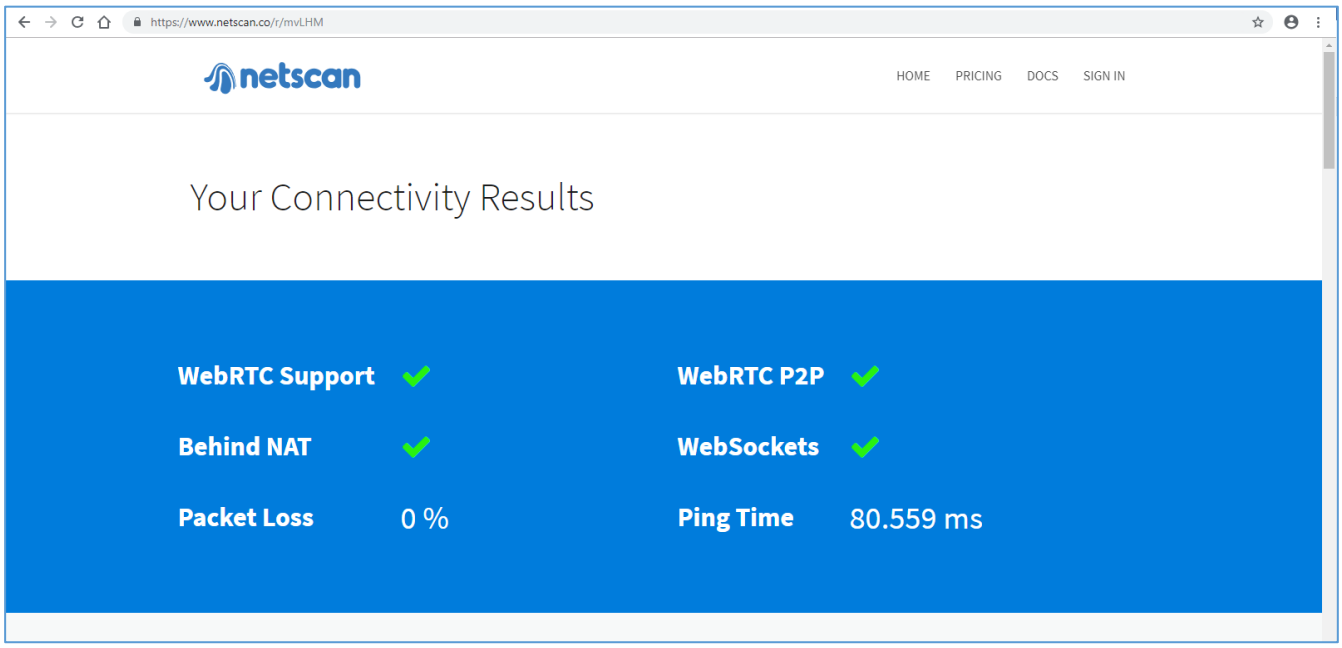
Depending on the network environment, you may have audio/video issues when trying to use the WebRTC video conference feature.

If you do experience issues we recommend that you first go to the following links and run the system checks to make sure that WebRTC operation is working normally.

You can check your system meets the WebRTC requirements either at: https://test.webrtc.org or http://www.netscan.co/demo/






https://www.netscan.co/r/mvLHM
netscan
HOME
PRICING
DOCS
SIGN IN
Your Connectivity Results
WebRTC Support
WebRTC P2P
Behind NAT
WebSockets
Packet Loss
0 %
Ping Time
80.559 ms

Notes and Limitations

- If the Webpro TCP port is changed from default in Program 90-54-01, the port needs to be included in the InUC URL. For example, if Program 90-54-01 is set to 7777, then the InUC URL would be http://{IP address}:7777/uc/
- The information shown in user details when clicking a buddy list entry is pulled from Program 20-57.
- When sending an instant message, pressing the Enter key will carriage return to the next line. To send a message with the Enter key, Program 20-64-05 should be set to 1: SendIM.
- Sort settings are not retained when moving from a sorted home screen to another InUC
- Web Client screen and back. When going back to the home screen from any other view, the home screen is sorted by default in alphabetical grouping.
- If the SV9100 system is reset, InUC Web Client presence information and status messages are not retained. Users must reset all presence and status messages.
- In a NetLink environment, InUC Web Client users must point to the URL of the main system. Pointing to the URL in the secondary system will display an "error 204 nocontent" .
- SV9100 supports a maximum of 255 InUC Web Client users.
- Instant Message is a one to one or one to many but is not many to many. For example, if a users sends an instant message to three users, when they reply, only the user that sent the original message receives it, not all three.
- The following is a maximum number of Instant Messages that can be stored in the activity history.
    - GCD-CP10: 500 per user in the client application
    - GCD-CP20: 100 per user in the system
    - When this limit is reached, the oldest message is removed to make room for the new message.
- Instant Message History
    - A maximum of 100 sending and receiving messages can be saved each login account. These messages are saved on the SD-card. When log-in again, the saved messages will appear within the Instant Message Window.
    - When the system database is initialized, messages on SD-card are lost.
    - When the system is rebooted, messages on SD-card remains.
    - To save messages on SD-Card, 50MByte disk space is required.
    - If less than 50 Mbyte, Instant Message History is deleted, and Resend Instant Message from the system does not work.
- Resend Instant Message
    - When a message is sent to Off-Line client, the message is queued by the SV9100 system.
    - When message recipient becomes On-Line, the message is re-sent from the system automatically. Even if sender's browser is closed, the message will be sent to the recipient.
    - When the recipient queue is full, sending message is fail. The error is displayed at the sender's screen.
    - When the sender's message history exceeds 100 messages, if sender's message is queuing
    - in the system, the message in queue may be lost. The error is not displayed at the sender's screen. For example, if the sender sent over 100 messages but some messages were queued. Then messages in queue may not reach to the recipient.
    - When the sender is Off-Line, the message will be queued by sender's client. When the recipient becomes On-Line, the message is sent. In this case, the message is not queued by the system. If the browser is closed while in queue, the message is lost.
    - If Programming 20-57-01 User ID is changed while there are queued messages in the system, these messages are lost.
- The device must meet the specs recommended below or delays can occur in video:
    - Windows – Core i5 2.7 GHz or better CPU with 4 GB of RAM
    - Android – Quad-Core 2.5 GHz or better CPU with 3 GB of RAM
- If InUC Web Client B logs in with the user ID of InUC Web Client A who is already logged in,
- Client A will be logged out with the option to reconnect.
- When the window size is less than 520px, the list mode is displayed on the home page. If the window size is larger than 520px, the card mode is displayed in the home page.

- BLF status is displayed even when an InUC user is not logged into InUC Web Client.
- If the user is Offline, the Presence Icon is grayed out. If the user is online, the Presence icon is colored in.
- One Call Forward and DND icon is shown for all Call Forward and DND types.
- If a URL that starts with HTTP:// or HTTPS:// is sent in an Instant Message, it is displayed as a hyperlink in the message. If the user clicks the hyperlink, it will open in a new browser window.
- If the IM port is set to 0 in Program 20-64-03, no web clients sessions will be accepted.
- If a user has multiple Email addresses in Program 20-57, when initiating an Email from
- InUC Web Client, the 1st Email address is used.
- When a user invites someone to a Video Conference, the invitation is sent as a hyperlink in an Instant Message
- When a client creates a Video Conference, the conference page opens in a new browser window.
- If a device goes into hibernate mode, logged in InUC Web Clients will be disconnected with an option to reconnect.
- When an IM is received, Chrome on a mobile device will show a notification in the web client window.
- In Chrome on PC, a popup notification is shown at right-bottom of the screen. If user clicks the popup notification, the IM window is opened. When the IM window has already opened, the IM window moves to the front.
- In Internet Explorer 11 on PC, if a parent window is minimized in task bar, a parent window moves to the front. If a parent window has shown, a name of parent window in task bar blinks.
- When using Android OS, a notice action isn't performed at the time of receiving IM.
- Call Control functions are not supported by the Demo/Free license. The Encryption license
- (0030) is not included in the Demo/Free license. Desktop Phone Mode requires license
- 0082 (InUC Web 1st CTI).
- If an InUC Web Client user loses connection for more than five minutes, other clients will show the disconnected user as Offline.
- The extension number the InUC Web Client controls is set in Program 20-57-41.
- If the controlled desktop phone is for a SLT, only Call is supported.
- If the user logs into InUC Client while the controlled phone is not idle, the status is not updated and will update when the phone goes idle.

- If a user enables headset mode (Program 11-11-65), a Headset key (05) must be programmed on the phone for the InUC Web Client to be able to control the phone.
- Call History is only shown when logged in with desktop phone mode, browser phone mode or ST500 Mode.
- Call History only supports multiline terminals.
- Call History displays a maximum of 50 called numbers and a maximum of 50 incoming numbers. If the number of calls exceeds these limits, the oldest calls are deleted from the list.
- For the desktop phone mode, at default, Call History will only show the latest call from a number. To see each call from the same number, Program 15-02-73 should be set to 1:unpack. Even with Program 15-02-73 set to 1:unpack, multiple calls within the same minute only show the latest call.
- The Function Key page shows the name and additional data of the programmed key including the color and blink pattern of the key.
- The Function Key page does not support DSS consoles.
- The Function Key page only shows keys the phone physically has or is licensed for. If a phone has 12 keys but is programmed in the system with 48 function keys, only the 12 actual keys will show on the Function Key page.
- A maximum of 32 Function Keys are supported on the InUC Web Client Function Key page.
- If Function Keys are changed, a re-login is required to apply the changes to the web client.
- If Custom Presence states are changed, the InUC Client will not reflect any changes until a re-login occurs.

- InUC Web Client does not support virtual extensions for call control. Program 20-57-41 cannot be a virtual extension. However, virtual extensions can appear on a button on the controlled extension.
- A dialed number string cannot contain a "P", "R" or "@". If the dialed number contains any of these, the telephone icon is not displayed.
- SV9100 TAPI integrations including UC Suite and InUC do not support virtual extension appearances of real extensions in Program 11-02 (Secondary Incoming Extensions (SIE) keys). Only virtual extensions assigned in Program 11-04 are supported.
- InUC Web Client supports multi-language display.
- When a user inputs a part of dial digits or name, the InUC Web client predicts the rest of the digits or name from a contact list and speed dial data. It will show a predictive list of candidates to the user in a drop down list.
- If you need to send additional dial digits while talking, click the Dial Pad button on the control bar. A Dial Pad appears, then click on the Dial button to send the DTMF tone. This feature is only available for Multiline terminals associated with InUC Web Client.
- An instant Message screen opens in the another window. Multiple windows can be displayed. Multiple windows is possible only from a PC. The tablet/smart phone is not supported.
- The system can use an SSL certificate from an SSL certificate provider for HTTPS connection.
- InUC Web Client Application can be updated without rebooting via User Programming (UA level) or Web Programming. 4MB of space in the SV9100 is required. Users might need to clear the browser cache after updating. Do not update from multiple PCs at the same time.
- The ST500 requires activation code 5b76f5ae44743c40 to enable UC support for the
- SV9100 CP20. UC Settings in the ST500 profile will not show up without this activation key.
- GT890 terminals do not support the Web Conference feature within the UC tab.

Conditions for Browser Phone Mode

- Browser Phone requires an Encryption license (0030).
- A VoIPDB card is required.
- A Web Phone License (0084) is required for Browser Phone Mode. This is a floating license- the number of installed licenses is the maximum number of clients that can be connected to the SV9100 at the same time. If there is no available license when a client attempts to login, an error message is displayed and the user may only login in no-phone mode. If the license is lack at logging in, the error message is displayed, and user can log in as a no-phone mode.
- When terminating media packets in VoIPDB, VoIPDB channel license is consumed. This call consumes one channel about one call as same as the conventional encrypted call.
- Peer-to-Peer (P2P) communication can be used in voice or video calls between Browser
- Phones when the P2P settings of the two browser phones are enabled. P2P communication does not consume a VoIP resource channel. P2P communication must be enabled to make a video call.
- Browser phone is not supported if NetLink setting is enabled in PRG51-01-01. When logging into browser phone mode in NetLink network, the error message is displayed and the InUC Web Client logs in as a no-phone mode.
- The video call between Browser Phone via AspireNet and SIP/H.323 system interconnection is not supported. It will be a Voice Call.
- When the user accesses with unsupported OS and browser, the “Browser Phone” is not displayed in select box of Telephony on Login screen.
- If a VoIPDB is not installed during log in, an error message is displayed and the user cannot log in no-phone mode.
- A Ringtone, Ringback tone and Holding tone are implemented in the browser phone. These sounds are fixed and they can't be changed.
- A USB Handset/Headset and Bluetooth Handset/Headset are supported as a microphone and speaker device. However, their key operations including a hook key of a device are not supported.
- Android OS and iOS is not supported.

- Only Chrome is supported.
- Video calls with Simple MCU and SIP video terminal are not supported.
- The call history data does not save to the SV9100 system, and when a client logs out, the call history data is deleted.
- Every time a call ends, the call history is generated automatically.
- The upper limit of the call history data on a client is 1000. When the call history data exceeds this limit, the oldest history data is deleted and the new history data is registered.
- Browser phone is not supported as an ACD Agent.
- Browser phone does not support ISDN sub addresses.
- When a browser phone answers a callback, recall, or initiates a call pickup, a VoIP resource is used regardless of peer to peer settings. Video cannot be used when this happens.
- If a user clicks Hold before a called trunk party answers, the call will end.
- Completing a transfer before a trunk party answers is not supported. The trunk party must answer before the transfer can happen. If transfer is attempted before the trunk party answers, the transfer fails and the call will recall.
- If two browsers phones are engaged in a call and switch the camera or microphone on/off, turn screen share on/off, click hold, or change video quality at the same time, the call will end.
- Browser phone only supports SIP info for DTMF. RFC 2833 is not supported.
- Barge-in to a video call cannot be used.
- In case of P2P communication disable, a Video call and video enable operation by a browser phone are restricted and the call will end.
- Browser Phones that have been registered and are logged out will show as BUSY in the
- BLF Area/Buddy List.
- If the InUC Web Client calls a station that is forwarded, the InUC Web Client shows you are ringing/talking to the forwarded station even after it has forwarded and been answered by the forward destination station.
- Use in following port is regulated in Chrome. Please confirm the latest edition by a Google Chrome site. Reference URL:
  https://src.chromium.org/viewvc/chrome/trunk/src/net/base/net_util.cc?view=markup

Regulated Port	Usage	Regulated Port	Usage	Regulated Port	Usage	Regulated Port	Usage
1	Tcpmux	77	priv-rjs	139	netbios	601	??
7	Echo	79	finger	143	imap2	636	ldap+ssl
9	Discard	87	ttylink	179	BGP	993	ldap+ssl
11	Systat	95	supdup	389	ldap	995	pop3+ssl
13	Daytime	101	hostriame	465	smtp+ssl	2049	nfs
15	Netstat	102	iso-tsap	512	print/exec	3659	apple-sasl/ PasswordServer
17	qotd	103	Gppitnp	513	login	4045	lockd
19	chargen	104	acr-nema	514	shell	6000	X11
20	ftp data	109	Pop2	515	printer	6665	Alternate IRC [Apple addition]
21	ftp access	110	Pop3	526	tempo	6666	Alternate IRC [Apple addition]
22	ssh	111	sunrpc	530	courier	6667	Standard IRC [Apple addition]
23	telnet	113	auth	531	chat	6668	Alternate IRC [Apple addition]
25	smtp	115	sftp	532	netnews	6669	Alternate IRC [Apple addition]
37	time	117	uucp-path	540	uucp	65535 (0xFFFF)	Used to block all invalid port numbers third_party/ WebKit/Source/ platform/ weborigin/ KURL.cpp, KURL::port
42	name	119	nntp	556	remotefs		
43	nicname	123	NTP	563	nntp+ssl		
53	domain	135	loc-srv/ epmap	587	stmp?		