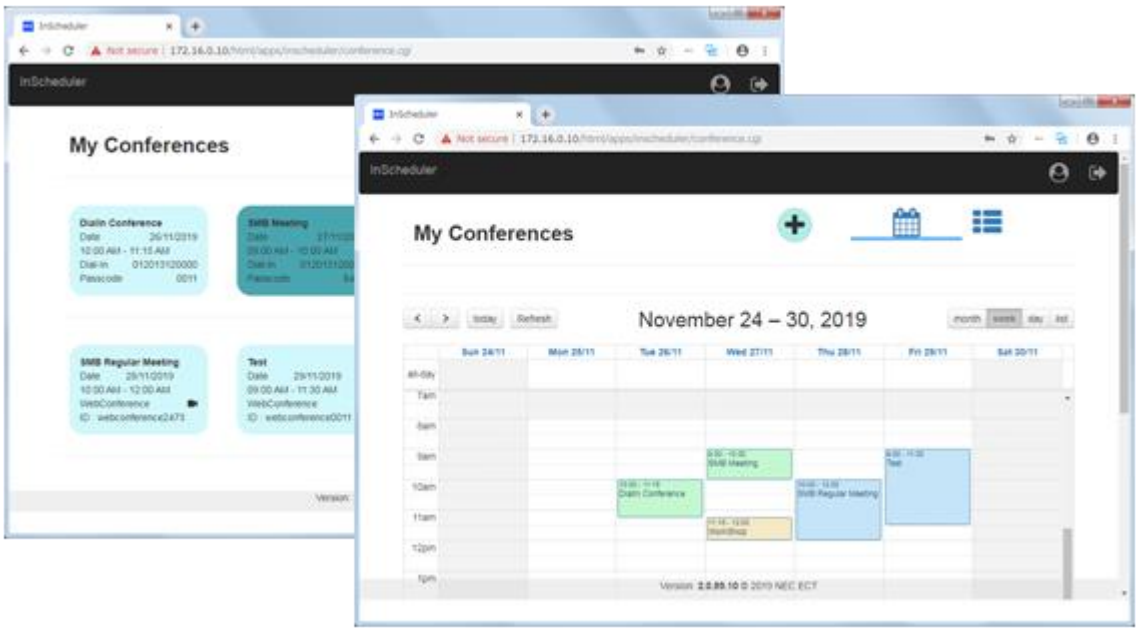
SV9100 InScheduler Installation Manual



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

Contents

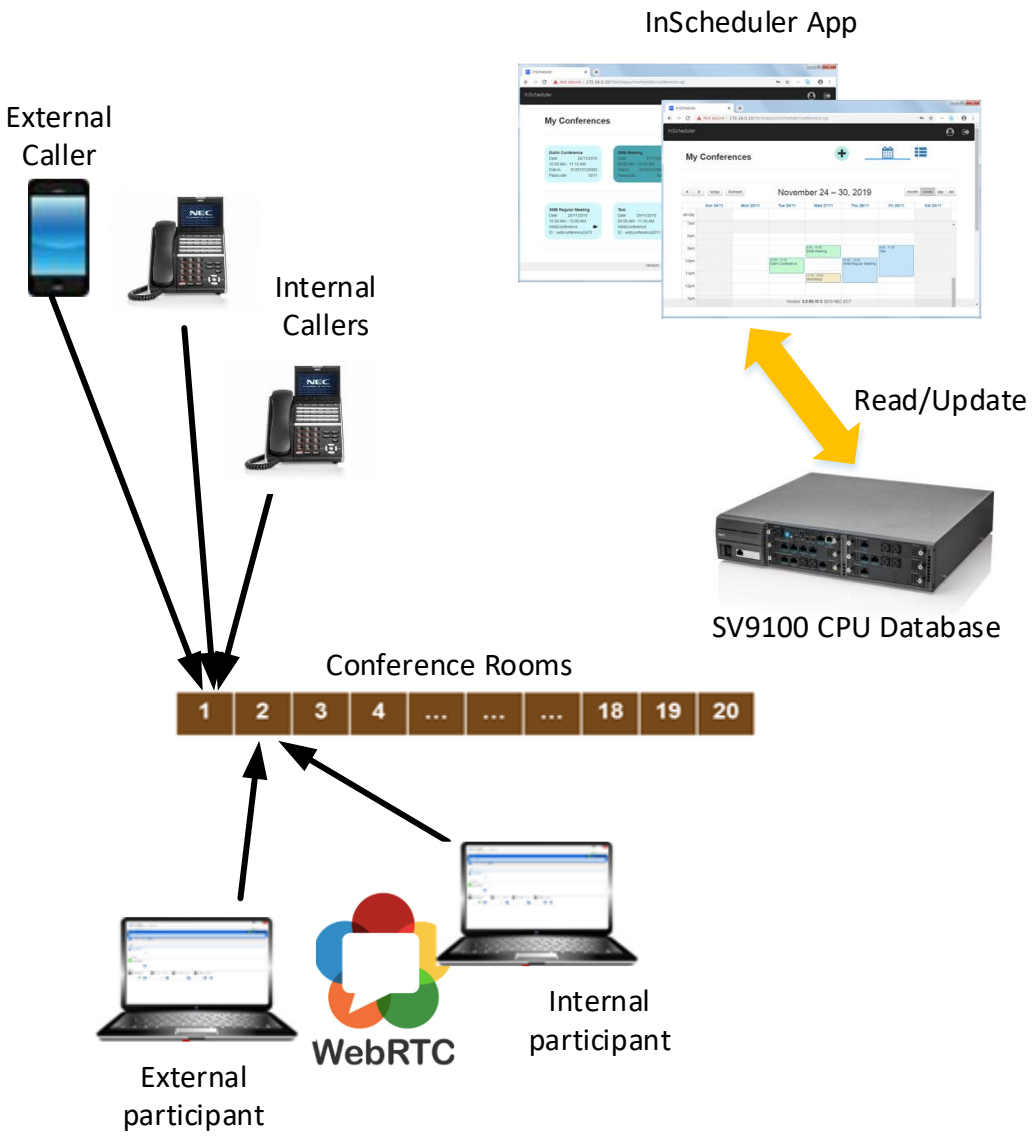
What is InScheduler?

The Conference InScheduler app is an application that is installed on the SV9100 system which provides users with the ability to schedule Remote Conferences and Web Video Conferences in the SV9100 system.

The SV9100 Remote Conference feature allows access into a secure conference group by dialling a conference pilot number. Conference circuits on the SV9100 system processor join each user to a conference based on the selected Conference Group number. The SV9100 Video Conference with WebRTC (Web-Conference) feature allows users to video conference using a unified communication Web Application in a browser. A maximum of four web-conferences and a maximum of eight users can participate in a web-conference.

The Conference InScheduler application leverages the Remote Conference feature and Web Video Conferencing of the SV9100 by allowing the scheduling of previously unreserved conference calls. The scheduling feature is available for multiple user logins who share the licensed Remote Conference resources.

A maximum of 32 conference participants is possible for one Conference and the system can be licensed for up to 20 Remote Conference groups or 4 Web Video conferences. Scheduling allows these resources to be reserved by unique passcodes automatically when needed and then released for other users.



System Requirements

SV9100 CP20 (v10.50.00)
Ethernet connection to either CCPU (for Remote Audio Conference only) or VoIPDB (for Remote Audio Conference and WebRTC Video Conference)

- The system must have the LUA Application manager. The manager can be accessed http://IP Address of the CPU/html/apps/manager.cgi
- The InScheduler App will require a functional Remote Conference feature.
-
- The InScheduler App will require a functional WebRTC Video Conferencing feature.
- The InScheduler LUA license is required
- Web Browsers
  - Google Chrome version 71 or higher.
  - Safari

NEC recommends that you have prior knowledge on the following:
- Domain Name System (DNS)
- Network Address Translation (NAT)

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.
- TCP port 80 by default or custom port number configured in PRG90-54-01 Web Pro TCP port Number, opened on Firewall from the public internet and forwarded to the SV9100 IPL IP Address (PRG10-12-09).
- TLS configuration is recommended when utilising WebRTC off net. 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).
- 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.

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.

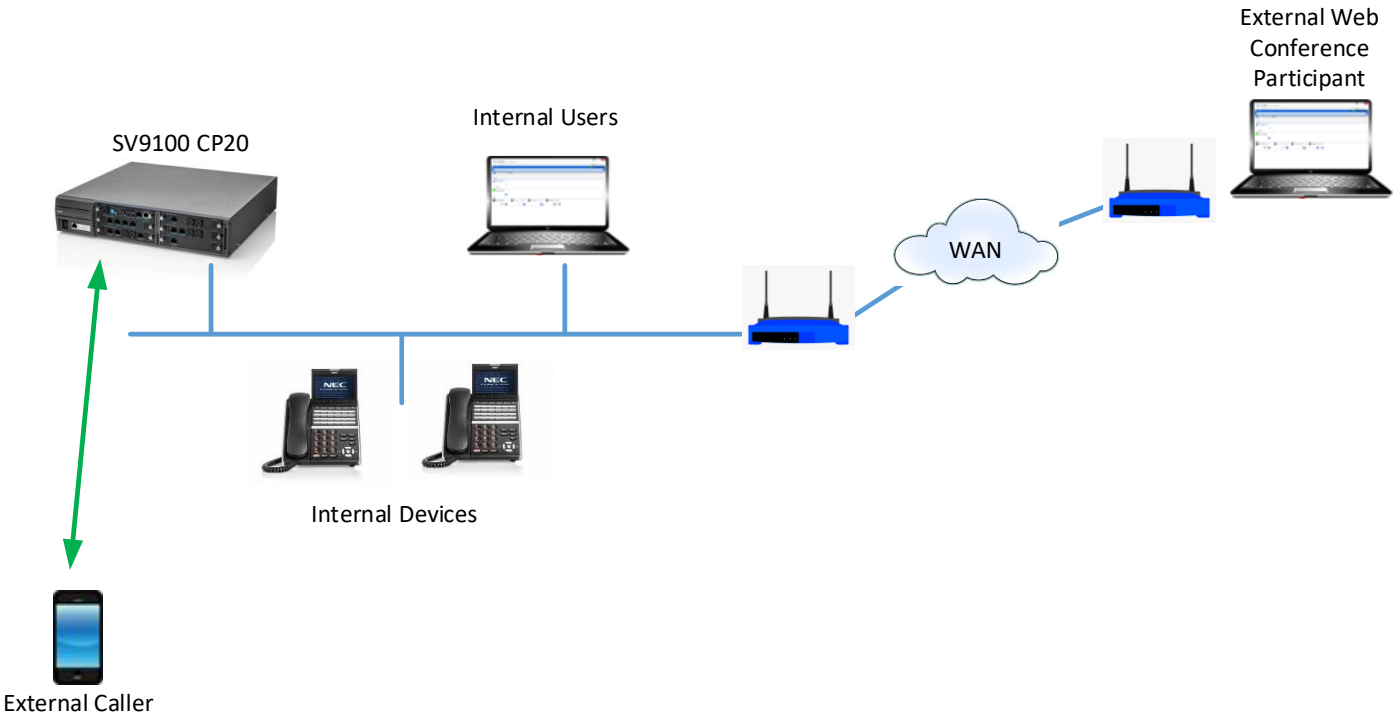
Application	Port Number(s)	Transport Protocol	WAN Router/Firewall Location
HTTPs	443 (default)	TCP	SV9100 Side - WebRTC Access
HTTP	80 (default)	TCP	SV9100 Side – InScheduler Access
HTTPs	8443	TCP	InScheduler access from InUC

SV9100 Licenses

Order Code	License Name	License Description
BE118840	Conference InScheduler LUA App License	This license is required for the application to be installed, to run and to be updated.
BE114073	Remote Conference License	The quantities of this license will determine the number of rooms that are available for scheduling.
BE119589	SV9100 Version License (R10)	System Software Version R10.
BE114082	SV9100 InMail VRS Port License	**SV9100 CP20 has 2 VRS licenses built in with the CPU**. If more are needed then this license is required. Used to set the password/pin for the conference.
BE114083	SV9100 InMail VM Box License	This license is required to set the recording option for the conference.
BE115845	Web Video Conference License	**SV9100 CP20 has 4 x Web Video Conference licenses built in with the CPU**. If more are needed then this license is required. The quantities of this license will determine the number of video conferencing users.

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.

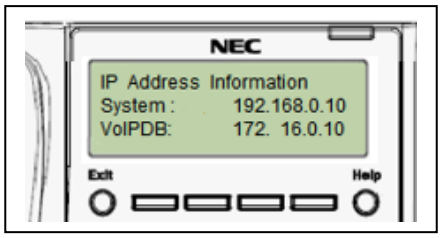
You must have SV9100 PCPro installed to your laptop/PC. This can be downloaded from BusinessNet.

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

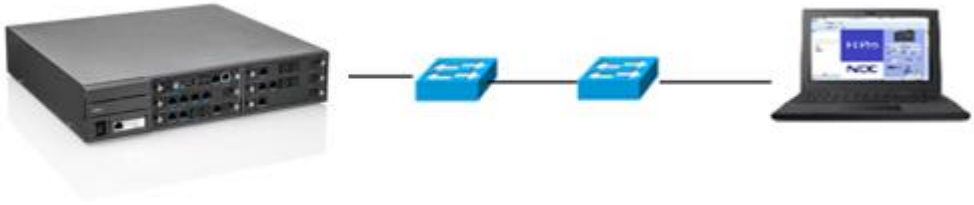
Connection default IP Address:
172.16.0.10 / 255.255.0.0

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



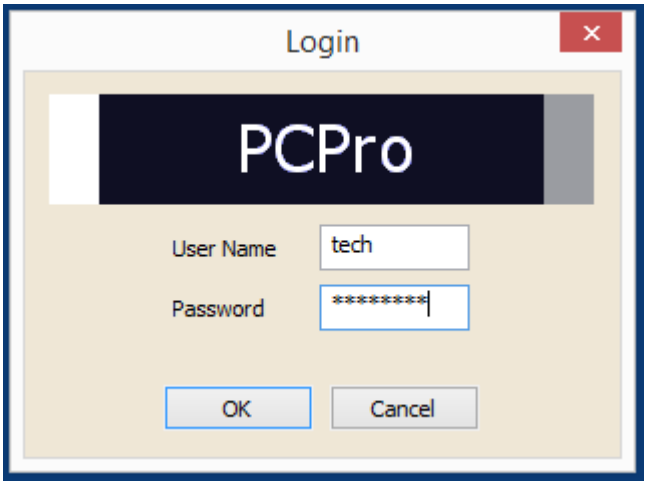
Direct to Ethernet connector on the SV9100 CPU card.

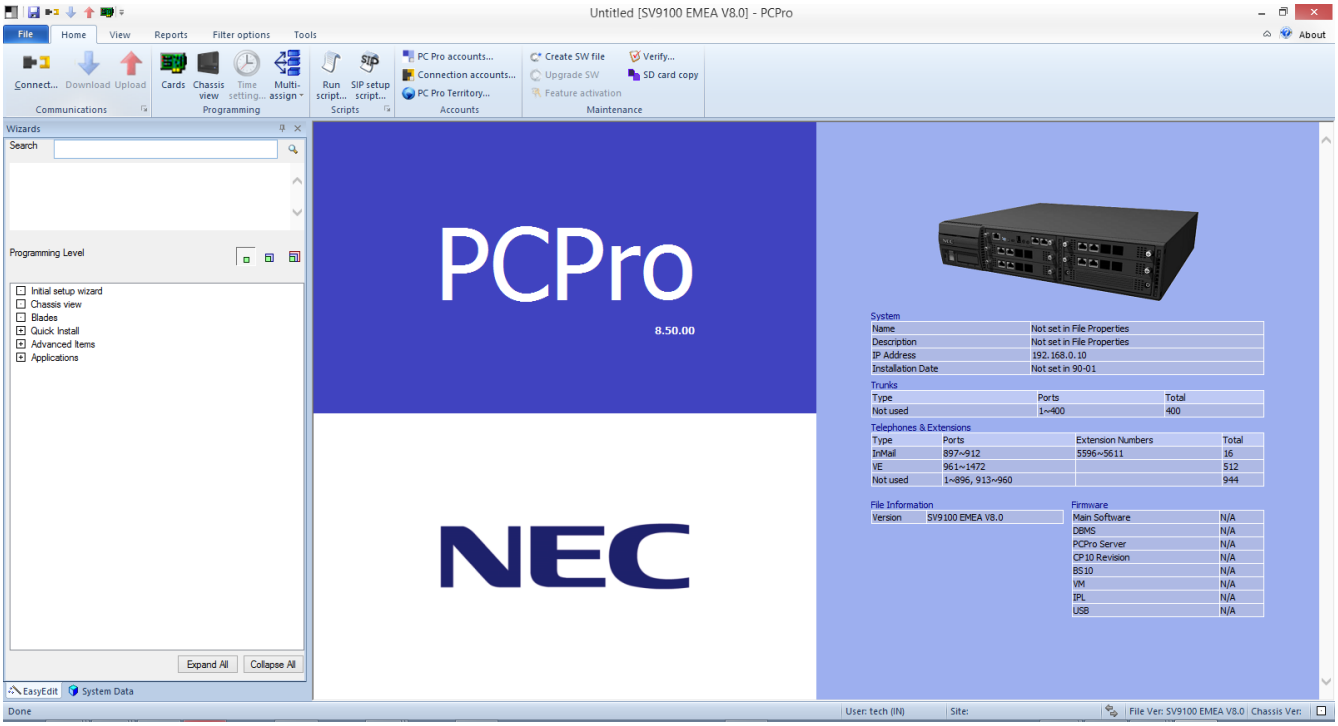
Via the customer's LAN.



SV9100 PCPro
Installer level access:
User Name: tech
Password: 12345678

It is highly recommended that the Installer login credentials be changed from the default to prevent unwanted access to SV9100 and InScheduler programming!

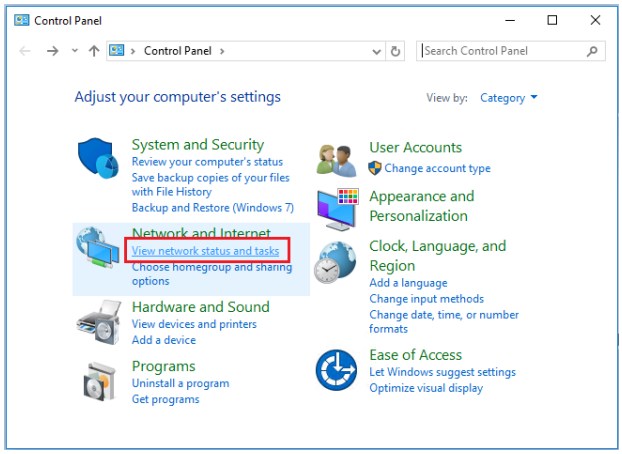




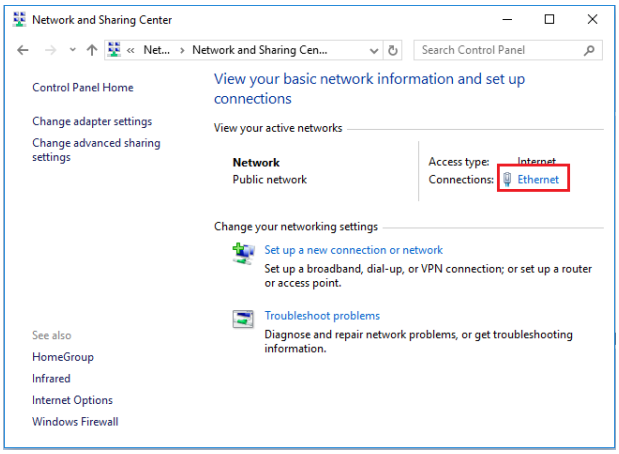
Change your PC IP Address

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'

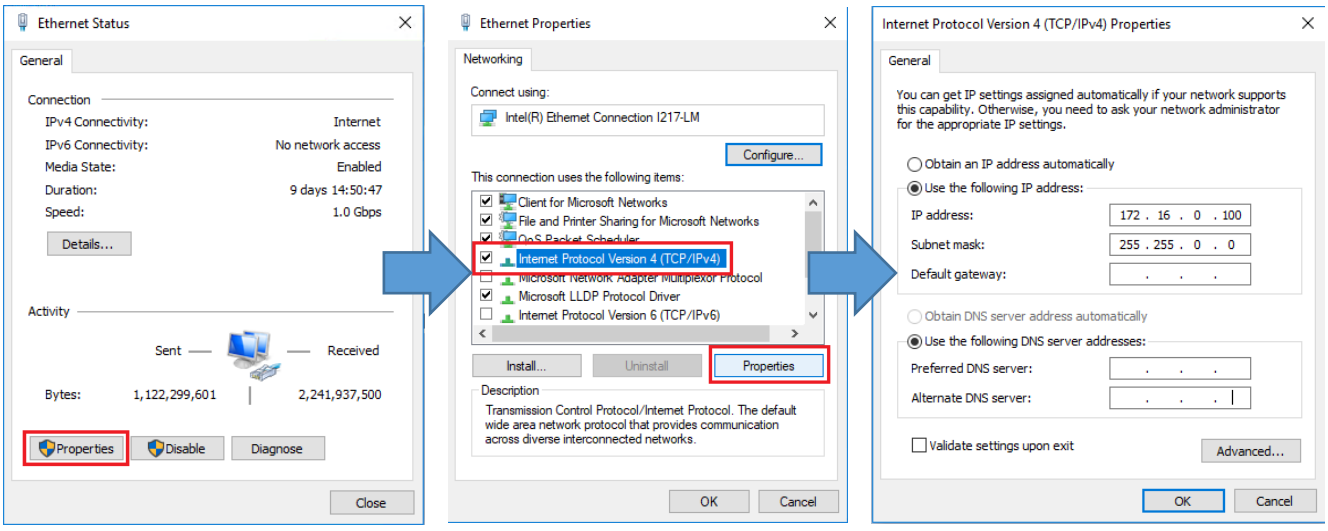


Edit the properties of your Ethernet adaptor



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.



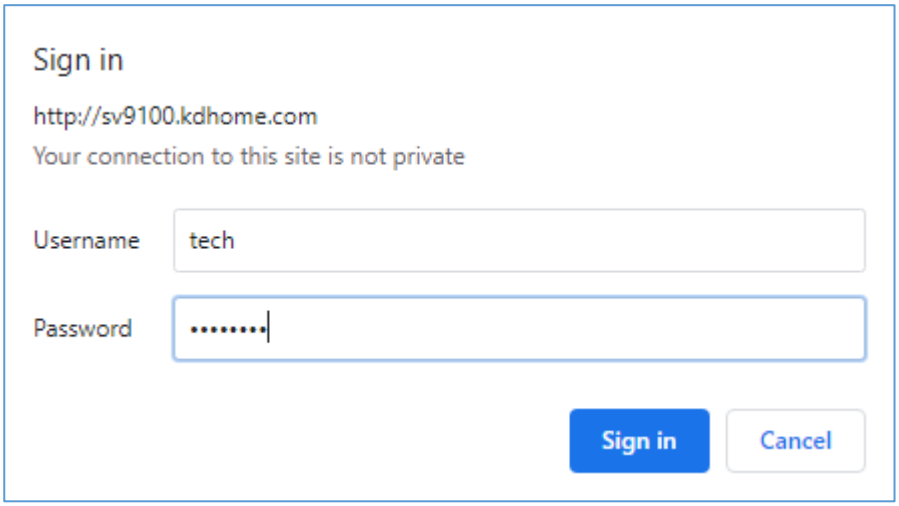
Install the InScheduler Application

The InScheduler Application is installed from the InApps Application manager. Access can be gained to this via the following URL, substituting the IP/FQDN of the SV9100 you're configuring.

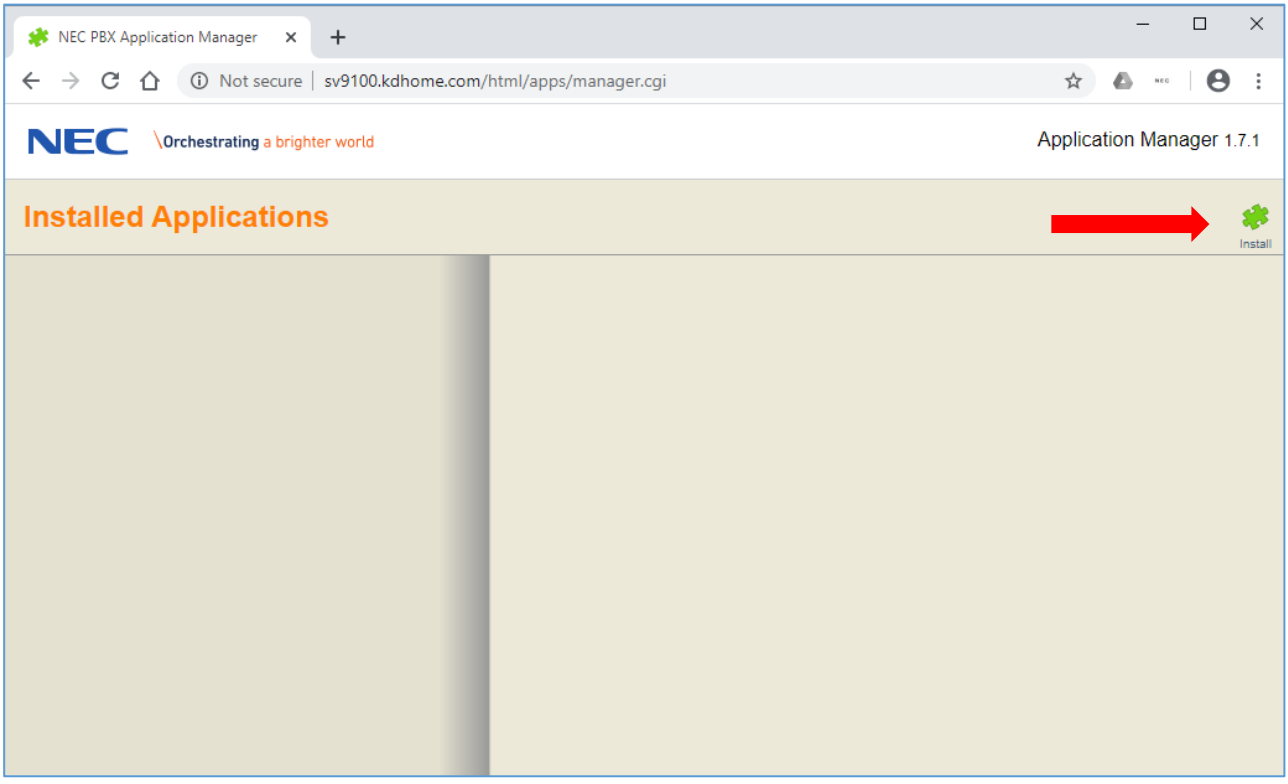
Error! Hyperlink reference not valid.

Application Manager access (default):
User Name: tech
Password: 12345678

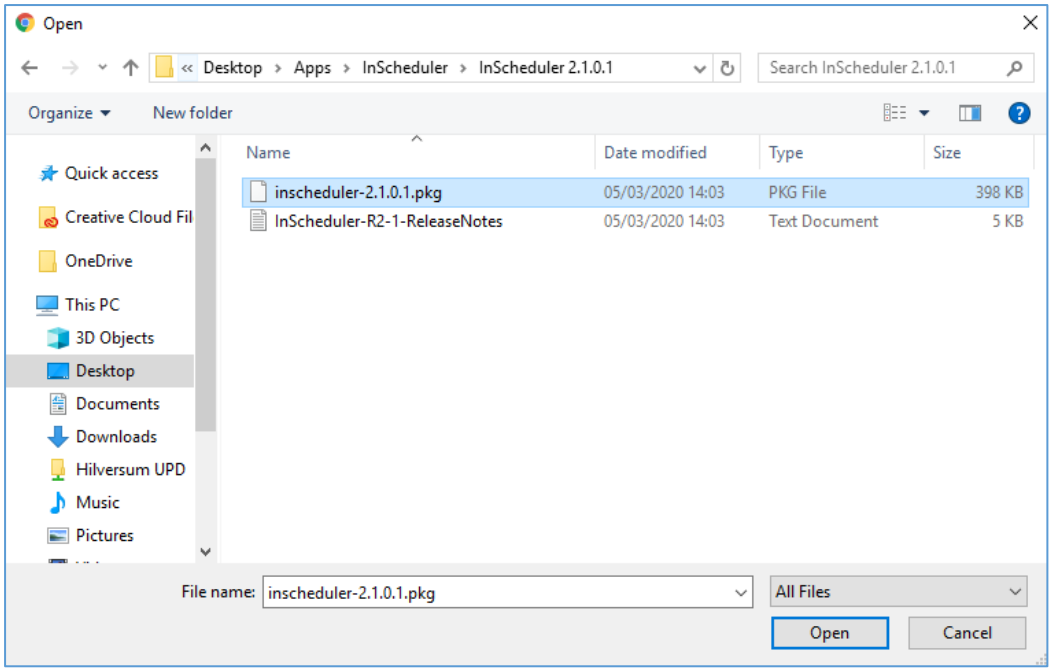
It is highly recommended that the Installer login credentials be changed from the default to prevent unwanted access to SV9100 and InScheduler programming!



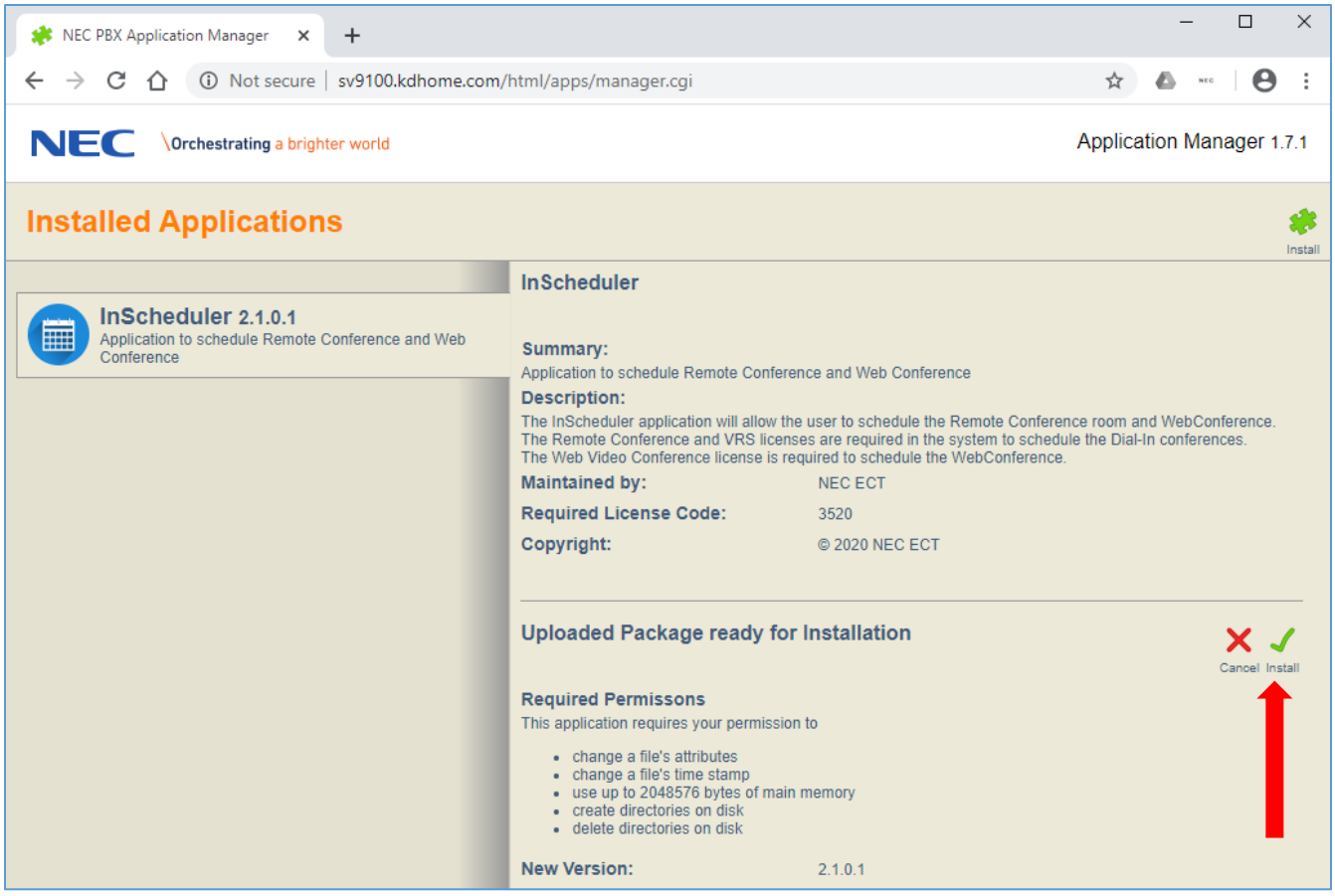
After logging in, select the Install option:



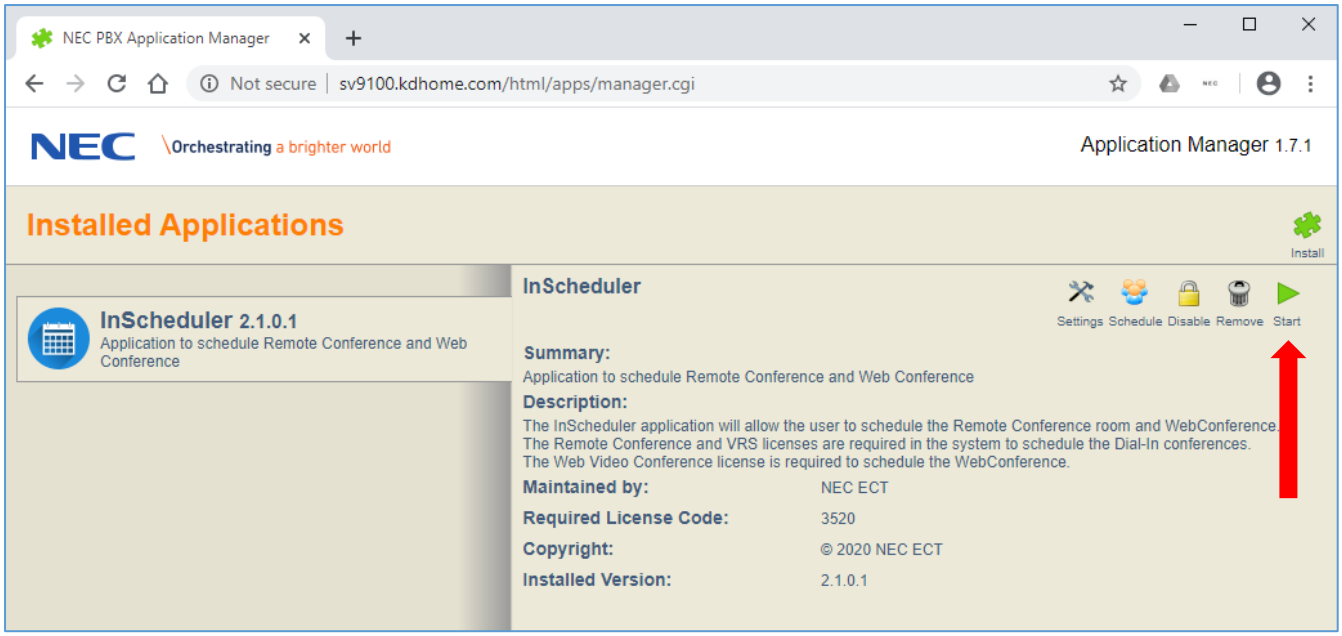
Browse to the location of the InScheduler installation package (.pkg) and select it.



Once the installation package has been uploaded, select Install to commence the installation of InScheduler:

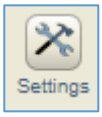


Once the installation is complete, InScheduler will need starting as a process, this is done by selecting Start:

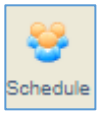


Once InScheduler is running, you can now perform the following:

- Access the Administration portal by selecting Settings.

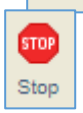


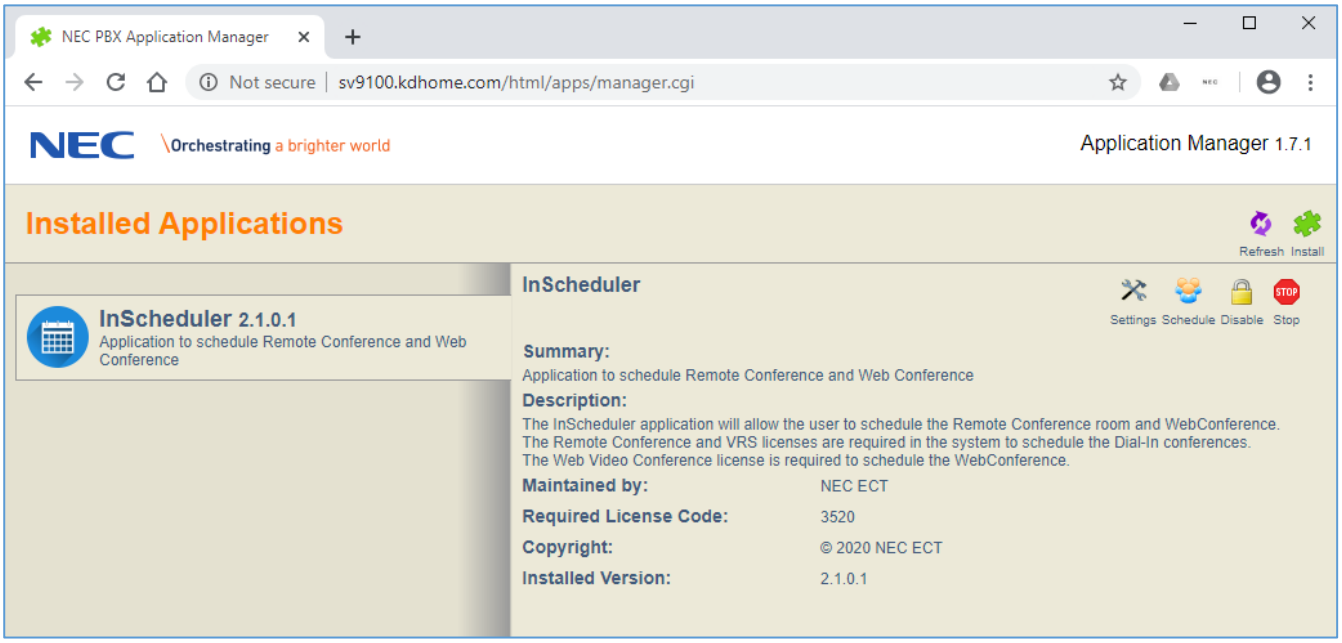
- Access the user login page to schedule a Remote conference or Web Conference.



- Disable the InScheduler Application.

- Stop the InScheduler Application.



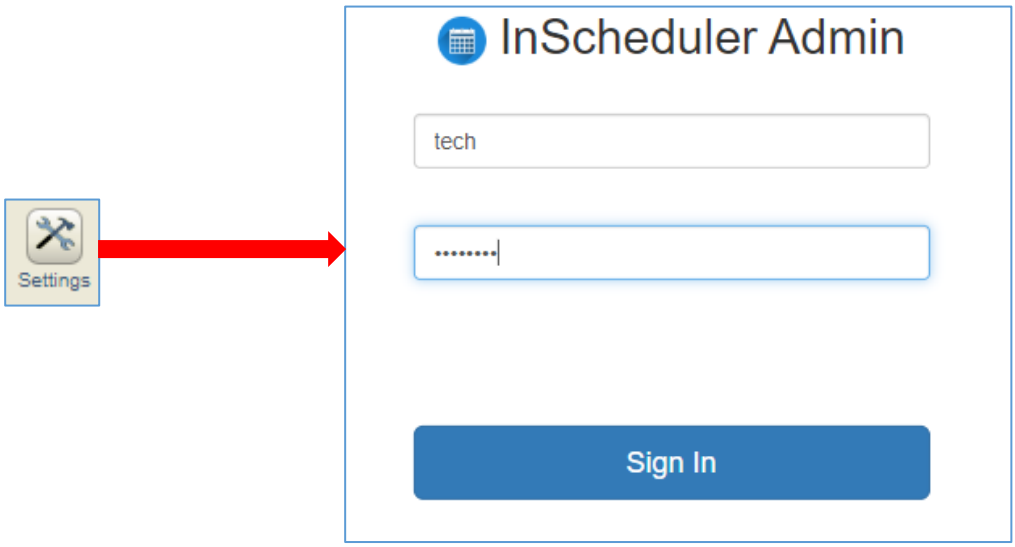


InScheduler Administration

The Administrator login for InScheduler follows the system setting for an Installer level login. The default user name and password are **tech/12345678.**

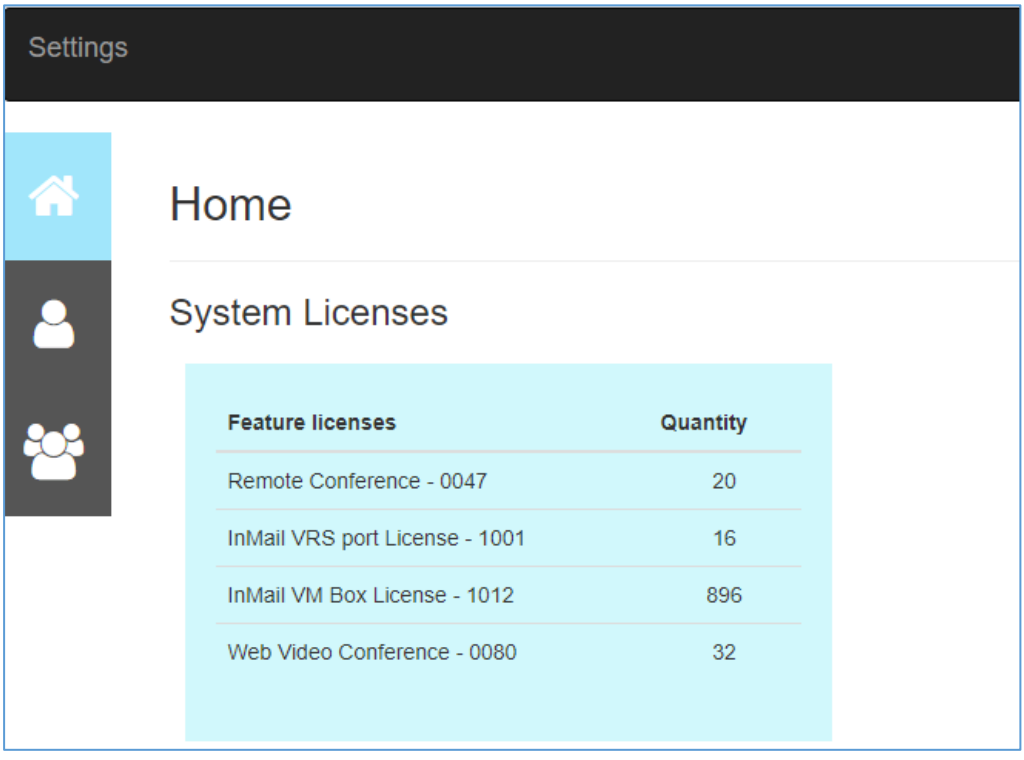
The InScheduler application will automatically retrieve this information from the system every few minutes.

It is highly recommended that the Installer login credentials be changed from the default to prevent unwanted access to SV9100 and InScheduler programming!



The home page will show the Administrator the required licenses for InScheduler and the quantity of each on the system, access to the list of users on the system and information about the conference rooms.

Lack of activity after 1 hour will result in the Administrator being logged out automatically.

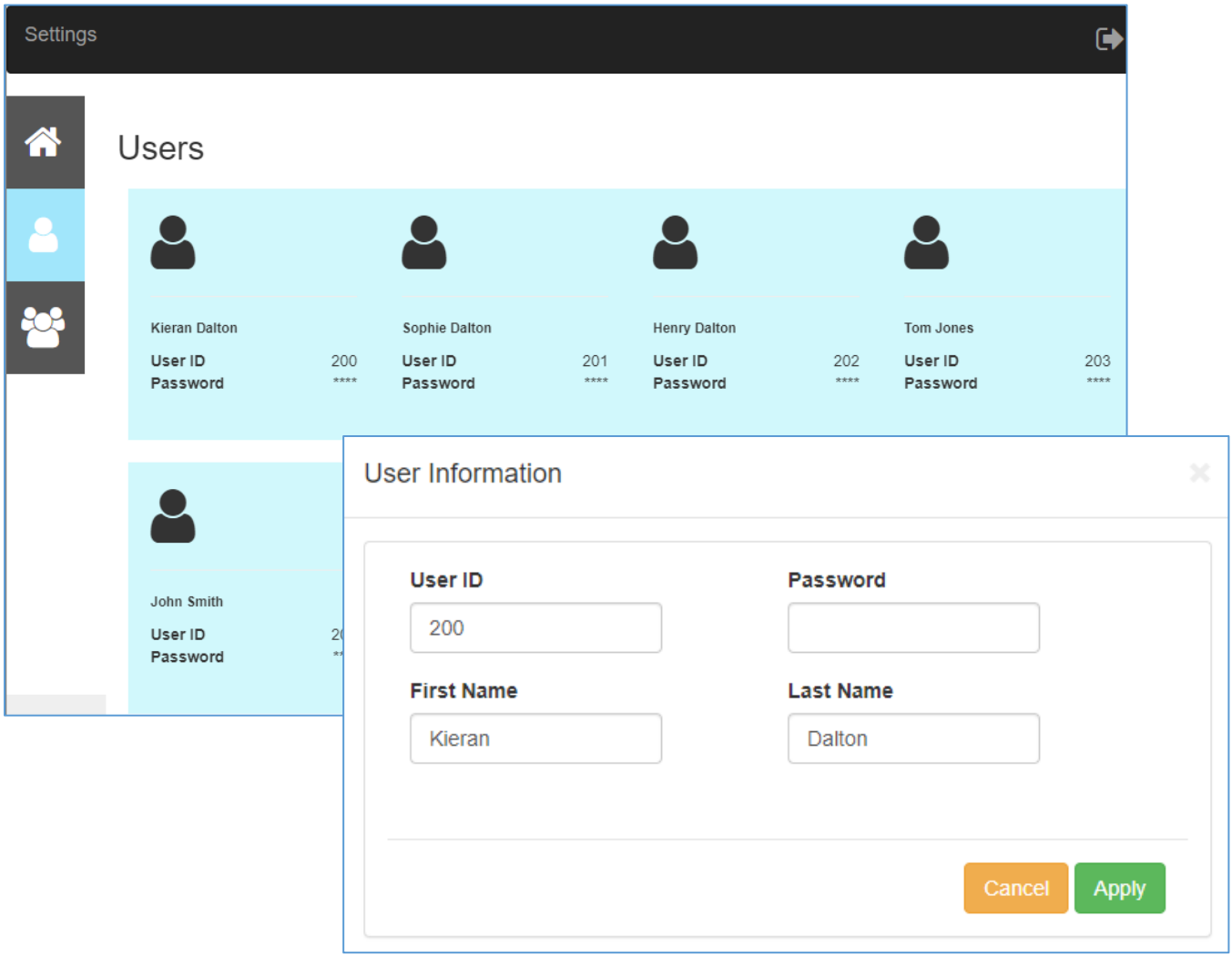


- The list of users shown is taken from PRG 20-57 in the SV9100. (Easy Edit > Applications > InUC > InUC Users.)

There are a maximum of 255 users available on the system. These users are used when video conferences using WebRTC are scheduled.

The User ID, password, first name and last name are shown. Selecting a user allows you to modify their password*, all other attributes are read only.

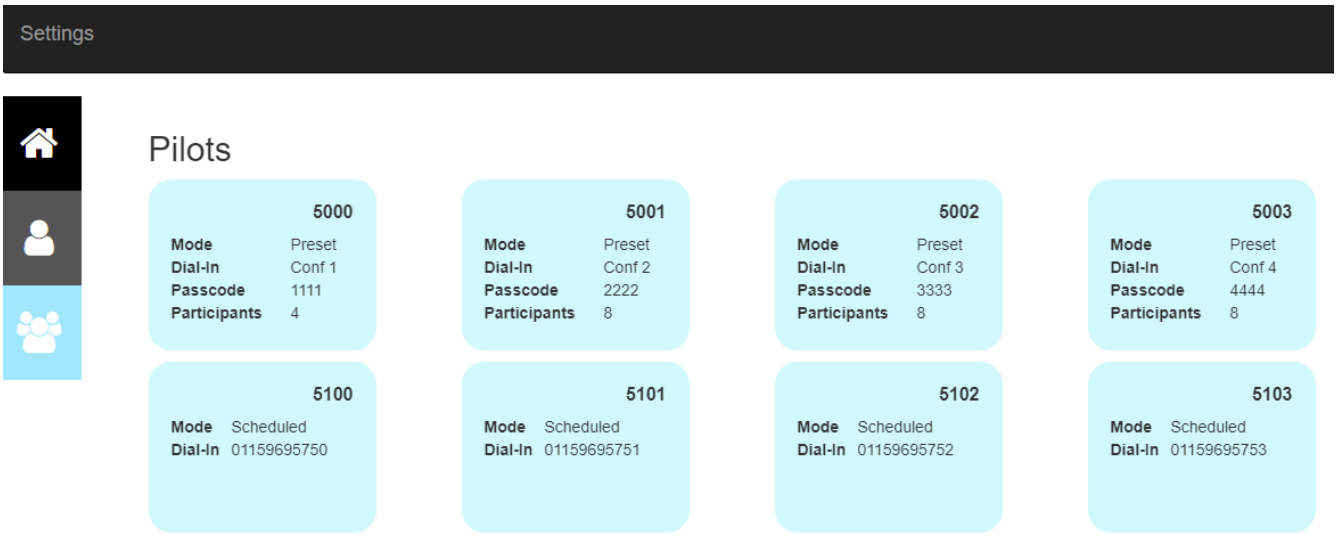
*Password must be a complex password.



- The list of conference rooms available is taken from PRG 20-34. (Easy Edit > Extensions> Extension > Remote Conference > Remote Conference Setup)

This list is only showing the Remote Conference rooms, and does not show anything related to video conference rooms using WebRTC.

The Pilot number is read only, however selecting a conference room will allow some changes to be made.



InScheduler will only use a conference room when the Password Mode has been set to **Schedule** in PRG 20-34-06. This means that some conference rooms can be used for adhoc requirements, where scheduling isn't required, and other conference rooms can be created and used by InScheduler exclusively.

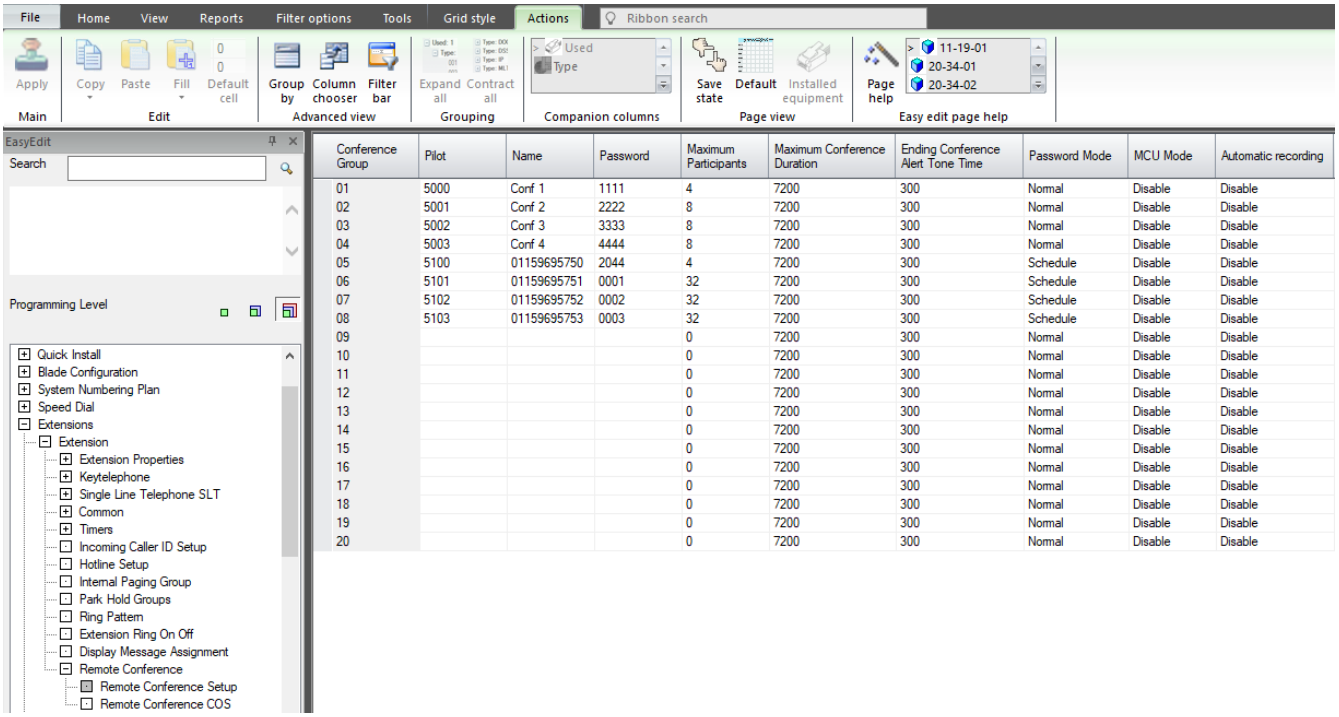
Conference Group	Pilot	Name	Password	Maximum Participants	Maximum Conference Duration	Ending Conference Alert Tone Time	Password Mode
01	5000	Conf 1	1111	4	7200	300	Normal
02	5001	Conf 2	2222	8	7200	300	Normal
03	5002	Conf 3	3333	8	7200	300	Normal
04	5003	Conf 4	4444	8	7200	300	Normal
05	5100	01159695750	2044	4	7200	300	Schedule
06	5101	01159695751	0001	32	7200	300	Schedule
07	5102	01159695752	0002	32	7200	300	Schedule
08	5103	01159695753	0003	32	7200	300	Schedule
09				0	7200	300	Normal

Remote Conference Configuration

InScheduler requires a functioning Remote Conference feature.

For InScheduler to reserve and assign a security passcode against a conference room, it must have a Password mode type of Schedule.

- Easy Edit > Extensions> Extension > Remote Conference > Remote Conference Setup



Conference Group	Pilot	Name	Password	Maximum Participants	Maximum Conference Duration	Ending Conference Alert Tone Time	Password Mode	MCU Mode	Automatic recording
01	5000	Conf 1	1111	4	7200	300	Normal	Disable	Disable
02	5001	Conf 2	2222	8	7200	300	Normal	Disable	Disable
03	5002	Conf 3	3333	8	7200	300	Normal	Disable	Disable
04	5003	Conf 4	4444	8	7200	300	Normal	Disable	Disable
05	5100	01159695750	2044	4	7200	300	Schedule	Disable	Disable
06	5101	01159695751	0001	32	7200	300	Schedule	Disable	Disable
07	5102	01159695752	0002	32	7200	300	Schedule	Disable	Disable
08	5103	01159695753	0003	32	7200	300	Schedule	Disable	Disable
09				0	7200	300	Normal	Disable	Disable
10				0	7200	300	Normal	Disable	Disable
11				0	7200	300	Normal	Disable	Disable
12				0	7200	300	Normal	Disable	Disable
13				0	7200	300	Normal	Disable	Disable
14				0	7200	300	Normal	Disable	Disable
15				0	7200	300	Normal	Disable	Disable
16				0	7200	300	Normal	Disable	Disable
17				0	7200	300	Normal	Disable	Disable
18				0	7200	300	Normal	Disable	Disable
19				0	7200	300	Normal	Disable	Disable
20				0	7200	300	Normal	Disable	Disable

Program Data	Name	Input Data	Description	Default Value
20-34-01	Remote Conference Group Setup - Conference Name	Up to 12 characters	InScheduler will use the value of this setting to show as the Dial-in number.	Conf x
20-34-02	Remote Conference Group Setup – Password	Maximum of 4 numbers.	Conferences 1 ~ 4 = 1111 Conferences 5 ~ 20 = blank	
20-34-03	Remote Conference Group Setup - Max participants	0 to 32	Conferences 1 ~ 8 = 8 Conferences 9 ~ 20 = 0	
20-34-04	Remote Conference Group Setup - Max Conference Duration	0 to 64800 seconds	7200 seconds	7200
20-34-05	Remote Conference Group Setup - End Tone Alert Time	0 to 64800 seconds	300 seconds	300
20-34-06	Remote Conference - Password Mode	0 = Normal 1 = Skip 2 =Schedule	0	Normal
20-34-07	MCU Mode for Remote Conference	0 = Disable 1 = Mode1 2 = Mode2	0	Disable

20-34-08	Conference Group Setup - Automatic Recording	0 = Disable 1 = Enable	0	Disable
20-34-09	Conference Group Setup - Destination Mail Box	Enter mailbox number: 1 ~ 896	No Setting	
11-19-01	Remote Conference Group Pilot Number	Must work within current system dialling plan.	No setting	
20-11-31	Transfer to Remote Conference Class of Service	0 = Disabled 1 = Enabled	COS 1 ~ 15 = 1	Enabled

WebRTC Video Conferencing Configuration

For Full configuration of InUC and its features including WebRTC please consult the SV9100 InUC Installation Guide. Available on BusinessNet.

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.

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.

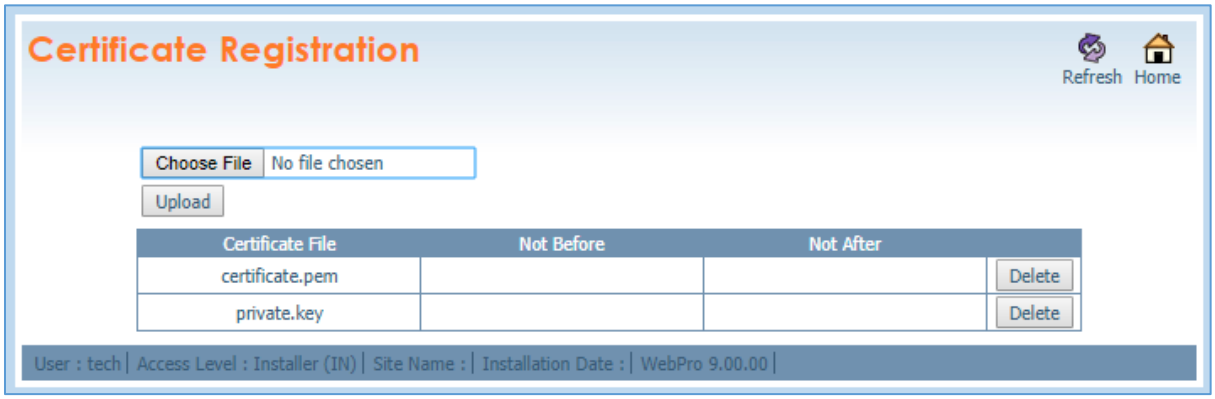
Application	Port Number(s)	Transport Protocol	WAN Router/Firewall Location
HTTPs	443 (default)	TCP	SV9100 Side InUC WebRTC
STUN/TURN*	3478	UDP	Client Side

* If utilising a locally deployed STUN/TURN server.

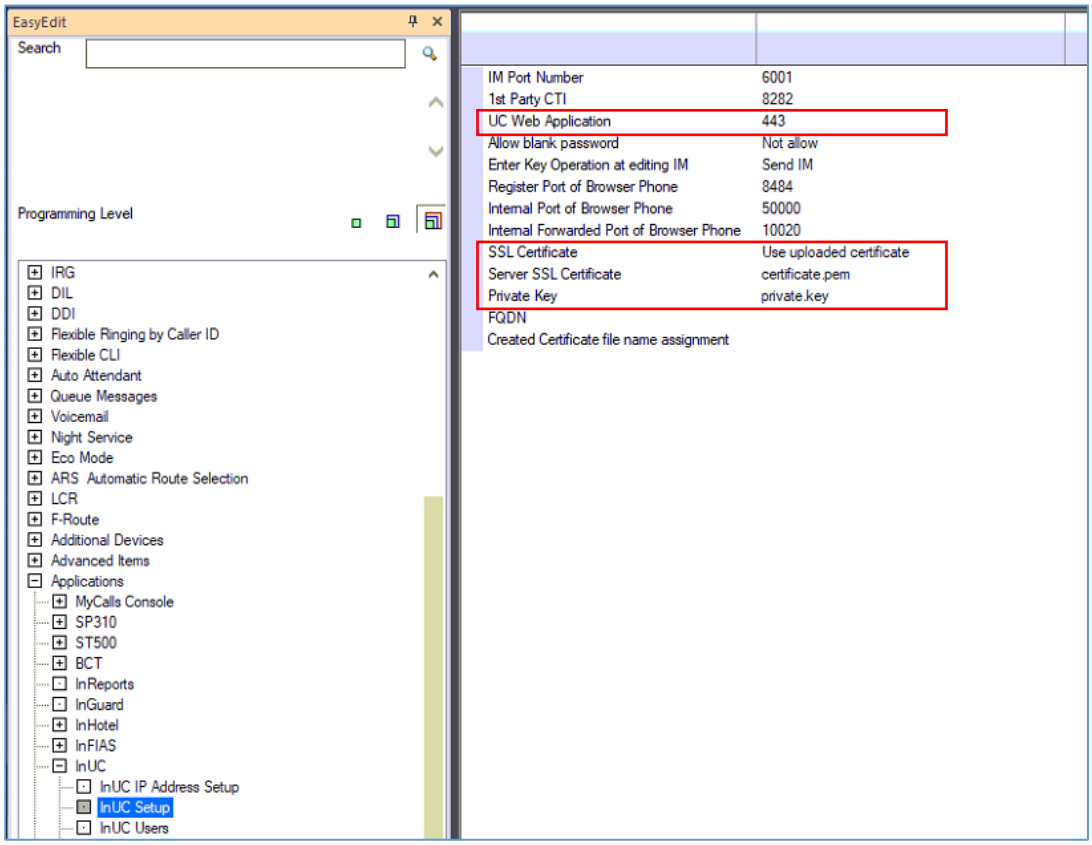
Configuring the SV9100 for TLS

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.



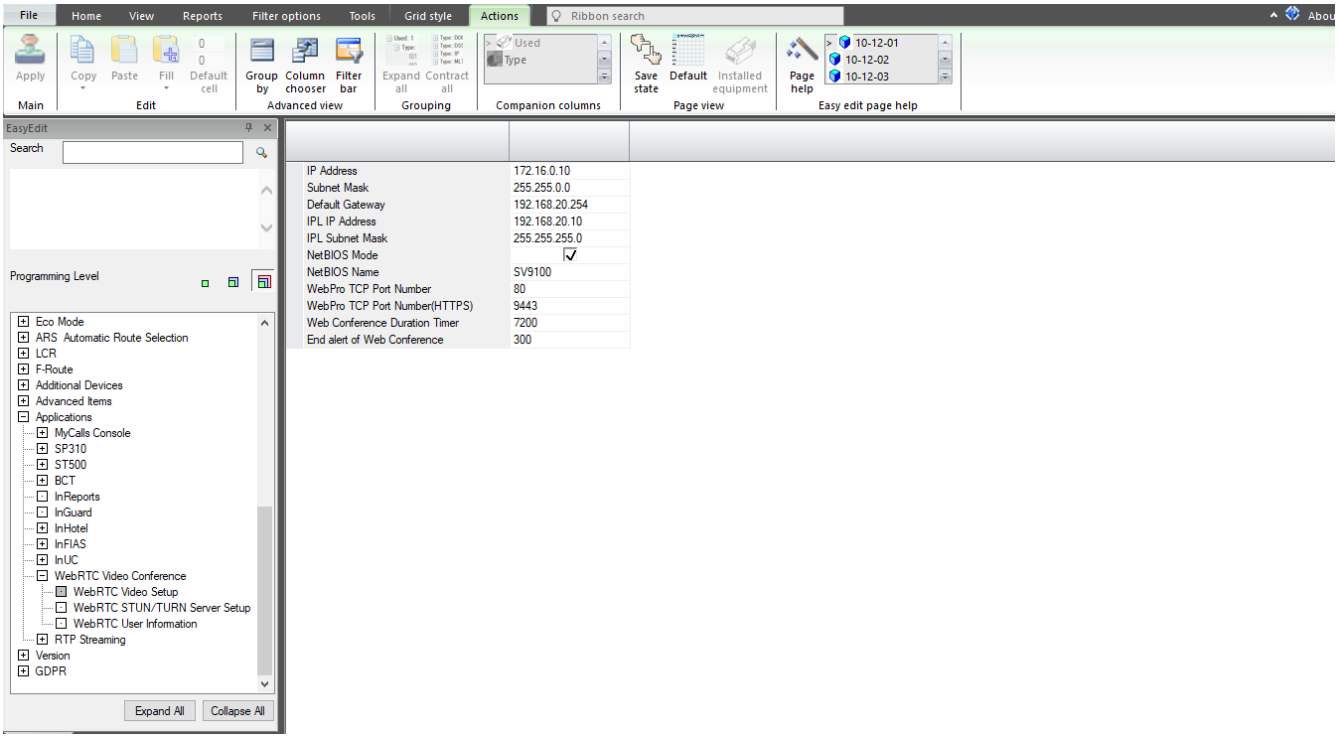
WebRTC IP and Port Configuration

From the **WebRTC Video Setup** screen you can check the IP configuration details of your SV9100 are correctly setup for use with WebRTC, as well as the ports being used.

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 > WebRTC Video Conference > WebRTC Video 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
10-62-01	NetBIOS Mode	0: Disabled 1: Enabled	Defines
10-62-02	NetBIOS Name	Up to 15 characters	Defines the NETBIOS name used by the system.
90-54-01	WebPro TCP Port Number		Defines the TCP port used for HTTP WebPro access.
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.
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.
20-64-02	End Alert of Web Conference	0 ~ 64800	The time for displaying an alert dialog message to all conference users before expiry of the Web Conference Duration Timer. (Default value is 300).

WebRTC STUN/TURN Server Setup

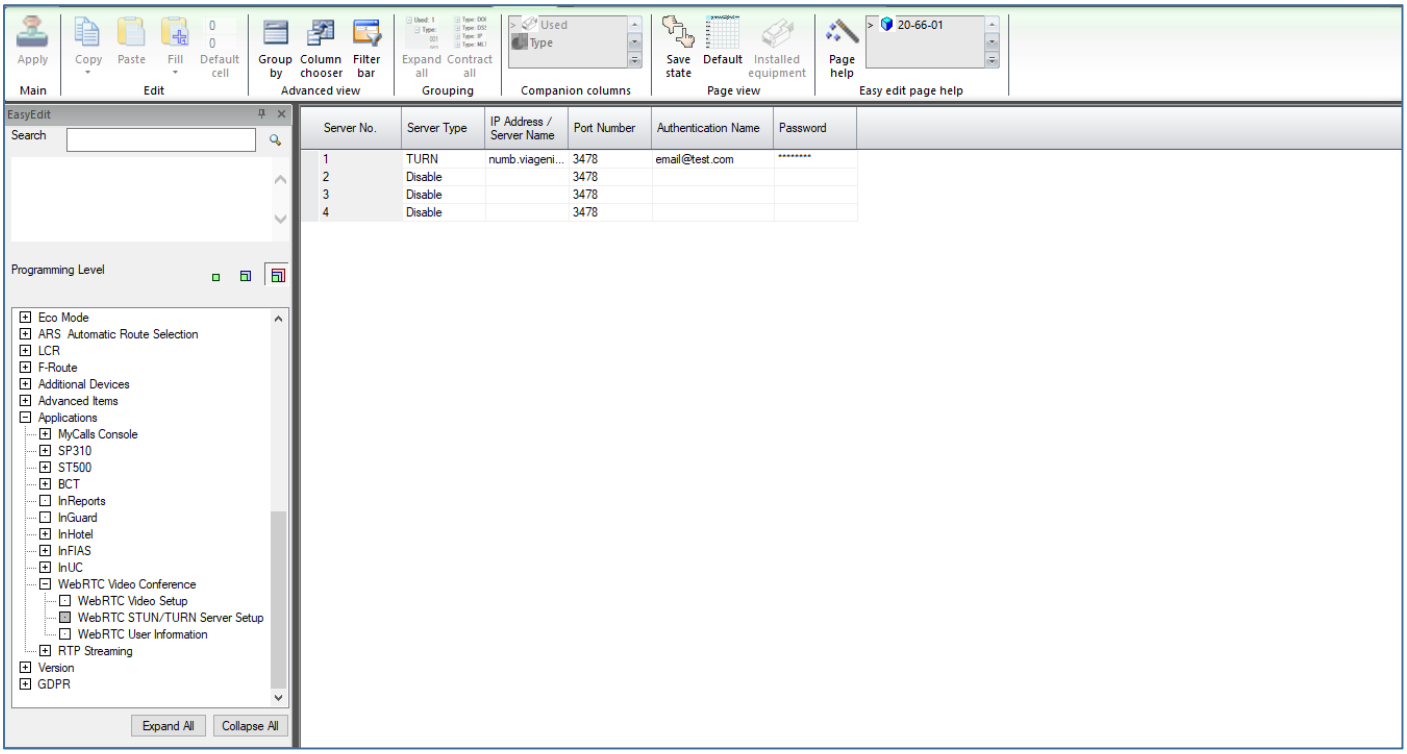
The **WebRTC STUN/TURN Server Setup** screen is used for configuring STUN/TURN server settings for allowing InUC clients to automatically learn their Public IP address details.

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 > WebRTC Video Conference > WebRTC STUN/TURN Server Setup



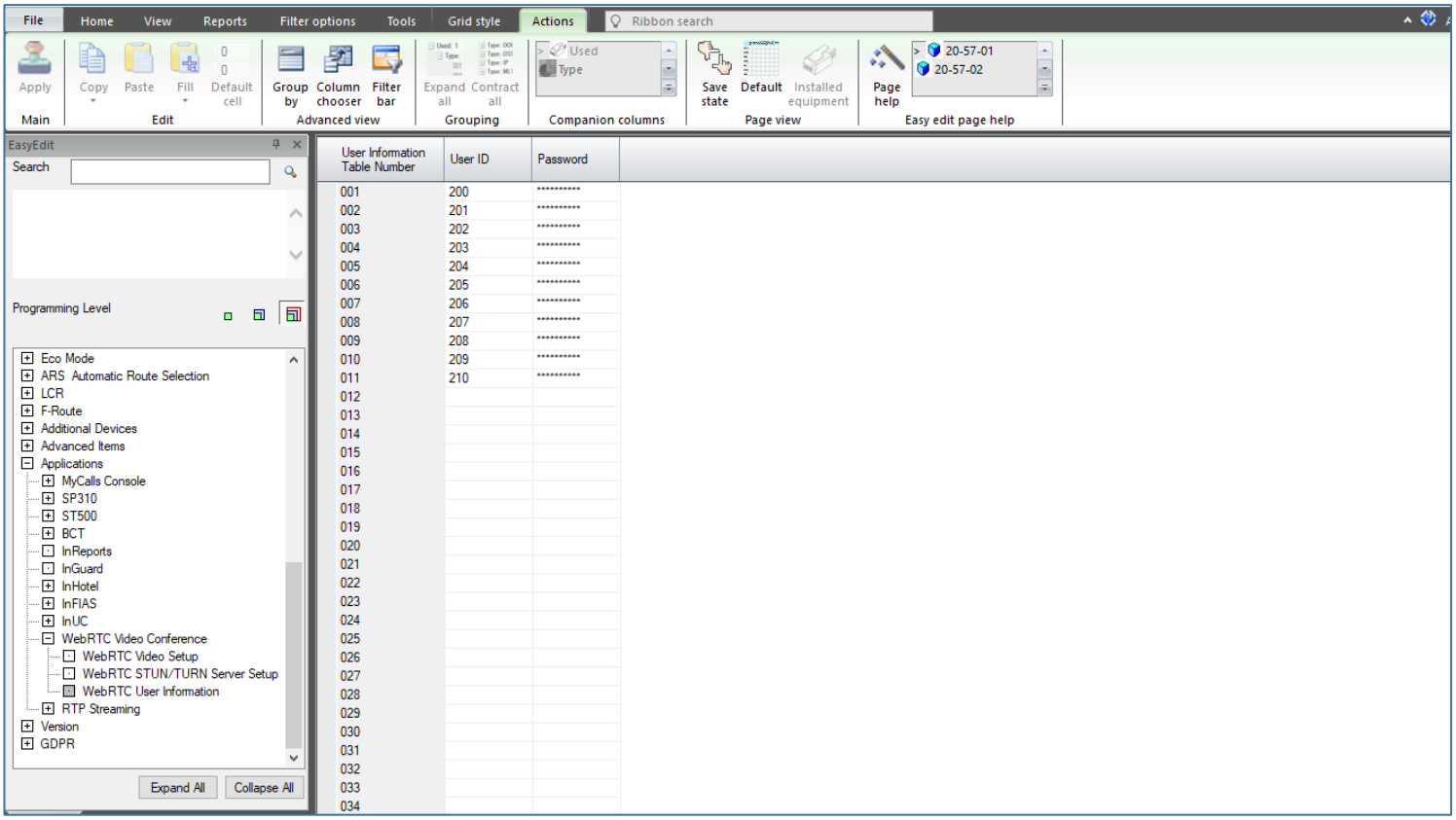
Program Data	Name	Input Data	Description	Default Value
20-66-01	Server Type	0: Disable 1: STUN Server 2: TURN Server	Enable the usage of STUN or TURN server settings.	0:Disable
20-66-02	IP Address / Server Name		Enter the IP address or FQDN of a valid STUN or TURN server.	Blank
20-66-03	Port Number		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

WebRTC User Configuration

Those users who have the ability to create video conferences must be defined in the system.

Here their User ID and Password can be assigned.

- Easy Edit > Applications > WebRTC Video Conference > WebRTC User Information



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. Must be complex.	Up to 16 characters.	Blank

Troubleshooting

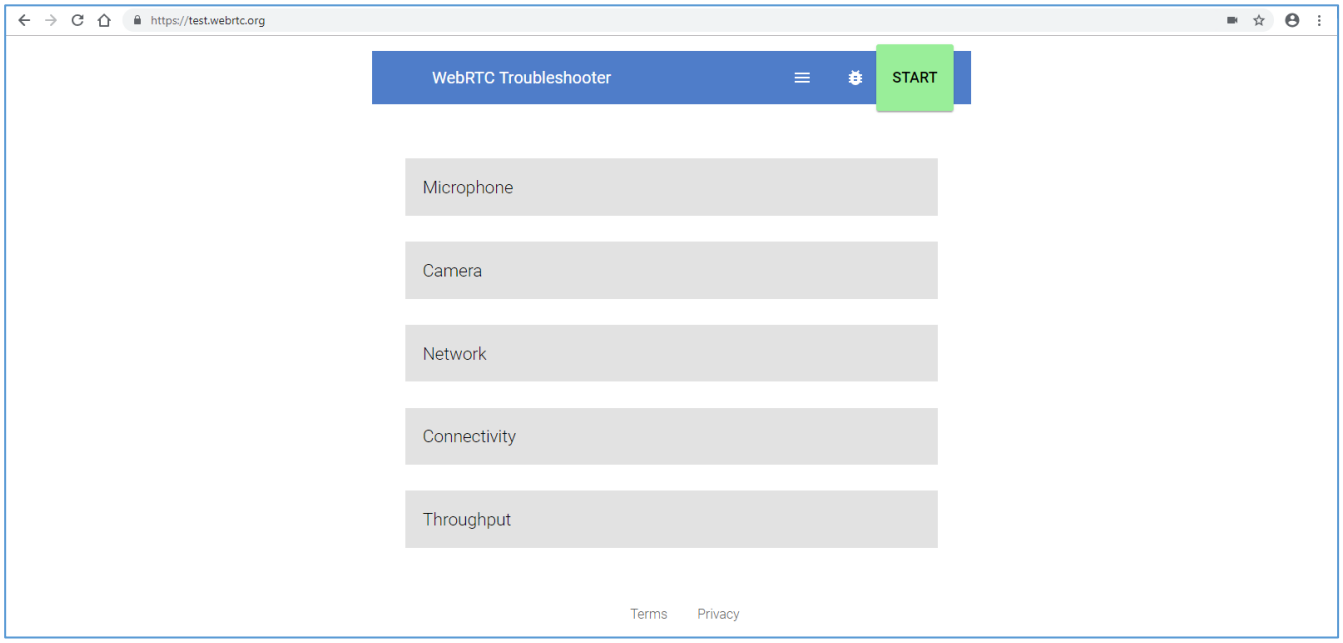
The Conference InScheduler App warning/error pop ups list.

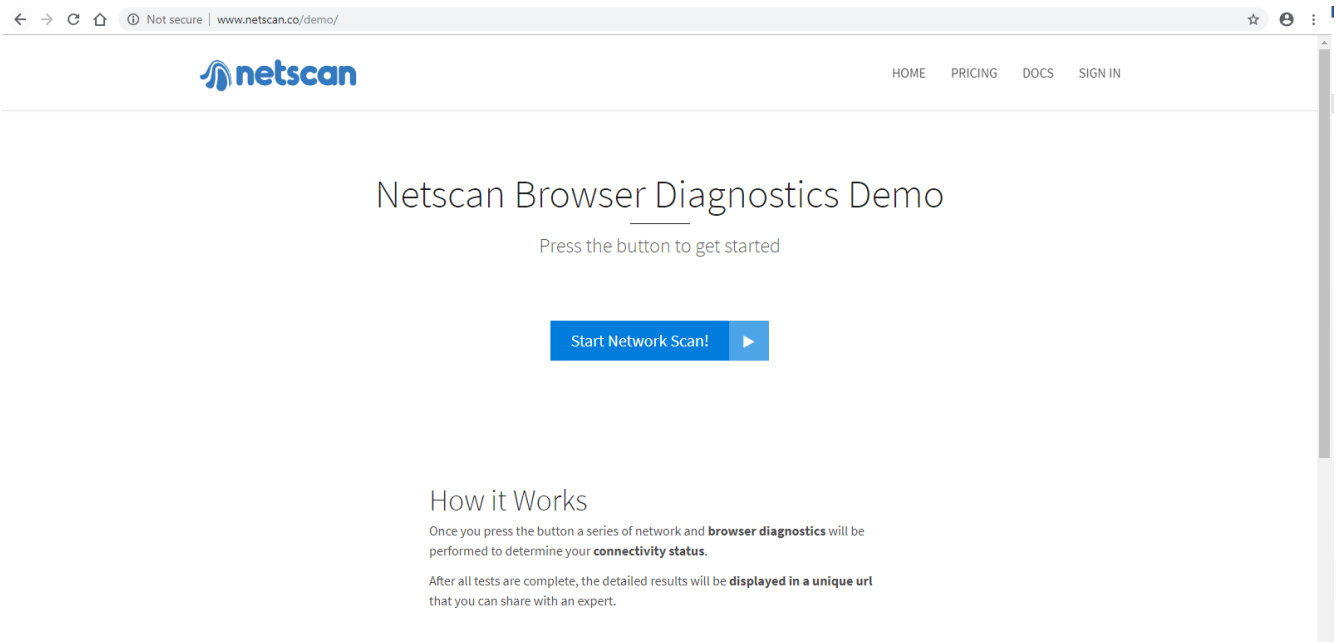
Error Pop up	Reason/Check
No Remote Conference rooms available.	There are no Remote Conference licenses in the system.
No Remote Conference Pilot numbers set.	The Remote Pilot numbers in the PRG 11-19-01 for the ports.
Username / Password mismatch.	Username and password do not match as programmed in the system.
Password must be 4 digits only.	The password must be 4 digits.
The conference duration must be 15 minutes minimum.	
The date and time needs to be from today or later.	
No Conferences are set for Schedule.	When any of the conference ports are not set to schedule.
Error in Scheduling. Please schedule in another time.	When CPU returns a write error, or not able to reach CPU.

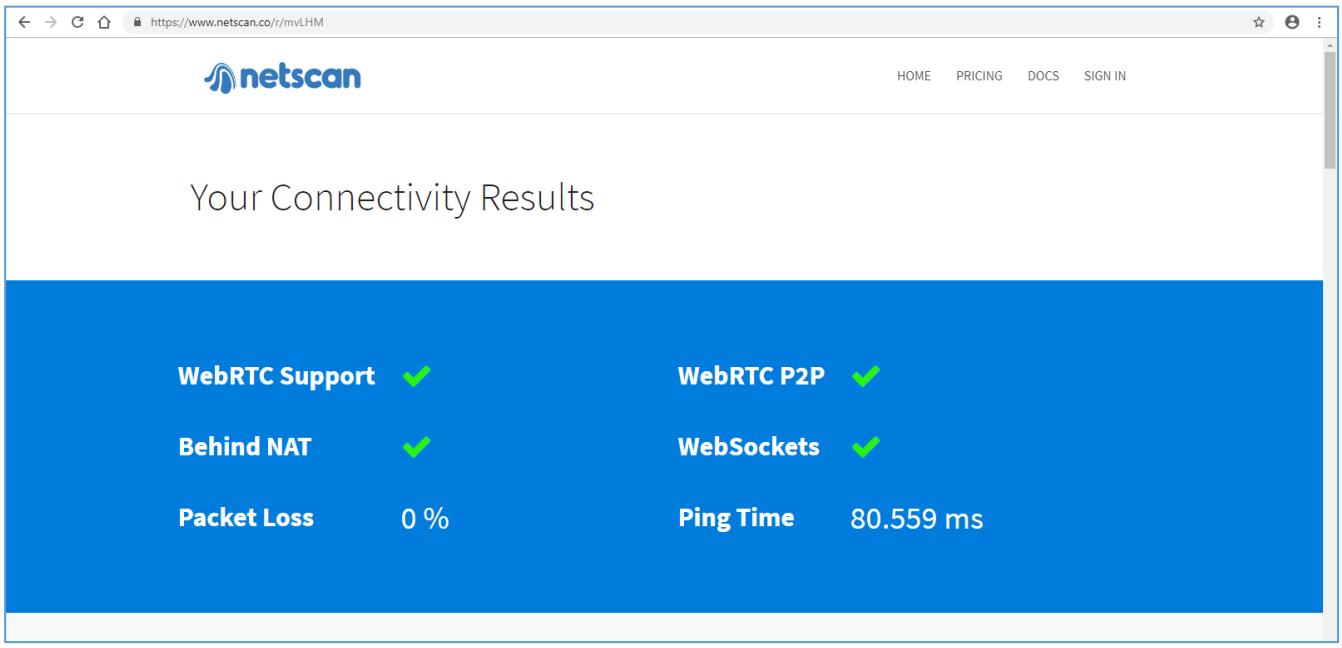
Depending on the network environment, you may have audio/video issues when trying to use the WebRTC video conference feature.

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

- Backup and Restore of scheduled data is NOT supported.
- InScheduler is not currently supported on the SL2100.
- InScheduler is not supported on the SV9100 CP10.
- https:// is not supported by the LUA manager and the LUA applications.
- There will be no user admission control based on host or participant.
- There will be no active user indication.
- The InScheduler application will not be active UI – meaning real time information during a conference is not shown.