

Thank you for your order for BT's One Voice SIP trunk UK. This Configuration document is provided as a source of guidance for the purpose of ensuring optimum performance when connecting the customer's CPE to the One Voice SIP service. This document and its contents are provided in confidence solely to enable the customer and their PBX maintainer to configure the CPE appropriately. Under no circumstances is this document or its contents to be shared with third parties.



Configuration Details to connect BT One Voice SIP trunk UK to – Audiocodes Mediant x000 (MxK) for MS Lync and TDM switches

Confidentiality Statement

All information contained in this Document is provided in confidence for the sole purpose set out within the objectives and scope of this document, and shall not be published or disclosed wholly or in part to any other party without BT's prior permission in writing, and shall be held in safe custody. These obligations shall not apply to information that is published or becomes known legitimately from some source other than BT.

All transactions are subject to the appropriate BT Standard Terms and Conditions.

Copyright

© British Telecommunications plc 2009
Registered office: 81 Newgate Street, London EC1A 7AJ

Contents	Page
1 Document Information	5
1.1 Specific	5
1.2 Author	5
1.3 Reviewers	5
1.4 Document History	5
2 Assumptions and Risk	7
3 Basic deployment	8
3.1 Deployment Steps	8
3.2 Checklist	8
3.3 Unpacking and mounting	9
3.4 Cabling	9
4 Basic Installation	10
4.1 Access to the gateway	11
5 Configuration using EWS	12
5.1 Manual Configuration.	12
5.2 Set Network settings	15
5.3 Loading a Scenario	16
6 Verify deployment.	18
6.1 PRI Status	18
6.2 Trunk Status	18
7 Certificates	20
7.1 Load Certificates for secure working.	20
Self Signed Certificate – Media Gateway	21
Self Signed Certificate – Certification Authority	22
Import Self Signed and CA Certificate – media gateway	24
8 Customer Configuration Euro ISDN	25
Routing and Manipulation Information	27

9	Customer Configuration QSIG	30
9.1	Advanced Network Settings	30
	Routing and Manipulation Information	32
10	Security	35
	Change gateway default password.	35
11	Backup of Configuration and Restore	36
12	Upgrade	37
13	References	39
14	Glossary	40
15	Appendix A – BootP Configuration.	41
15.1	Installing Boot P	41
15.2	Configuring BootP	42
16	Appendix B – Support Numbers.	46

1 Document Information

1.1 Specific

NAME	ROLE
Design Pattern Type	Module
ACF Number	ACT 32507
Line of Business Owner	BTID
Product Family	ECEP CPE
Parent ACT	None
Child ACT	None

1.2 Author

NAME	ROLE	CONTACT NUMBER
Steve Wade	Solutions Designer	441277328959 Steve.d.wade@bt.com

1.3 Reviewers

NAME	ROLE	CONTACT NUMBER
Roy D'Sa	Solutions Designer	+44 1277 328749 roy.dsa@bt.com
	Solutions Designer	Your Number Here Your Email Here

1.4 Document History

NAME	Changes	Version
Original	Original	Issue 1.0
	Layout changes and minor corrections.	Issue 1.1

*Note, the first iteration of a document should be Draft 1.0
Minor changes made to the document should increment by 0.1 (Dot revision i.e. 1.1 becomes 1.2).
Major changes to the document should result in an uplift of the whole figure by 1 (i.e. 1.5 becomes 2)
No documentation should reach its customer before peer review changes the document to an Issued status.*

Executive summary

This configuration guide describes how to deploy AudioCodes media gateways.

The document will show to configure and apply a basic configuration to the gateway. The use of templates and prepared files to standardise deployment and reduce install time is used.

The document will also describe a process to be used in the replacement of a faulty media gateway.

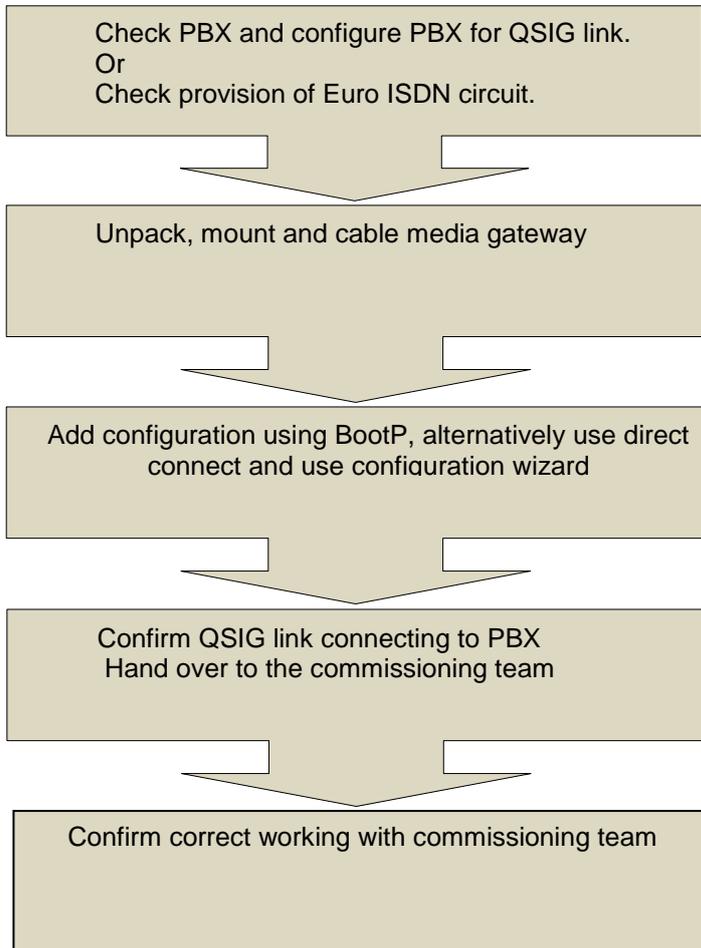
2 Assumptions and Risk

The AudioCodes media gateway is supported as part of the process for providing voice for Microsoft Lync. This is the new name assigned to the third generation of Microsoft Office Communication server. This process can also be used for Microsoft Exchange Unified Messaging and Microsoft Office Communication server.

The deployment of the gateway and connection to a Private Branch Exchange (PBX) or Public Switched Telephone Network (PSTN) should be carried out by an engineer familiar with the platform being connected to for the trunk service.

3 Basic deployment

3.1 Deployment Steps



3.2 Checklist

The following are needed before commencing installation

Item	Check
QSIG card for PBX or EuroISDN trunk	
RJ48C Cable from PBX to run to gateway or tool to make up.	
RJ45 crossover cable.	
PBX configuration information	
IP address and FQDN for media gateway and Microsoft endpoint	
Copy of media gateway files from Livelink. http://livelink.intra.bt.com/livelink/livelink.exe?func=ll&objId=121134726&objAction=browse&sort=name	

3.3 Unpacking and mounting

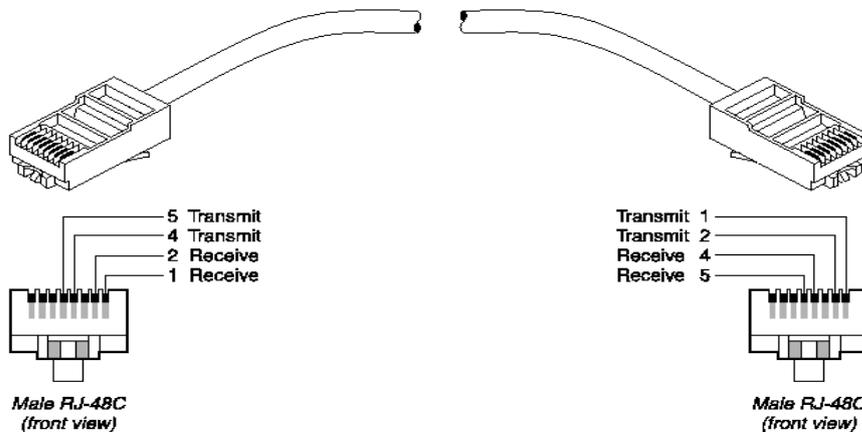
- Open the carton and remove the packaging materials.
- Remove the media gateway.
- Check for any signs of damage during transit.
- Retain any documentation and CD's.
- Remove the two mounting brackets and attach to the media gateway.
- Mount the media gateway in a 19" rack. It is recommended that a shelf or supporting bracket should be used.



3.4 Cabling

The media gateway has two standard RJ45 Ethernet ports for connection to the customer's network. These two ports are twinned; use both ports to provide resilience. The PRI link to the media gateway should be cabled as shown.

- Permanently connect the device to a suitable earth with the protective earth screw on the rear connector panel, using 14-16 AWG wire.
- Connect the E1/T1 trunk interfaces. This is presented as an RJ48C. This pin out is shown.



RJ48 C Pin-Out

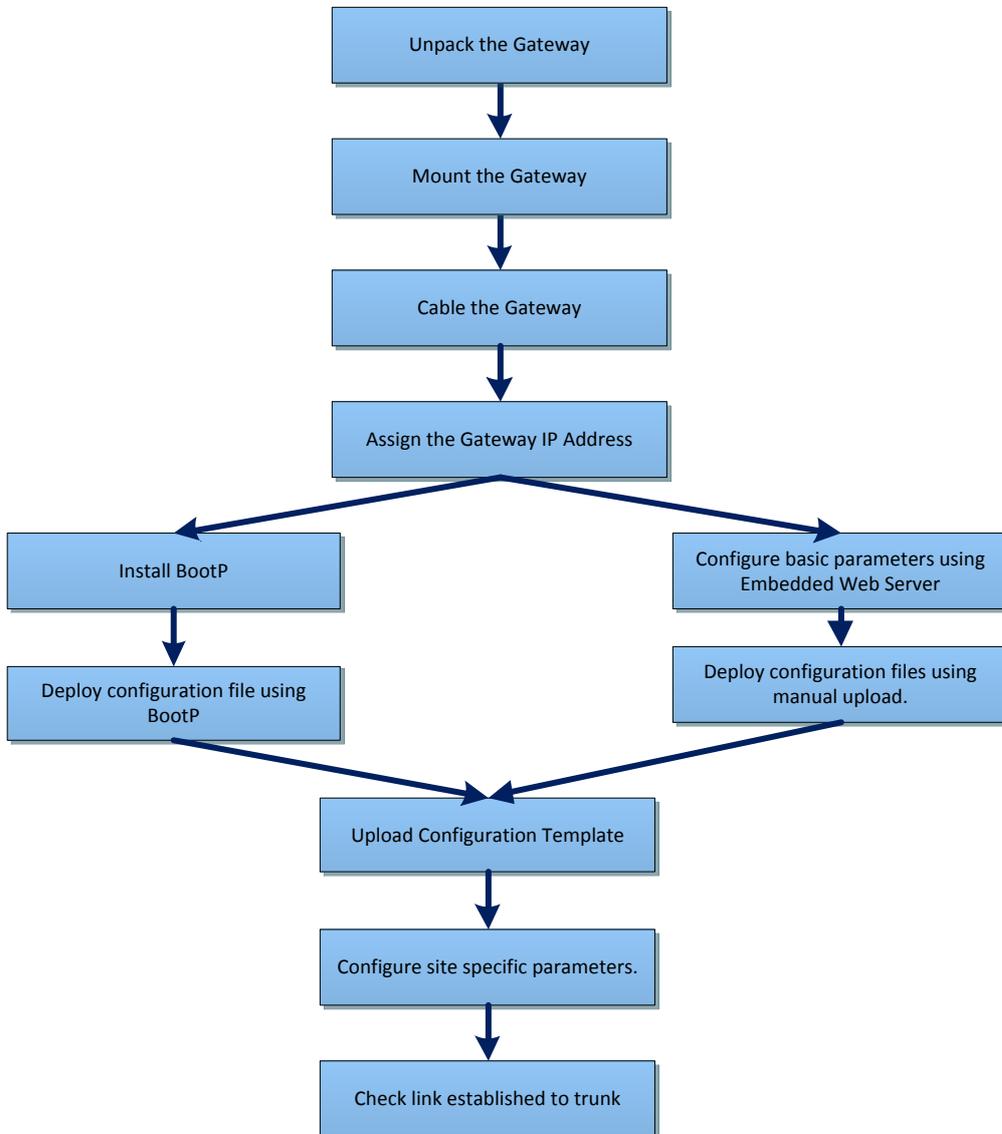
Pair	Signal	Male RJ48C Local	Male RJ48C Remote
1	Receive	2	5
1	Receive	1	4
2	Transmit	5	2
2	Transmit	4	1

The cabling and of presentation of the PRI interface is the responsibility of the PBX or PSTN provider and is not included in the scope of this document.

- Install the Ethernet connection This connection is RJ45C
- Connect the power supply.

4 Basic Installation

This chart indicates the steps required to deploy an AudioCodes media gateway.



4.1 Access to the gateway

The AudioCodes media gateway has an embedded web server that is used to manually assign an IP address to the device. Connect to the media gateway from a device with a suitable network connection or directly with a crossover cable.

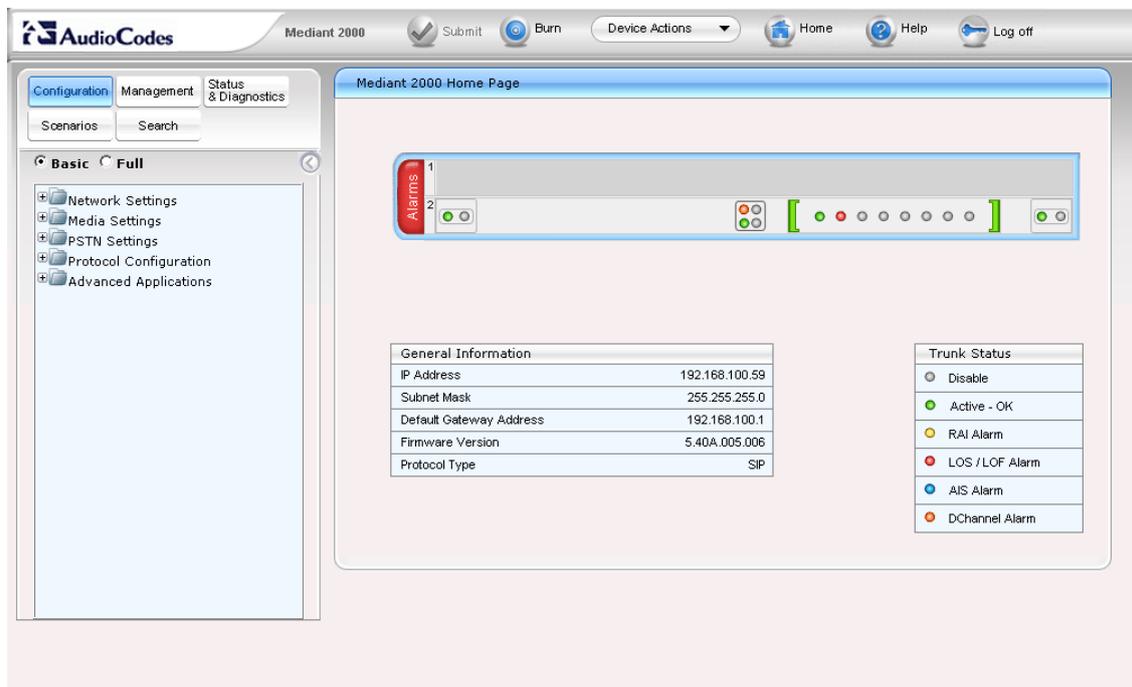
The media gateway is factory shipped with a pre allocated IP address. Assign an IP address to the device being used to connect to the media gateway. It is recommended to use 10.1.10.11/16 to initially access the media gateway.

Default IP Address	10.1.10.10 Subnet 255.255.0.0
Default Login	Admin
Default Password	Admin

Enter the default IP address into a web browser window running a minimum of Internet Explorer 6.0 or Mozilla Firefox 2.0. Enter the user name and default passwords these are **case sensitive** and click okay.



The home page icon is shown. The device can be navigated using the menus on the left hand side of the device.



5 Configuration using EWS

Use this process when BootP cannot to be used.

5.1 Manual Configuration.

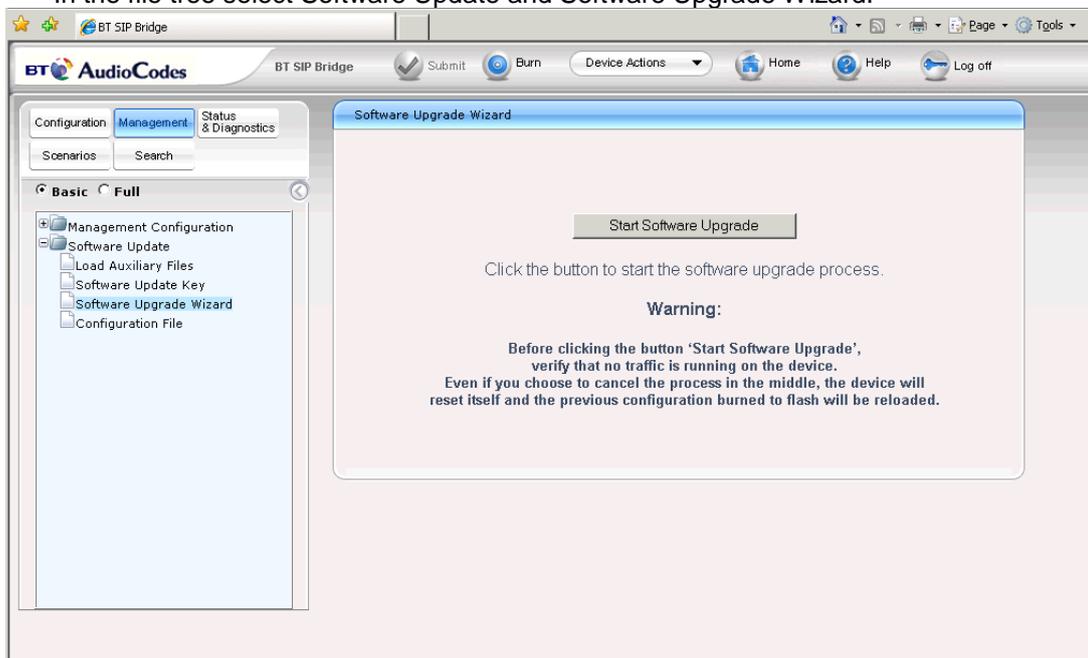
The media gateway is configured by uploading a configuration file containing most of the required settings. All the required files including firmware are from Livelink

<http://livelink.intra.bt.com/livelink/livelink.exe?func=ll&objId=121134726&objAction=browse&sort=name>

From the zip file extract the contents to a local folder. The files required are the board.ini, TP1610_SIP_5.40.xx.xx.cmp, Uk, dat and Uk .ini

Manually connect to the device using the procedure described in [section 3.1](#).

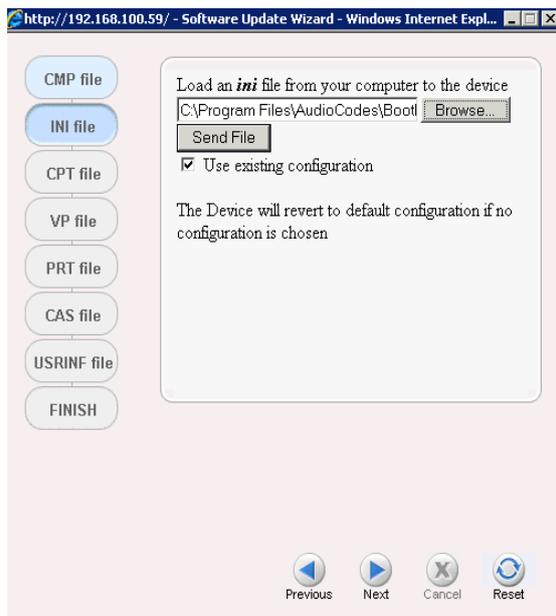
- In the top level menu on the left hand side select Management
- In the file tree select Software Update and Software Upgrade Wizard.



- In the Software Upgrade Wizard select Start Software Upgrade. The upgrade window opens.



- In the Software Update Wizard window select cmp file.
- Browse to the location where the downloaded files are located and select the TP1610 file.
- Select send file. The window updates as the file is loaded. A confirmation window is displayed when loaded.
- Select next.



- In the Software Update Wizard select ini file.
- Browse to the board.ini file and select send file.
- Once the file is uploaded select next.

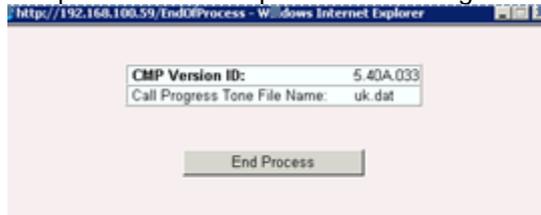


- In the Software Update Wizard select cpt.file
- Browse to the folder and select the uk.dat file.
- Click to send the file. The file is uploaded.
- Select next for VP file
- Select next for PRT file.
- Select next for the CAS file.
- Select next for USRINF file.
- Select FINISH



- Select the reset button to reset the gateway.

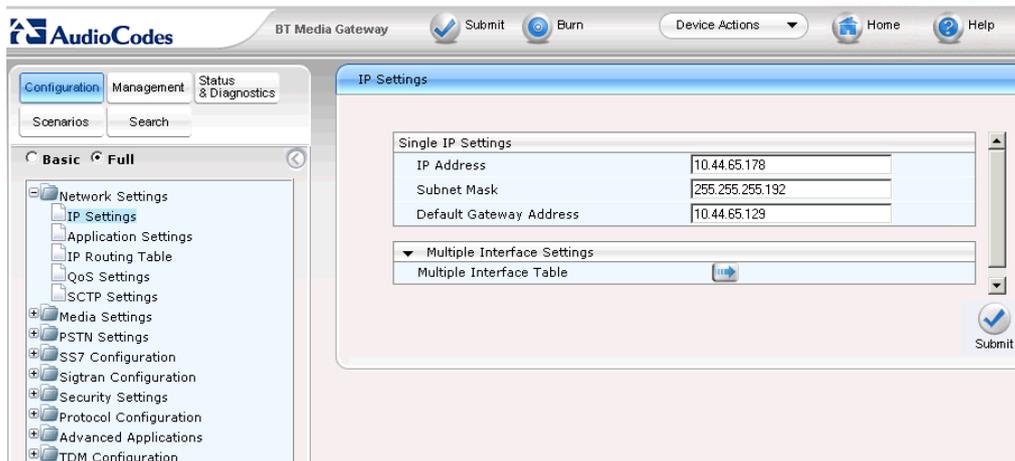
The gateway loads the files and if necessary upgrades the firmware this can take several minutes to complete. When complete the following notification window is shown.



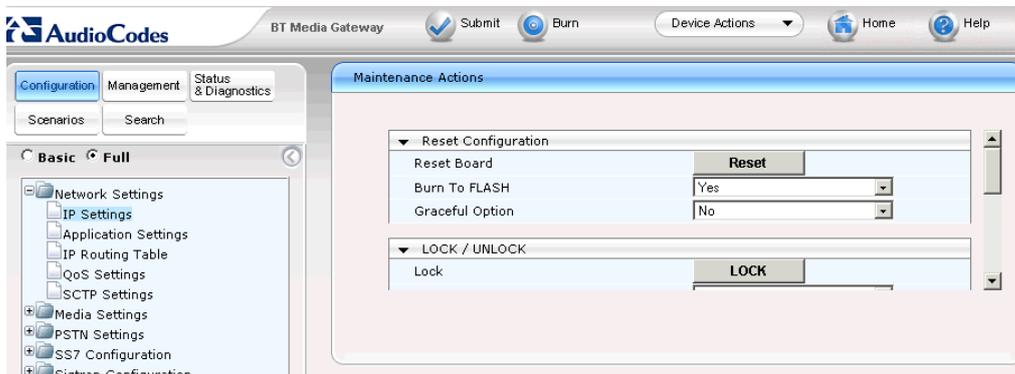
5.2 Set Network settings

Assign the correct IP address and the address for the media gateway.

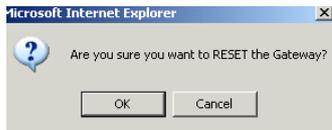
- In the top level menu on the left hand side select Configuration.
- In the file tree select Network Settings and IP Settings.
- Under Single IP configuration enter the Mediant 2000 IP address, subnet and gateway.
- Select submit.



- In the top title bar select Burn to save the configuration.
- In the top title bar select the drop down icon to the right of Device Actions and select Reset.



- In the Maintenance Action window select Reset.

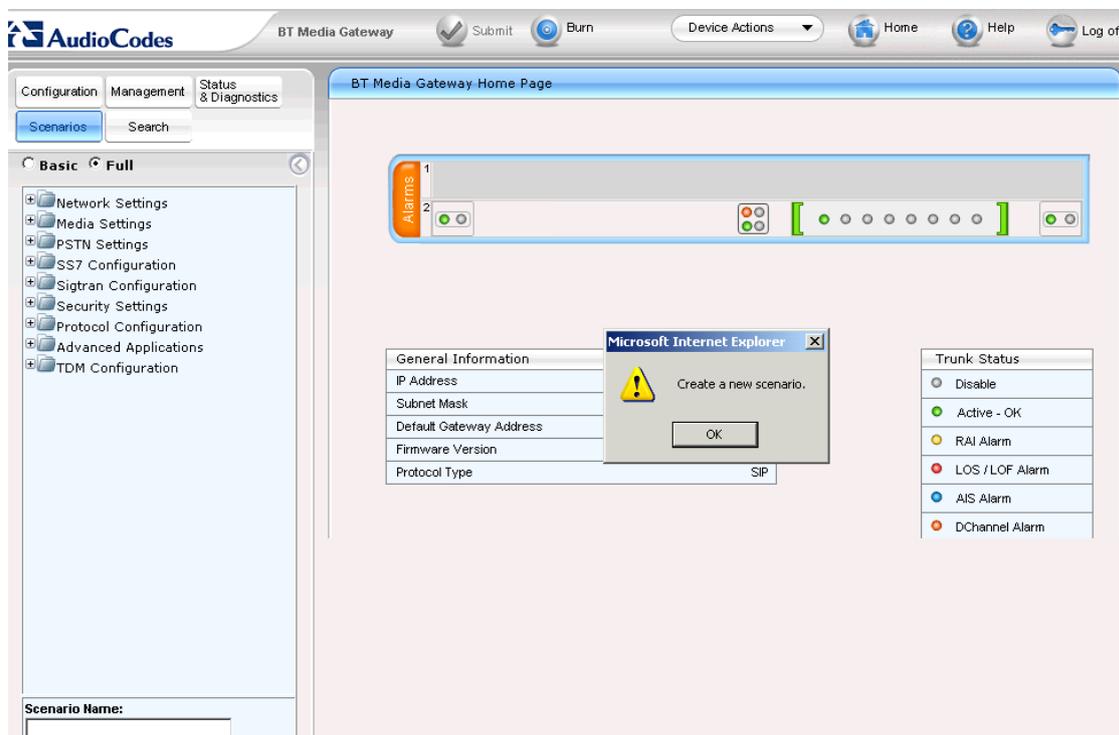


- In the confirmation window Select OK to reset the media gateway. Remember to switch to the new network settings to connect to the device.

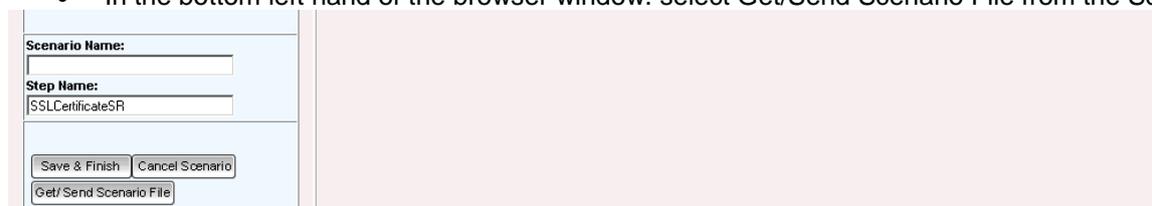
5.3 Loading a Scenario

The scenario is contained within the group of files downloaded from:

<http://livelink.intra.bt.com/livelink/livelink.exe?func=ll&objId=121134726&objAction=browse&sort=name>



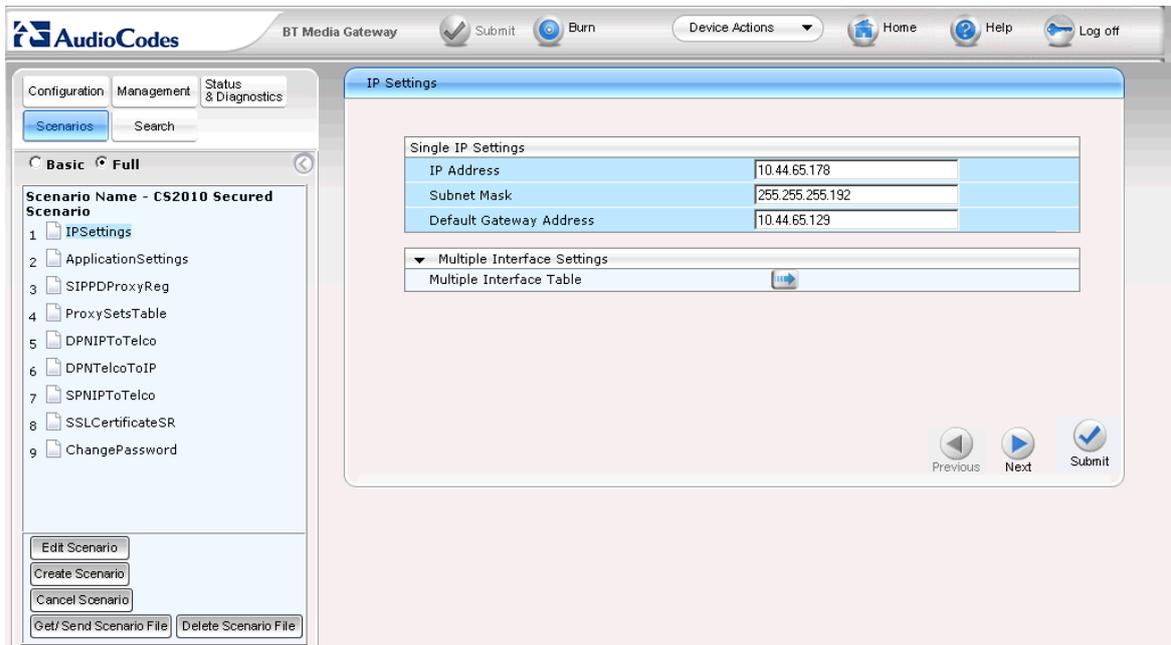
- In the top left hand menu select scenarios.
- Select OK to create a new session.
- In the bottom left hand of the browser window. select Get/Send Scenario File from the Scenario



- In the Send Scenario file from your Computer to the Device window select Browse. Browse to the Secured Scenario.dat file which is contained within the folder of documents obtained from Livelink.
- Select Send File.
- Confirmation is given to show that the file has loaded correctly.
- In the top level menu on the left hand side select Scenarios for a second time, there is a prompt that a scenario has been loaded.



- The Scenario Name shows the Secured Scenario. This contains the key elements required to configure the media gateway.



- Proceed to [Verify Deployment](#)

6 Verify deployment.

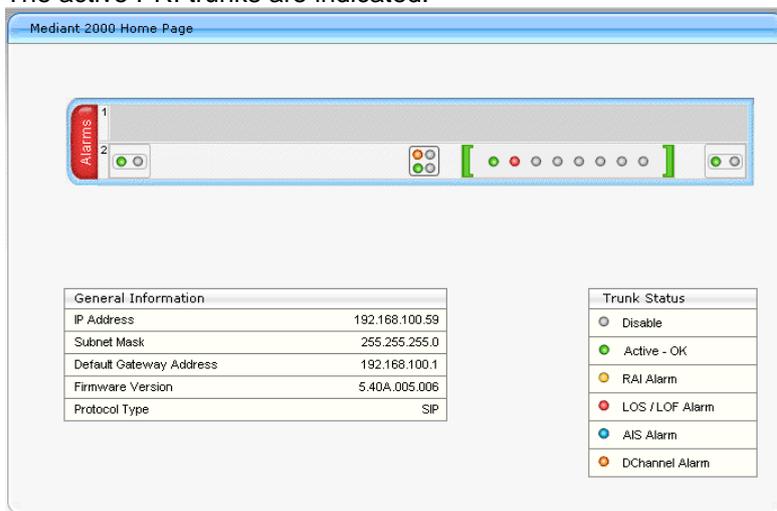
When an AudioCodes media gateway is deployed as part of a Microsoft managed solution. The onsite deployment must load the configuration files and establish the connection with the QSIG or Euro ISDN trunk. The commissioning team will complete the customer specific configuration required for the solution. Initial testing consists of checking that the PRI link is established, placing a call towards the gateway and checking for call presentation using Message Log.

6.1 PRI Status

If the link is configured correctly on the PBX or PSTN the active QSIG trunk will show an active icon.

- In the title menu at the top of the page select the home icon,

The active PRI trunks are indicated.

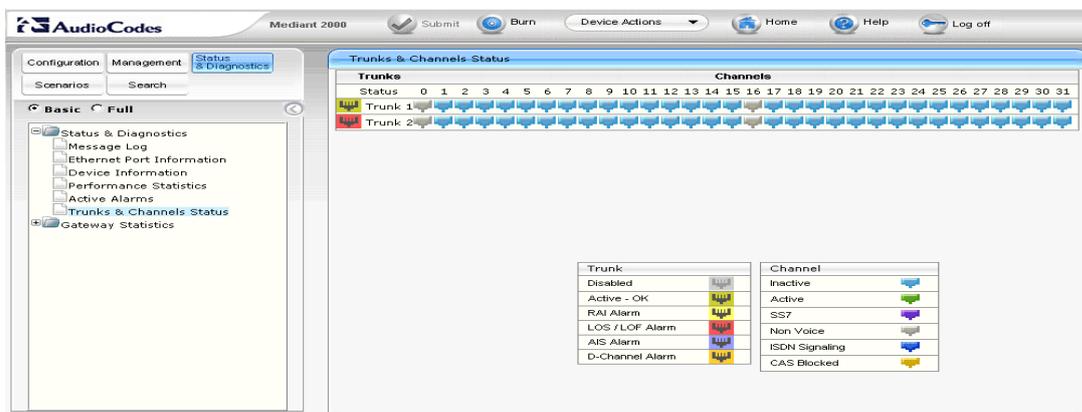


6.2 Trunk Status

To check the status of individual channels,

- In the top left hand menu select Status and Diagnostics.
- In the left hand tree menu expand Status and Diagnostic, Trunk Channel Stats

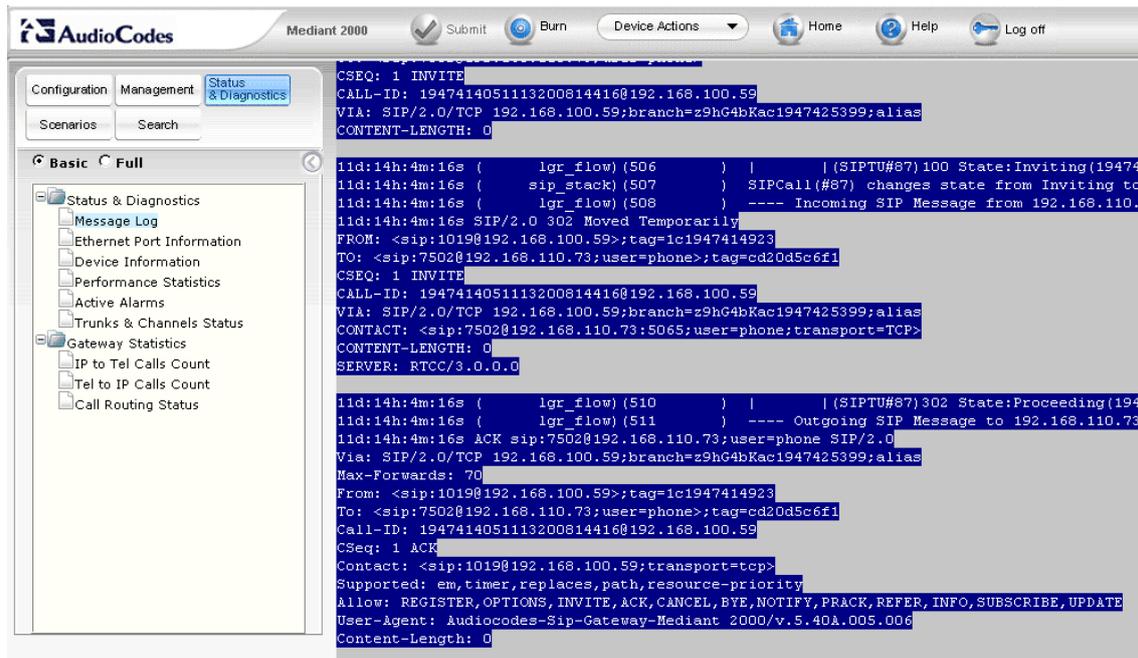
The channel status for the trunks is shown in the Trunk and Channel Status window.



Call Log

The media gateway has an in built log file for capturing real time call logs available. This can be used for problem investigation.

- From the top of the left hand menu select Status and Diagnostics.
- In the left hand tree select Status and Diagnostic, Message Log.
- Any calls through the gateway are shown in real time.
- Cut and paste information from this window to notepad to help analysis.
- Place a call over the QSIG/EuroISDN link to the gateway and check for presentation.



For more detailed tracing Syslog can be used refer to the AudioCodes documentation for further information (copy on CD).

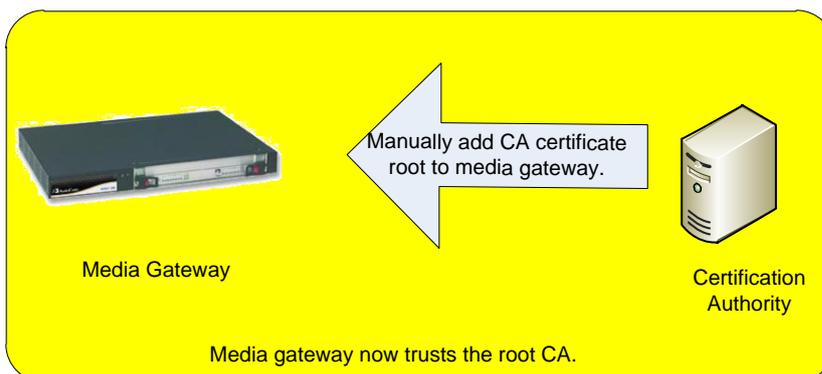
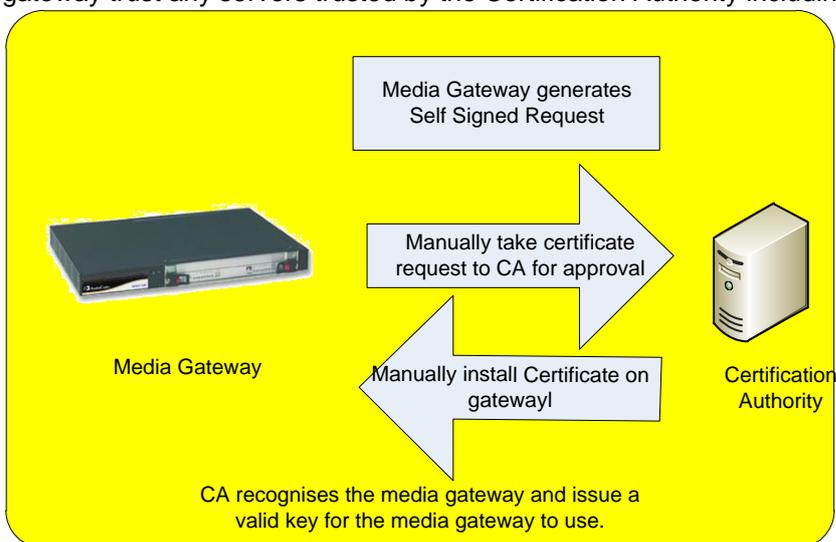
7 Certificates

7.1 Load Certificates for secure working.

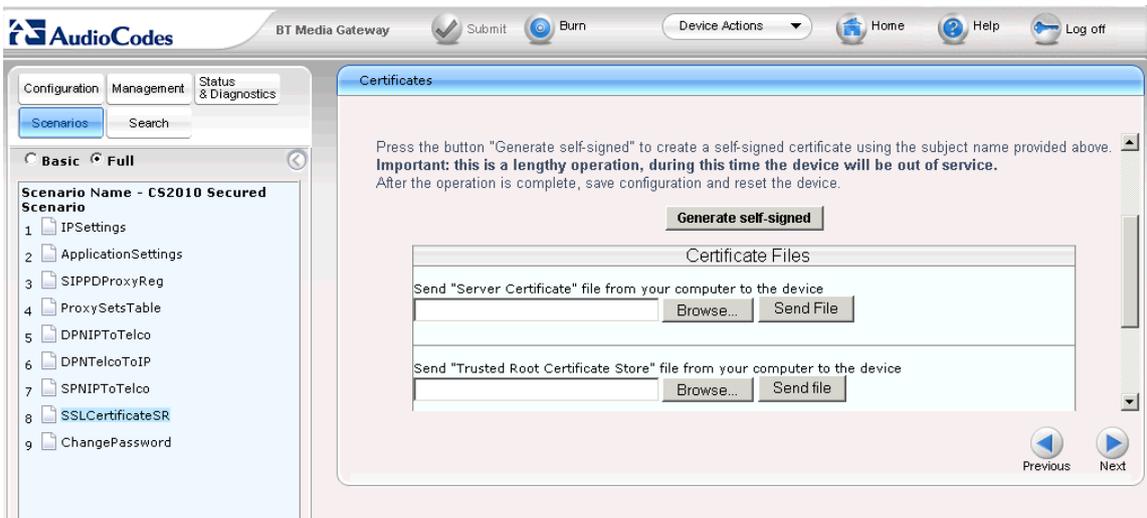
The media gateway needs to be trusted by Microsoft Lync. The gateway name and identity is exchanged with the Certification Authority. During the installation the Microsoft Lync servers also are secured by certificates with the Certification Authority. Both devices have valid certificates issued from the CA and allow secure communication between them.

The process is in a number of stages. The Media gateway creates a self-signed request. This is manually taken to the Certification Authority. The self-signed request is validated and a key is generated to be loaded onto the media gateway.

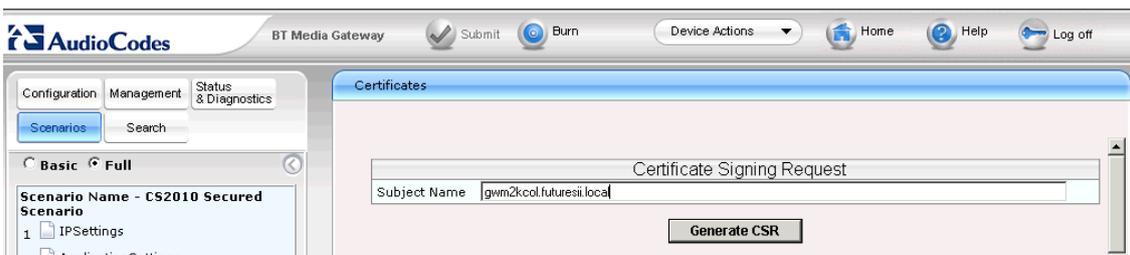
The media gateway needs the Root certificate from the Certification Authority loaded. This lets the media gateway trust any servers trusted by the Certification Authority including Microsoft Lync.



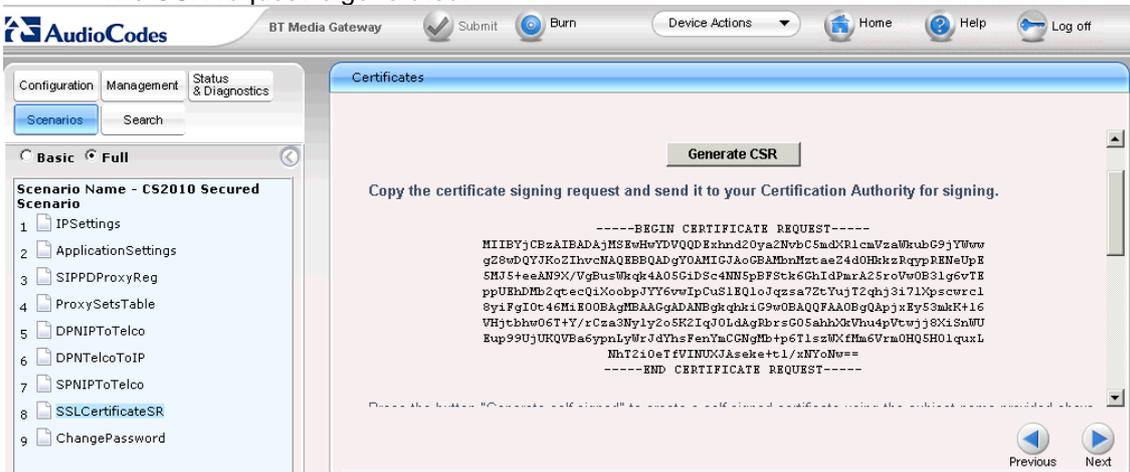
Self Signed Certificate – Media Gateway



- In the Subject Name field enter the name of the media gateway.
- In the Certificates window select Generate CSR



- The CSR request is generated.



- Select all the text from the key generated. Copy the text and save to a text editor such as notepad.

```

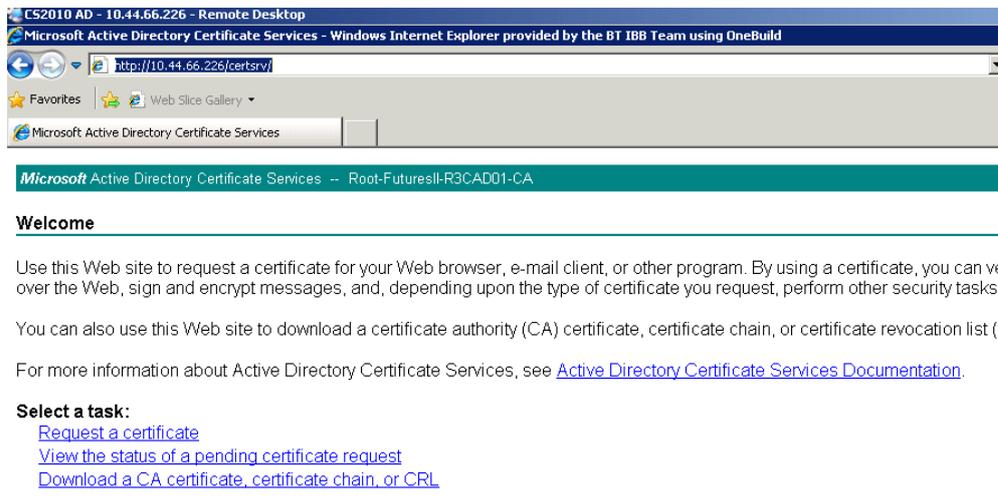
Untitled - Notepad
File Edit Format View Help
-----BEGIN CERTIFICATE REQUEST-----
MIIBYjCBZAIwBADAjMSwHwYDVQDEhhnd20ya2NvbC5mdXR1cmVzawkuubG9jYwVw
g28wDQYJKoZIhvcNAQEBBQADgTOAMIGJAoGBAMbnMzt ae24d0HkzRqypRINEUpE
SHJ5+eeAN9X/VgBusWkq4A05G1Ds4NN5pBFstk6ChIdParA25roVw0B31g6vTE
ppUeHDb2qt ecQ1XoobpJY6vWlPcUs1RQ1oJqzsa7ZcTujT2ghj3171XpsCwrc1
8yiFgT0c4CH8E00BAGMBAAgADANBqkqhk1G9w0BAQFAA0B9QApjxey53mkK+16
VHjtbhw06T+Y/rcza3nyly205k2IqJ0LdAgRbrsG05ahhxkVhu4pvtwj8X1SNWU
Eup99UjUKQVBA6ypnlywRjdyhsFenYmCGngmb+p6T1s2wxFMm6Vrm0HQ5H01quxL
Nht21oetFVINUXJAsake+t1/XNYONW==
-----END CERTIFICATE REQUEST-----
    
```

- Save the file. A manual process is required to load into the CA.

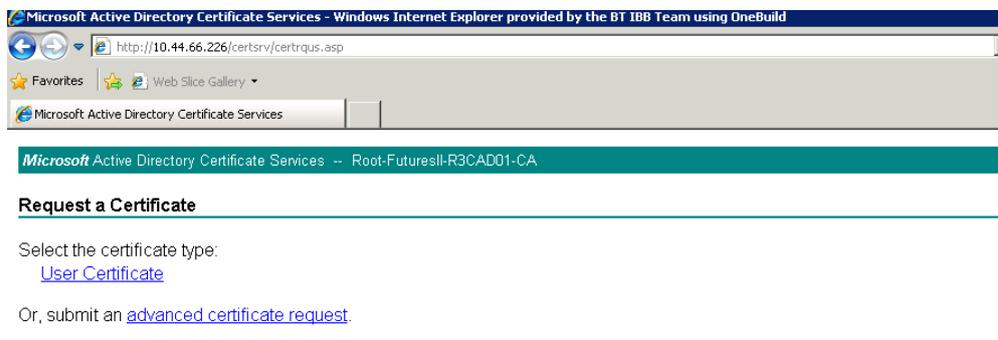
Self Signed Certificate – Certification Authority

This will need to be carried out by a person responsible for the CA.

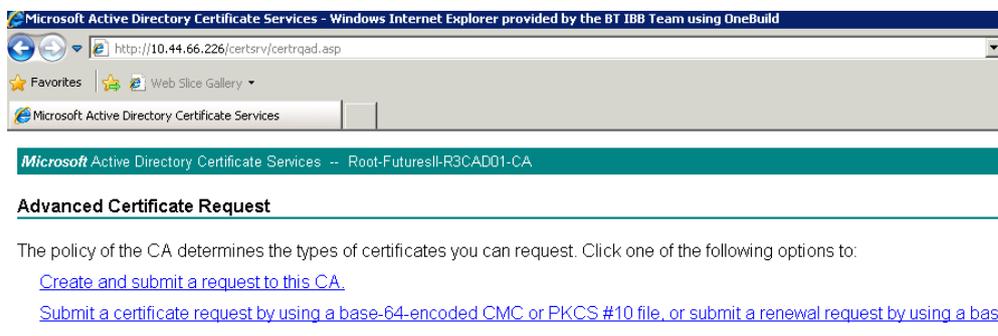
- Launch a web browser to connect to the CA and enter the correct credentials.
- From the Welcome window select Request a Certificate.



- From the Request a Certificate window select Advance certificate request.



- From the Advanced Certificate Request window select Submit a certificate request by using a base 64 encoded.



- Select Create and Submit a request to this CA.
- Copy the Certificate request from the gateway into the Base-64 file on the webpage.
- In the certificate template select Web
- Click submit.

Microsoft Active Directory Certificate Services -- Sub-FuturesII-R3CAD02-CA [Home](#)

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
5HO6fLMykyww/B06fzfG0s0iTABRO1USNrLhANOG  
6hP5C0G7v5xNyR1oSqOUQe72QryMfoSHtdmP7VeH  
d+FEGEwggmGRcZZCqQnBkj+NtJtvvq4=  
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

Additional Attributes:

Attributes:

[Submit >](#)

The certificate is generated and needs to be saved to subsequently install on the media gateway.

- From the Certificate Issued window chose to save as a Base 64 Encoded.
- Click the Download Certificate link.
- In the File Download –Security Warning window select Save
- In the Save As window assign a file name such as media gateway.cer cert.
- In the Save As Type leave unchanged as Security Certificate.

Microsoft Active Directory Certificate Services - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <http://10.44.66.227/certsrv/certifnsh.asp>

Microsoft Active Directory Certificate Services -- Sub-FuturesII-R3CAD02-CA

Certificate Issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded

 [Download certificate](#)
[Download certificate chain](#)

The CA certificate is also required to be downloaded and added to the media gateway.

Microsoft Active Directory Certificate Services -- Sub-FuturesII-R3CAD02-CA

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

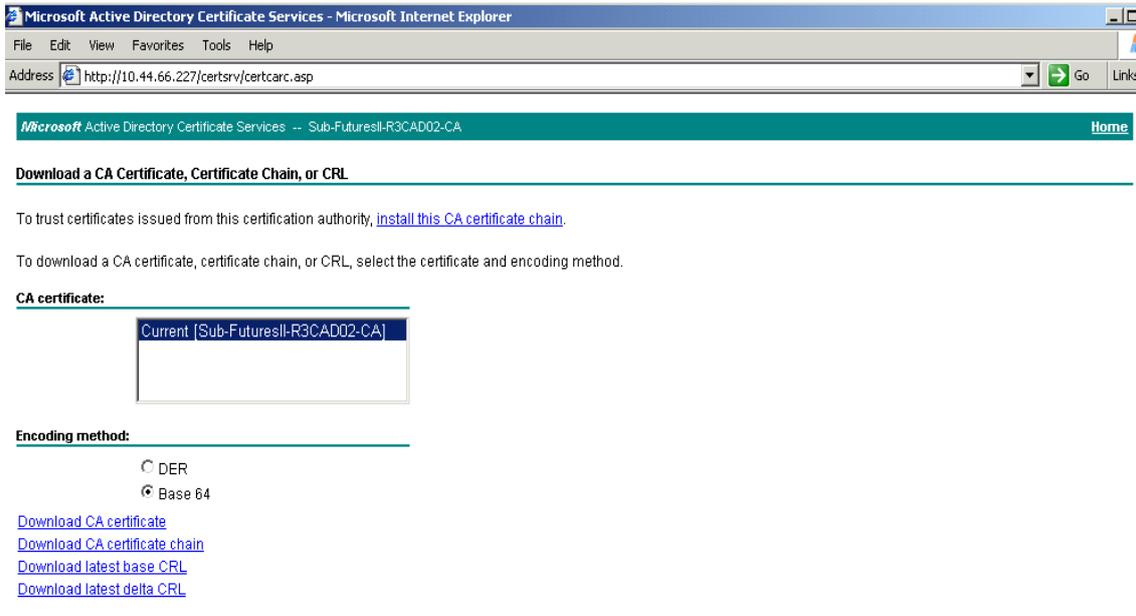
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

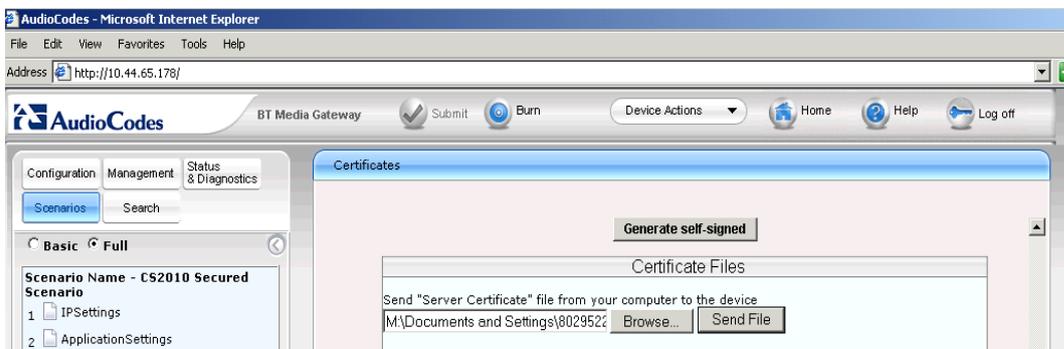
- Select the Download a CA Certificate, certificate chain or CRL.
- Select encoding method Base 64.
- In the Encoding Method select Base 64.
- In the Download a CA Certificate, Certificate Chain or CRL select download CA certificate.



- In the File Download – Security warning dialog box select Save.
- In the Save As window assign a file name such as certnew.cer.
- Manual move the certificate ready to import into the media gateway.

Import Self Signed and CA Certificate – media gateway

The self-signed certificate generated by the CA and CA Certificate both need to be imported into the media gateway.



- In the Certificates window of the media gateway.
- In the Send “Server Certificate” file from your computer to the device. Browse to the certificate created and saved as media gateway.cer
- Click on Send File to import the certificate.
- In the Send “Trusted Root Certificate Store” file from your computer to the device window. Browse to the root certificate created and saved as certnew.cer.
- Click on Send File to import the certificate.

The media gateway does not allow for the current certificates to be checked. The media gateway overwrite the existing certificates with any new certificate that is applied.

8 Customer Configuration Euro ISDN

The sample Board.ini file contains most of the settings required to deploy the media gateway when connecting directly to a Euro-ISDN interface. To help in configuration of the gateway a scenario can be used. This helps navigates to the prompts required to be changed. If the scenario is not loaded the browser can be used to navigate to the required prompts.

Advanced Network Settings

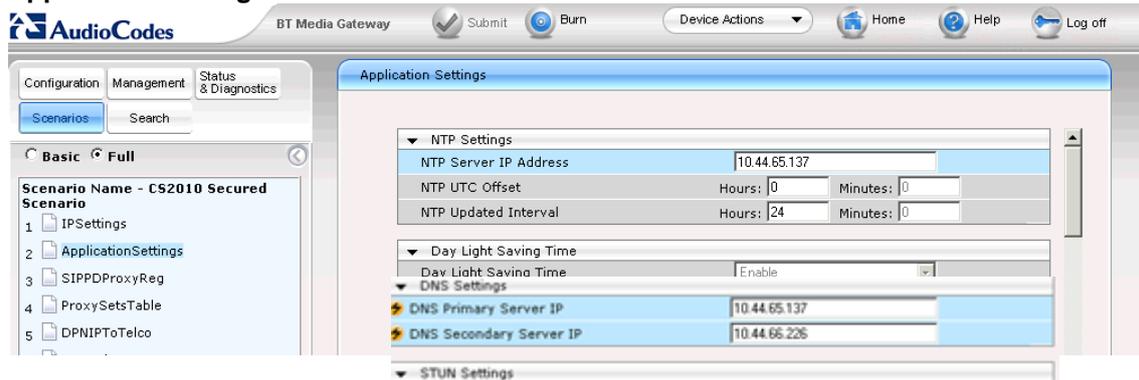
The initial scenario tasks look at setting the media gateway with the correct network settings. You require the following information:

Information Required	Customer Information	Example Information
IP, Subnet and Default Gateway Address		10.44.65.177 255.255.255.192 10.44.65.129
NTP server address.		10.44.65.137
DNS server address.		10.44.65.137
FQDN for the Microsoft Lync front end server.		r3mcsvse01.futuresii.local
FQDN name for the media gateway. This requires creation of an A record within the DNS server to be created.		gwm2kcol.futures.bt.local

IP Settings

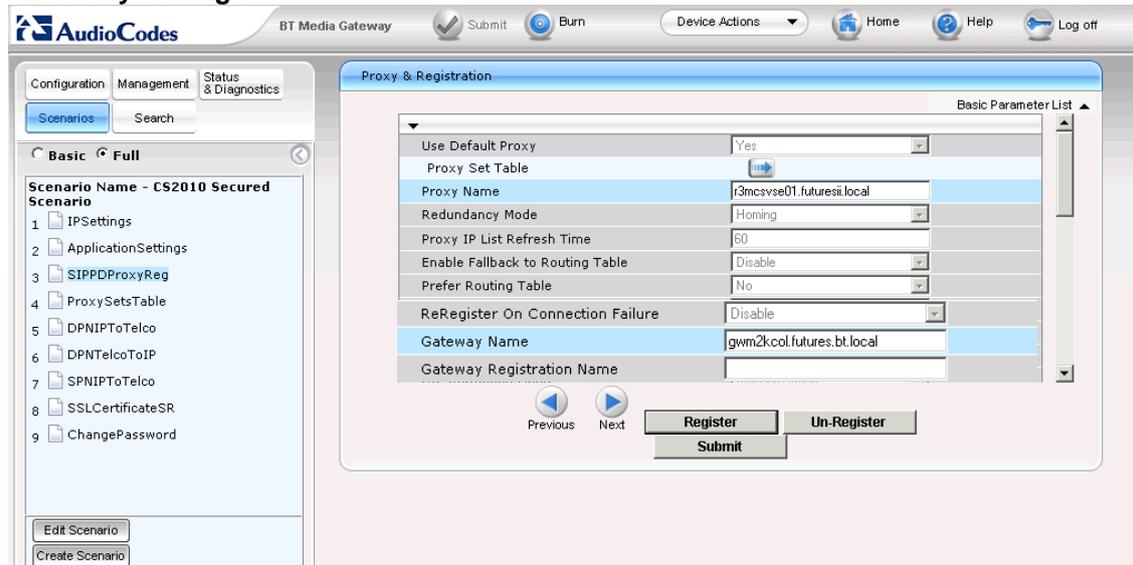
- Modify and insert the required IP Address, Subnet Mask and Default Gateway Address.
- Click Submit.
- These prompts can be set from Configuration, Network Settings, Ip Settings.

Application Settings



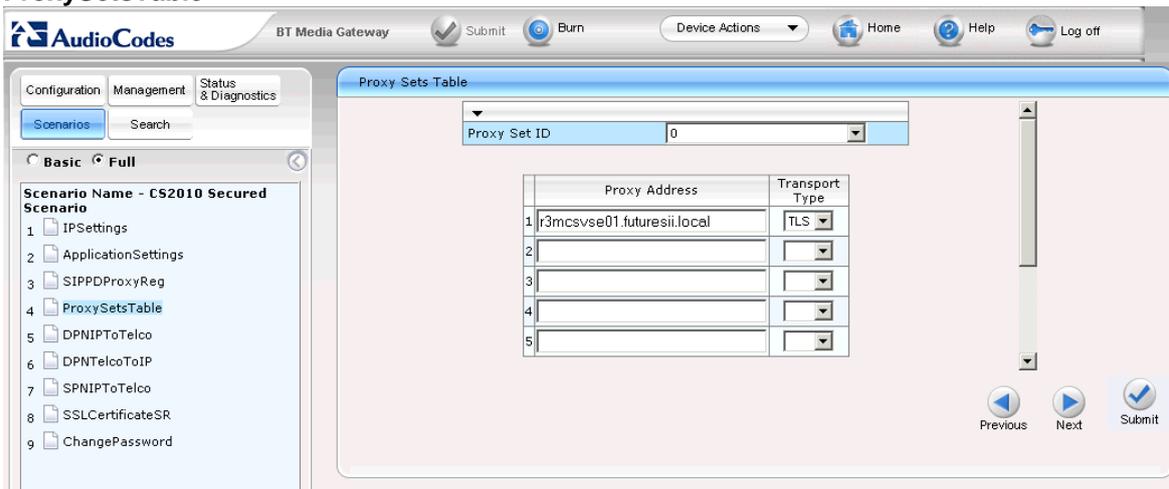
- Modify and insert the required NTP Server Address.
- Modify and insert the required DNS Server Address.
- Click Submit.
- These prompts can be set from Configuration, Network Settings, Application Settings.

SIP Proxy Settings



- Modify and insert the FQDN of the Microsoft Lync server in the Proxy name field.
- Modify and insert the DNS name assigned to the gateway in the Gateway name field..
- Click Submit.
- These prompts can be set from Configuration, Protocol Configuration- Proxies,Registration,IP Groups - Proxy and Registration.

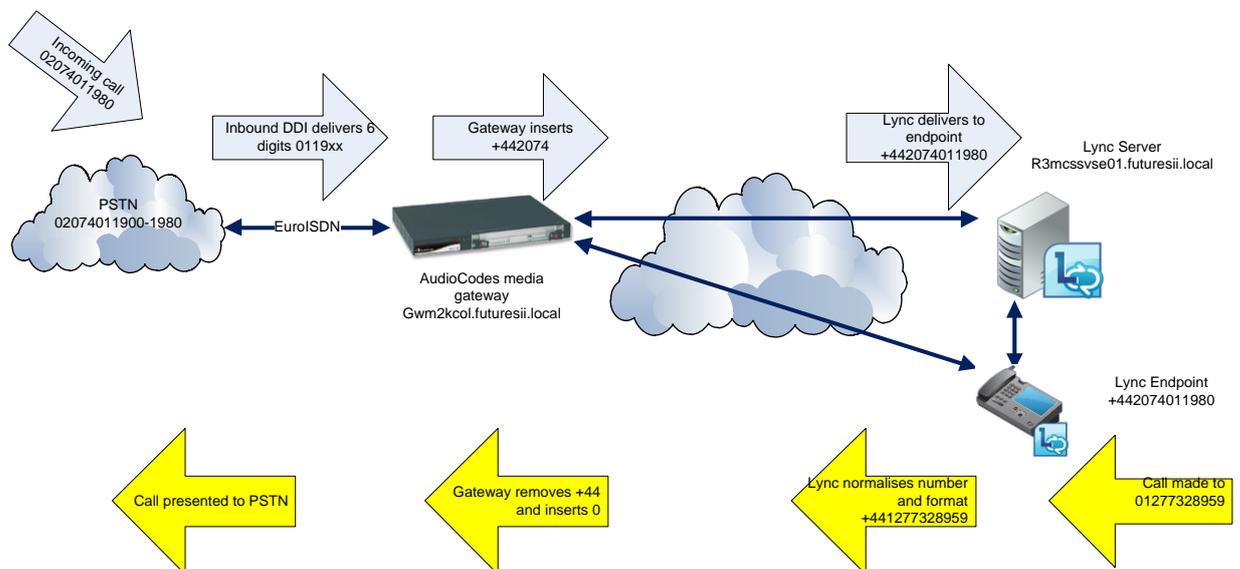
ProxySetsTable



- Check proxy set ID 0 is selected.
- Modify and insert the FQDN of the Microsoft Lync server in the Proxy Address field.
- Check the Transport Type is set to TLS.
- Click on Submit.
- These prompts can be set from Configuration, Protocol Configuration- Proxies,Registration,IP Groups – Proxy Sets Table.

Routing and Manipulation Information

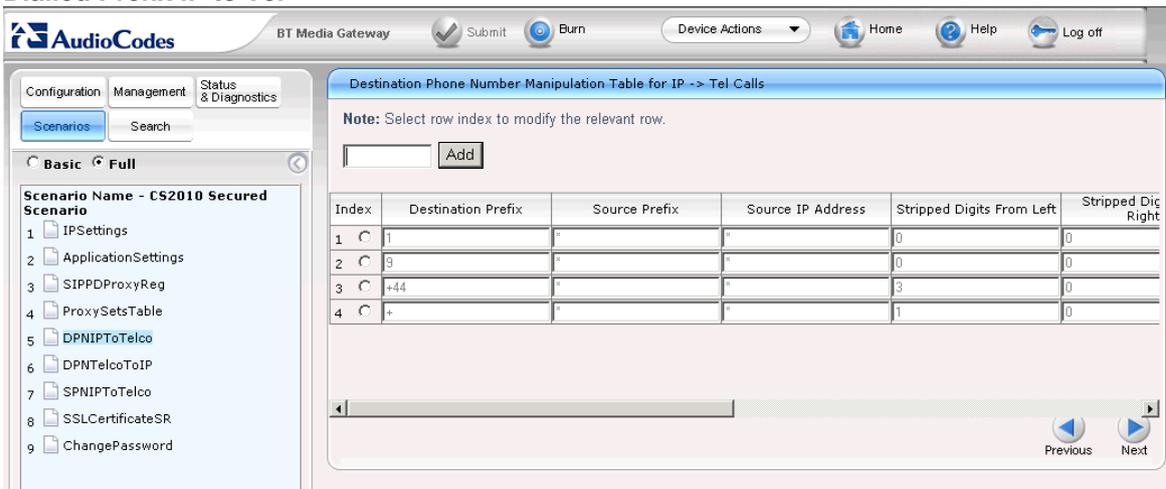
The sample scenario is created for a customer using the following numbering scheme.



The allocated PSTN range is 02074011980-1989. The DDI number delivered to the gateway 011980 this is manipulated by the gateway to +442074011980 for presentation to Microsoft Lync.

When a Communicator endpoint makes a call, in this example to 01277328959, Microsoft Lync normalises the number to +441277328959. Microsoft Lync then determines permissions and route to make the call and if allowed passes the call to the gateway. The gateway removes the +44 and inserts 0 to allow the call to be presented to the PSTN.

Dialled Prefix IP to Tel

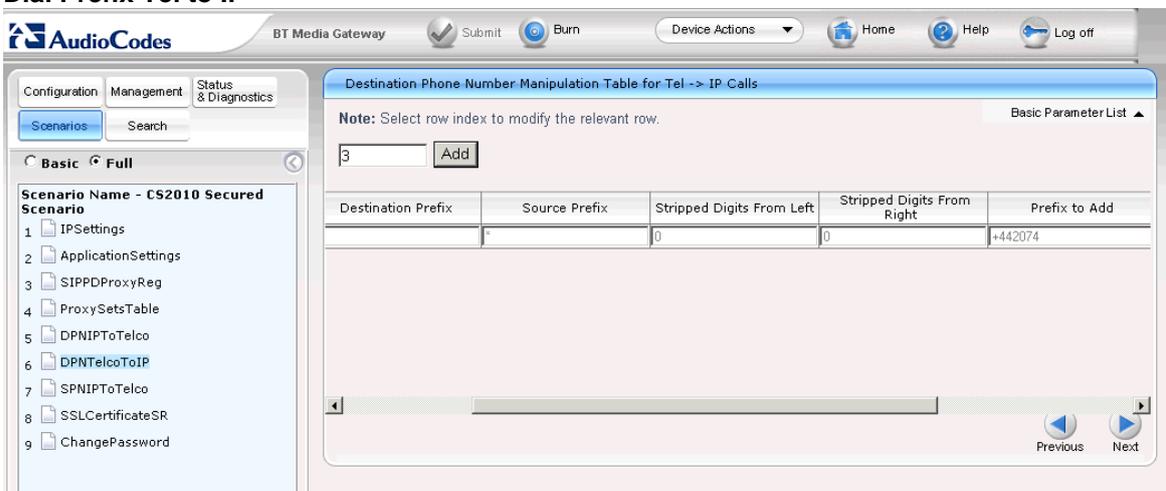


The standard routing should be correct for most UK customers connecting the media gateway directly to the PSTN via Euro ISDN.

The standard scenario also manipulates the formats received from Microsoft Lync for international and service numbers. Local calls are normalised to the full e164 number so do not need further manipulation.

- Check the settings can be applied to this customer.
- These these prompts can be set from Configuration, Protocol Configuration- Mainpulation Tables – Dest Number IP to Tel.

Dial Prefix Tel to IP

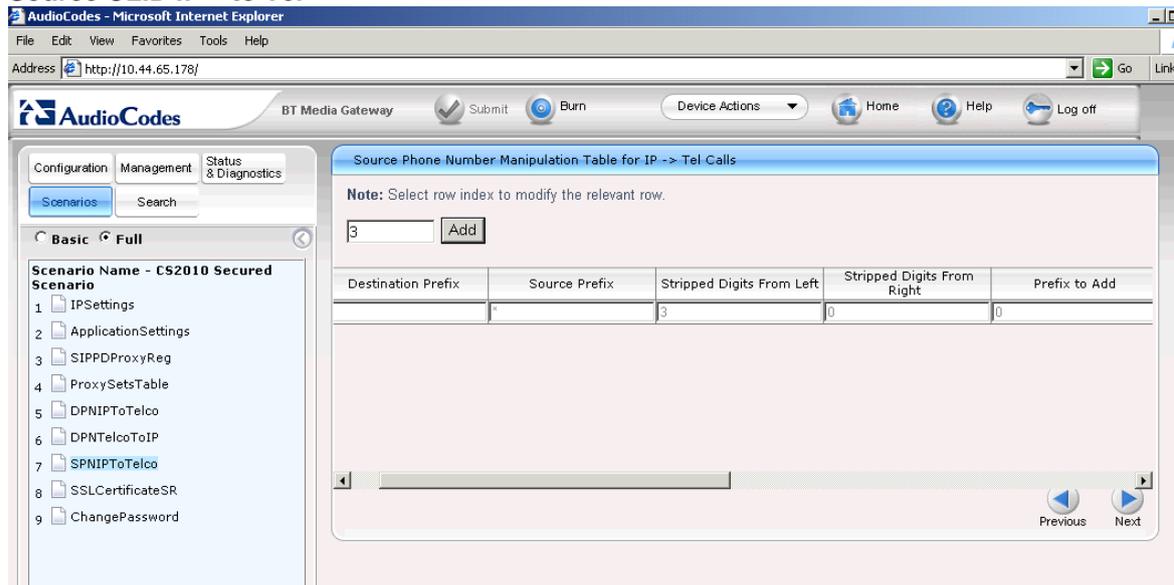


The standard scenario contains an example that builds a six digit DDI number into an E164 format number by adding the required prefix.

- Modify the Prefix to Add settings to contain the required site prefix.
- Select Apply to modify the changes.
- These prompts can be set from Configuration , Protocol Configuration- Mainpulation Tables – Dest Number Tel to IP.

Multiple DDI ranges could be accomodated with additional enties. The Destiantion Prefix can be expanded to cover the required range.

Source CLID IP – to Tel



The standard configuration should be correct for most customers connecting the media gateway directly to the PSTN. If changes are required these will need to be made on the individual lines and submitted.

The source number of the person making the call is passed from Microsoft Lync to the gateway in the format +442074011980. This is changed to the UK format of 02074011980 to allow the CLID to be presented to the called party.

- These prompts can be set from Configuration, Protocol Configuration- Manipulation Tables – Source Number IP to Tel

Tel to IP Routing



- Modify and insert the FQDN of the Microsoft Lync server in the Dest Ip Address field.
- Check port 5067 is defined.
- Click Submit.
- These prompts can be set from Configuration, Protocol Configuration- Proxies,Routing Tables, Tel to IP Routing.

9 Customer Configuration QSIG

The sample Board.ini file contains most of the settings required to deploy the media gateway when connecting directly to a legacy PBX via a QSIG interface. To help in configuration of the gateway a scenario can be used. This helps navigate to the prompts to be changed. If the scenario is not loaded the browser can be used to change the required prompts.

9.1 Advanced Network Settings

The initial scenario tasks look at setting the media gateway with the correct network settings. You require the following information:

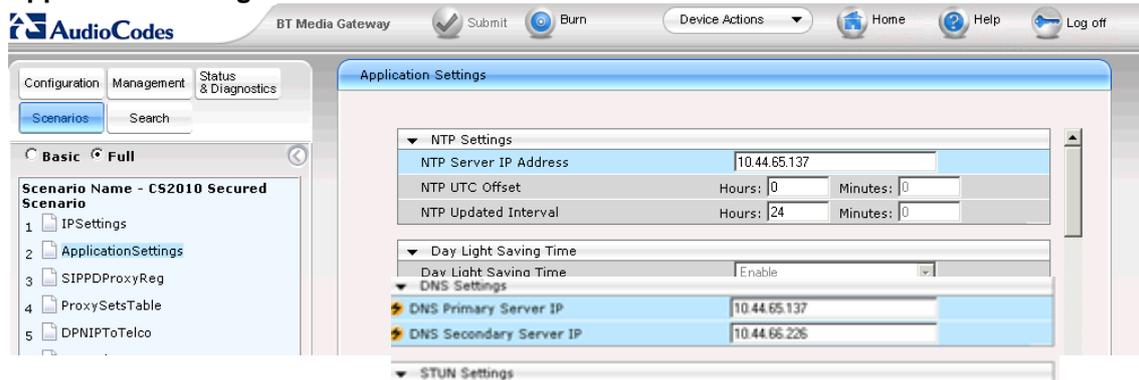
Information Required	Customer Information	Example Information
IP, Subnet and Default Gateway Address		10.44.65.177 255.255.255.192 10.44.65.129
NTP server address.		10.44.65.137
DNS server address.		10.44.65.137
FQDN for the Microsoft Lync front end server.		r3mcsvse01.futuresii.local
FQDN name for the media gateway. This requires creation of an A record within the DNS server to be created.		gwm2kcol.futures.bt.local

IP Settings

The screenshot shows the 'IP Settings' configuration page. On the left, there is a sidebar with a 'Scenarios' section containing a list of tasks: 1. IPSettings, 2. ApplicationSettings, 3. SIPProxyReg, 4. ProxySetsTable, 5. DPNIPToTelco, 6. DPNTelcoToIP, 7. SPNIPToTelco, 8. SSLCertificateSR, and 9. ChangePassword. The main content area is titled 'IP Settings' and contains two sections: 'Single IP Settings' and 'Multiple Interface Settings'. The 'Single IP Settings' section has three input fields: 'IP Address' with the value '10.44.65.178', 'Subnet Mask' with '255.255.255.192', and 'Default Gateway Address' with '10.44.65.129'. The 'Multiple Interface Settings' section has a 'Multiple Interface Table' button. At the bottom right, there are three buttons: 'Previous', 'Next', and 'Submit'.

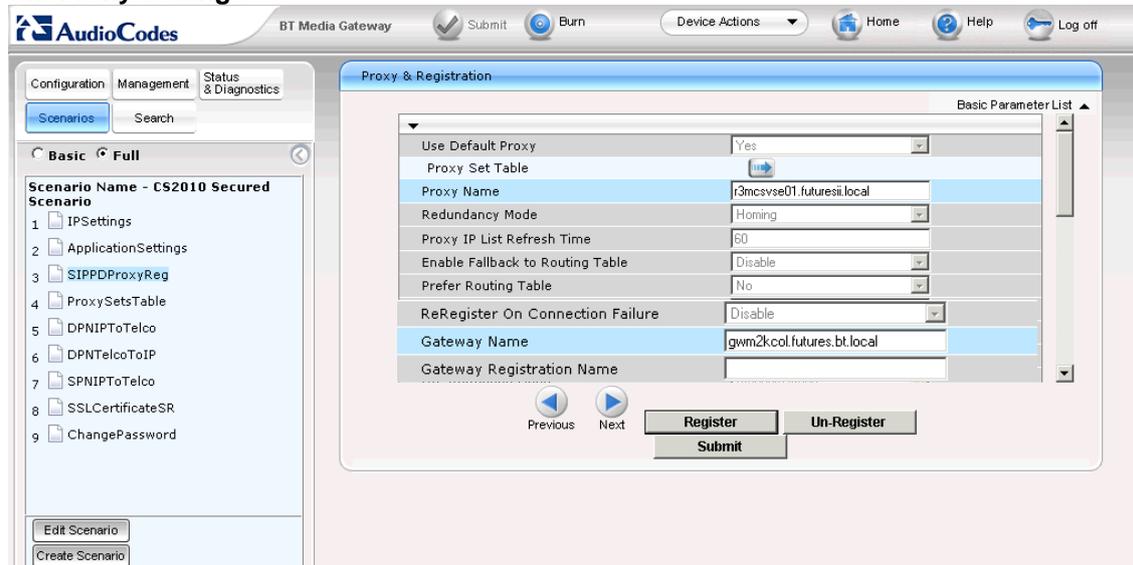
- Modify and insert the required IP Address, Subnet Mask and Default Gateway Address.
- Click Submit.
- These prompts can be set from Configuration, Network Settings, Ip Settings.

Application Settings



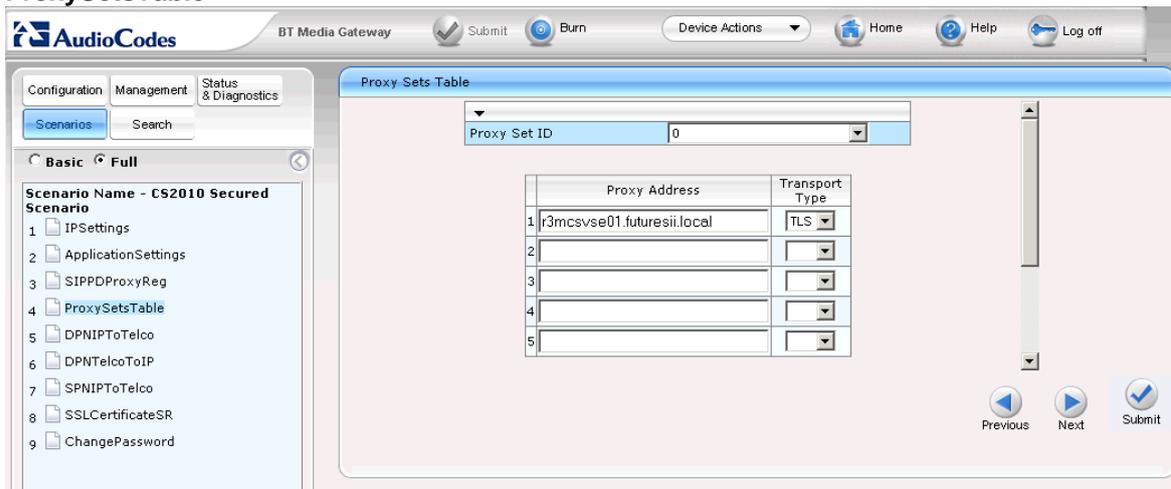
- Modify and insert the required NTP Server Address.
- Modify and insert the required DNS Server Address.
- Click Submit.
- These prompts can be set from Configuration, Network Settings, Application Settings.

SIP Proxy Settings



- Modify and insert the FQDN of the Microsoft Lync server in the Proxy name field.
- Modify and insert the DNS name assigned to the gateway in the Gateway name field..
- Click Submit.
- These prompts can be set from Configuration, Protocol Configuration- Proxies,Registration,IP Groups - Proxy and Registration.

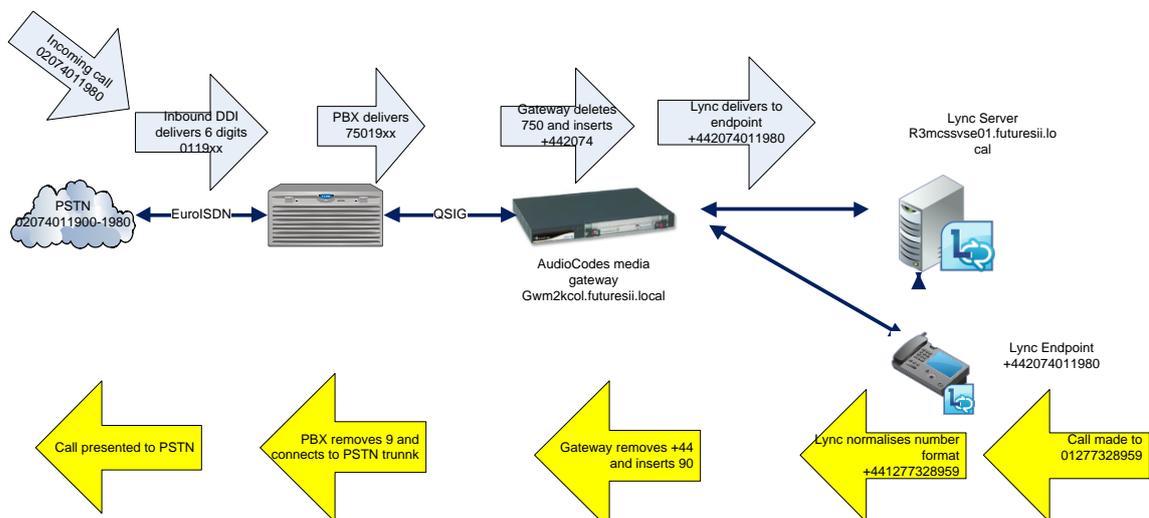
ProxySetsTable



- Check proxy set ID 0 is selected.
- Modify and insert the FQDN of the Microsoft Lync server in the Proxy Address field.
- Check the Transport Type is set to TLS.
- Click on Submit.
- These prompts can be set from Configuration, Protocol Configuration- Proxies,Registration,IP Groups – Proxy Sets Table.

Routing and Manipulation Information

The sample scenario is created for a customer using the following numbering scheme.



The allocated PSTN range is 02074011980-1989. The DDI number delivered to the PBX is 011980. The PBX is configured to pass this to the gateway via a QSIG route using 750 as a steering code followed by 011980. The gateway removes the 750 and inserts +442074, converting the number to +442074011980 for presentation to Microsoft Lync.

When a Lync endpoint makes a call, in this example to 01277328959, Microsoft Lync normalises the number to +441277328959. Microsoft Lync then determines permissions and route to make the call and if allowed passes the call to the gateway. The gateway removes the +44 and inserts 90 to allow the call to be presented to the PBX via the QSIG link. The PBX removes the leading 9 and places the call on a trunk to the PSTN.

Dialled Prefix IP to Tel

Index	Destination Prefix	Source Prefix	Source IP Address	Stripped Digits From Left	Stripped Digits From Right	Prefix to Add
1	1	*	*	0	0	
2	9	*	*	0	0	
3	+44	*	*	3	0	90
4	+	*	*	1	0	900

The standard routing should be correct for most customers connecting the media gateway to a PBX that requires level 9 for access to the PSTN.

The standard scenario also manipulates the formats received from Microsoft Lync for international and service numbers. Local calls are normalised to the full e164 number so does not need further manipulation.

- Check the settings can be applied to this customer.
- If connecting to a PBX the required PSTN access code will need to be inserted.
- If not running the scenario, these prompts can be set from Configuration, Protocol Configuration- Manipulation Tables – Dest Number IP to Tel.

Dial Prefix Tel to IP

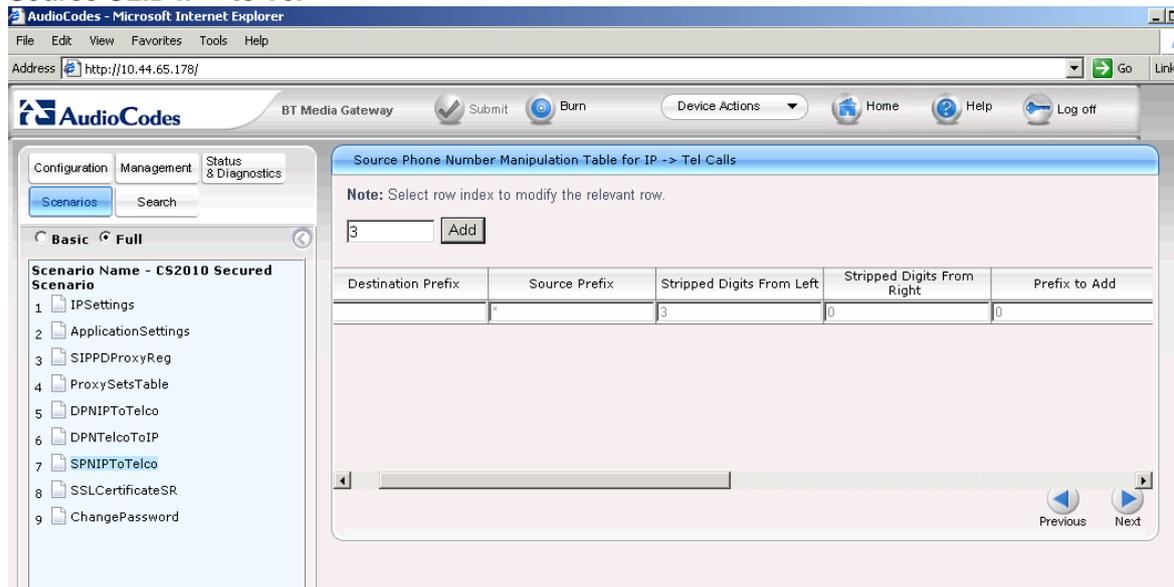
Index	Source Trunk Group	Source IP Group	Destination Prefix	Source Prefix	Stripped Digits From Left	Stripped Digits From Right	Prefix to Add
1	-1	-1	*	*	3	0	+442074

The standard scenario contains an example that removed a 3 digit steering code from the PBX and then builds the remaining six digit DDI number into an E164 format number by adding the required prefix.

- Modify the Prefix to Add settings to contain the required site prefix.
- Select Apply to modify the changes.
- If not running the scenario, these prompts can be set from Configuration , Protocol Configuration- Manipulation Tables – Dest Number Tel to IP.

Multiple DDI ranges can be accommodated with additional entries. The Destination Prefix can be expanded to cover the required range.

Source CLID IP – to Tel

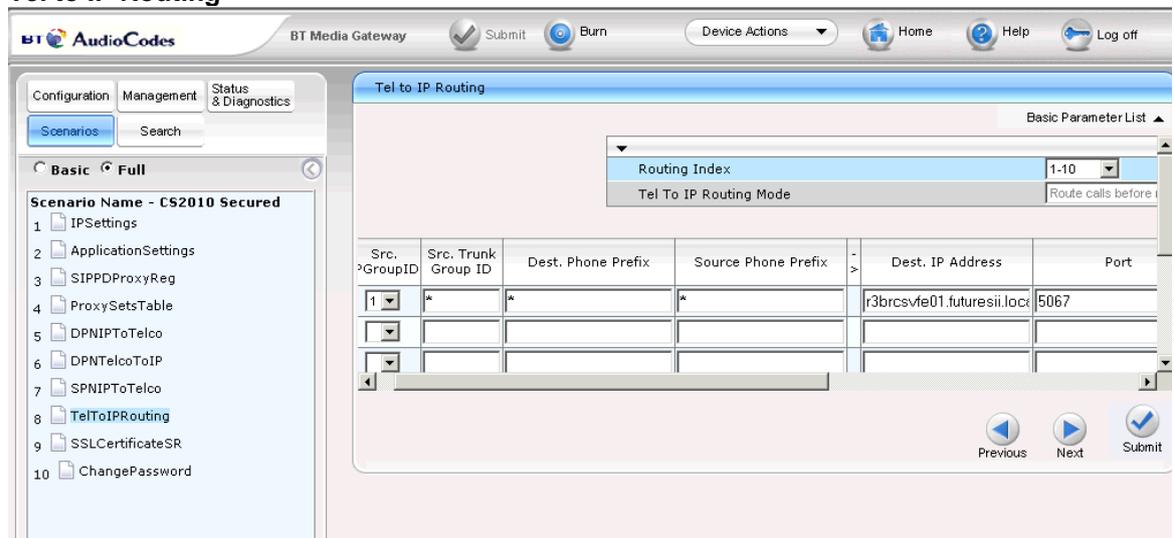


The standard configuration should be correct for most customers. The E164 number format is converted by the gateway into a format required by most PBX platforms for passing onto the PSTN.

The Source number of the person making the call is passed from Microsoft Lync to the gateway in the format +442074011980. This is changed to the format of 02074011980 to allow the CLID to be presented to the called party.

- If not running the scenario, these prompts can be set from Configuration, Protocol Configuration- Manipulation Tables – Source Number IP to Tel

Tel to IP Routing

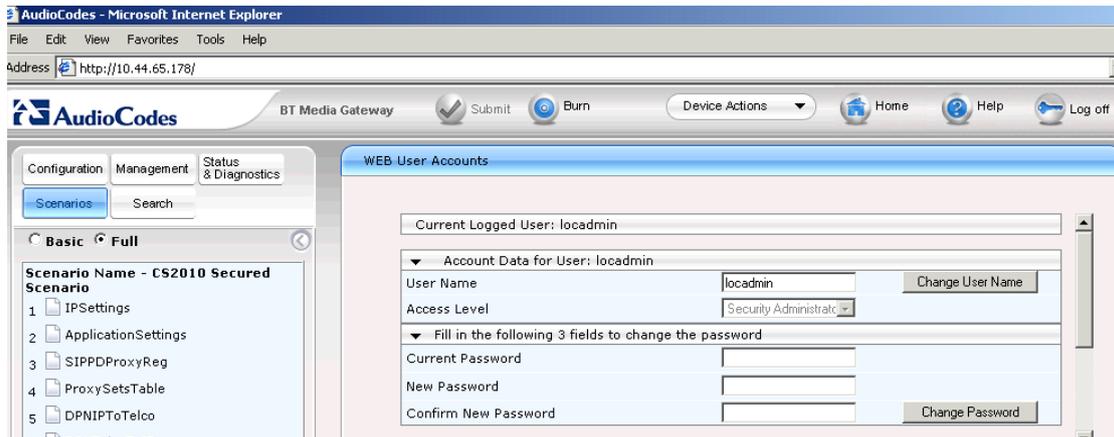


- Modify and insert the FQDN of the Microsoft Lync server in the Dest Ip Address field.
- Check port 5067 is defined.
- Click Submit.
- If not running the scenario, these prompts can be set from Configuration, Protocol Configuration- Proxies, Routing Tables, Tel to IP Routing.

10 Security

Change gateway default password.

The media gateway username of Admin and password of Admin need to be changed. The recommended user name should be locadmin. The default password should be set to the same as that used for other servers provided as part of the managed solution.



- In the Web User Accounts window under Account Data for User Admin, select Change User Name.
- Replace the Admin account name with locadmin.
- Select Submit.
- Login in with the new account name with the original password.

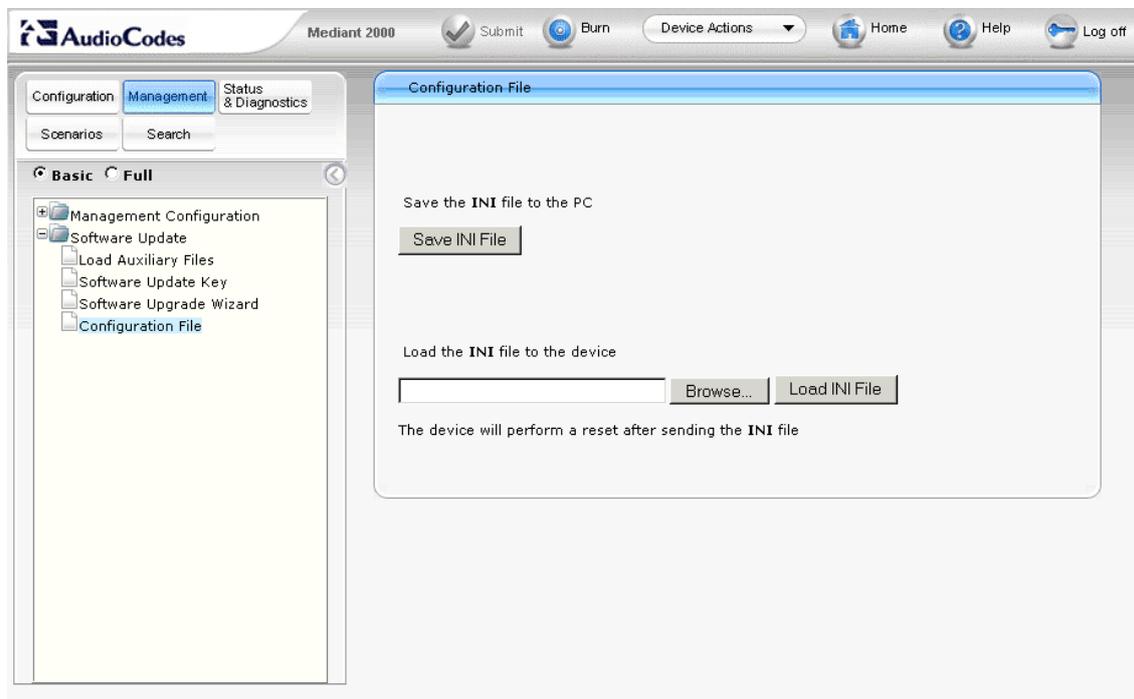
- In the Web User Accounts window under Fill in the following 3 field to change the password.
- Enter the current password.
- Enter and confirm the new password.
- Select Submit.
- Login with the new account name and new password.

11 Backup of Configuration and Restore

The media gateway will contain a modified Board.ini file that will contain the differences for this customer. A copy should be taken and stored with other customer related information. The certificate files are also customer specific. If the gateway is changed out then the new certificates will be required to be added to the media gateway.

Back up media gateway configuration.

- In the top left hand menu select Management.
- In the left hand tree expand Software Update and select Configuration File.
- In the Configuration File window select “Save INI File” from this device to your computer”
- Browse to a suitable folder to save the configuration file.



Restoring the media gateway.

The restoration process of the media gateway is the same as the process used to initially install the device.

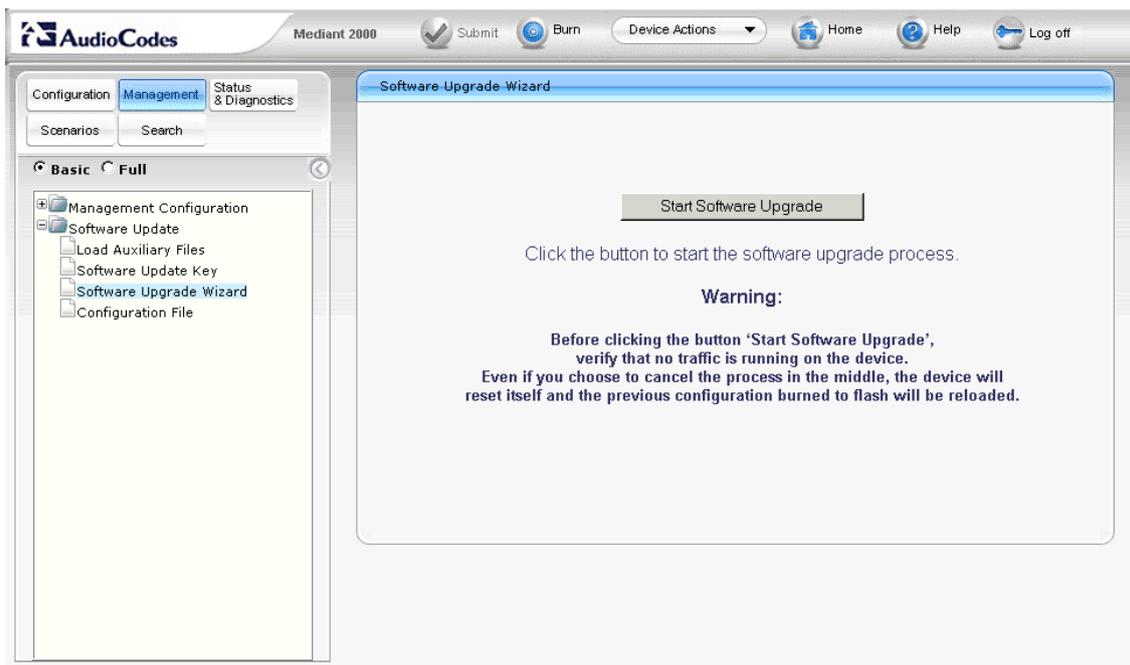
- Replace a physical unit reconnect all cables and relevant modules.
- Obtain a copy of the configuration files from Livelink.
- Obtain a copy of the customer specific board.ini file.
- Follow the [BootP](#) or [Embedded web server](#) installation procedure described.
- Contact the commissioning team to retest using the numbers listed at the end of this document.

12 Upgrade

The media gateway firmware may need to be upgraded periodically. The latest version of firmware is posted at <http://livelink.intra.bt.com/livelink/livelink.exe?func=ll&objId=121134726&objAction=browse&sort=name>

To upgrade the firmware

- In the top left hand menu select Management.
- In the left hand tree select Software Update and Select the Software Upgrade Wizard.
- In the Software Upgrade Wizard select Start Software Upgrade.



A warning message is shown, once an upgrade is requested the device will automatically reset.

- Click on any other tab to navigate away from this page if selected inadvertently.
- If you wish to continue click the “Start Software Upgrade”.



- In the load a CMP file window select Browse.

- Navigate to the firmware to be installed this is CMP file.
- Click on send file.

The file is loaded and the option given to load additional files.

- Click on next until the upgrade is complete.
- The device will reset with the new configuration.

13 References

External References used.

Reference designs	Audiocodes LTRT-10005 Interoperability List v2.4.pdf
	AudioCodes LTRT-26003 Mediant 1000 & 2000 & MS OCS 2007 Quick Guide Ver 6.0.doc
	AudioCodes LTRT-18202 Enhanced Media Gateway and SBA.
	AudioCodes LTRT -68809 SIP User's Manual 6.0

14 Glossary

Expand / Change as required for your area and technologies.

AD	Active Directory
CA	Certification Authority issues and validates certificates.
GC	Global Catalogue
M1K	AudioCodes Mediant 1000 gateway
M2K	AudioCodes Mediant 2000 gateway
Microsoft Lync	Third generation of Microsoft Office Communication Server.
Media Bypass	Allows the voice path to be extended directly from a communicator client to a gateway without using a mediation server.
Mediation Server	Provides monitoring and protocol conversion from the Microsoft codec RTAudio, to the G711 protocol.
MS	Microsoft
PBX	Private Branch Exchange descriptive term for a telephone phone system.
PSTN	Public Switched Telephone Network
SIP	Session Initiated Protocol used to establish and clear down calls.
UCC	Unified Communications and Collaboration
VOIP	Voice over IP protocol.

15 Appendix A – BootP Configuration.

BootP is the preferred method to use to configure the media gateway. This will apply most of the required configuration in a single step. If the use of BootP is not possible the manual process can be used, this is described in the [section 6](#).

All the required files needed to deploy using Boot P are posted on Livelink at this location

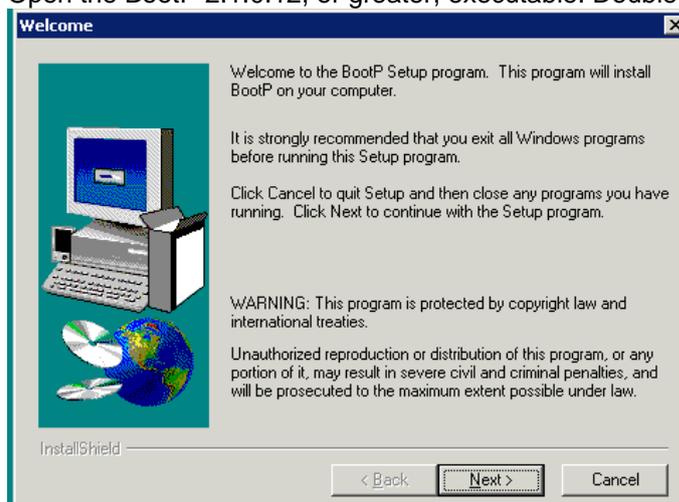
<http://livelink.intra.bt.com/livelink/livelink.exe?func=ll&objId=121134726&objAction=browse&sort=name>

They are available in a single downloadable file. This includes a copy of the BootP software. A copy of BootP is also provided on the installation CD supplied with the media gateway.

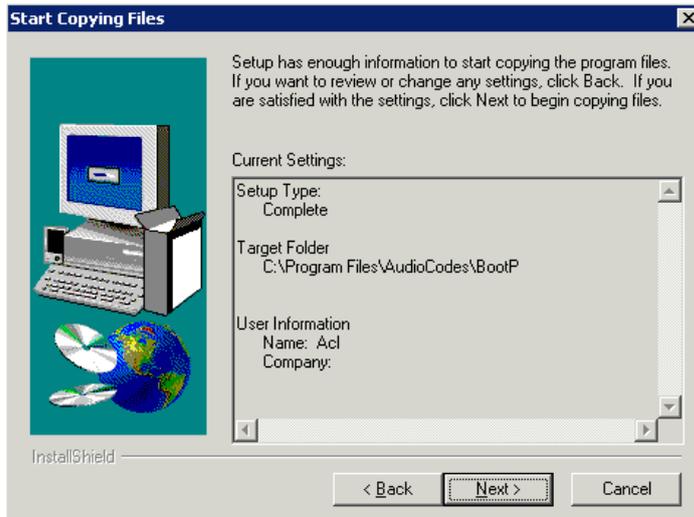
Due to many routers not passing BootP it is recommended that you run from a device within the same network segment. If this is not possible use a PC connected directly to the media gateway using a crossover cable connected to Ethernet port 1.

15.1 Installing Boot P

Open the BootP 2.1.0.12, or greater, executable. Double click on setup.exe



- In the Welcome window select next,
- In the Read Me Information window select next.
- In the Choose Destination Location window, accept the default location select next.
- In the Select Program Folder window select next.



- In the Start Copying Files window select next.

When the program has finished installing, select finish completing the installation.

15.2 Configuring BootP

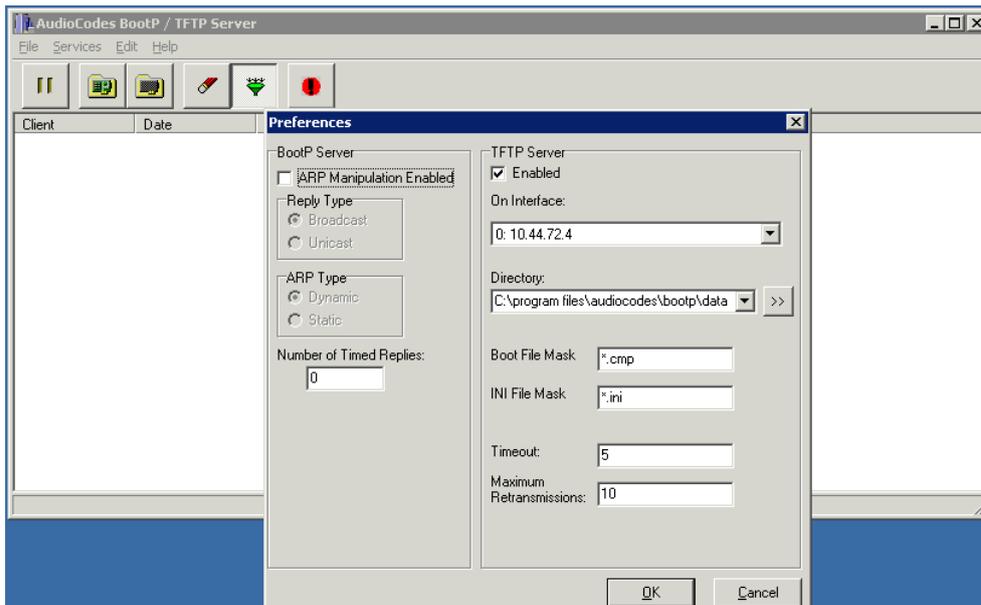
Check that the following files downloaded from Livelink are copied into the :\program files\AudioCodes\BootP\data

BoardQSIG.ini
BoardEuroISDN.ini
TP1610_SIP_F6.00A.xx.xx.cmp
Uk.dat
Uk.ini
Secured scenario.dat
BTACLogo.gif

Launch the Boot P application from Program Files, BootP, BootP.exe

Configure preferences:

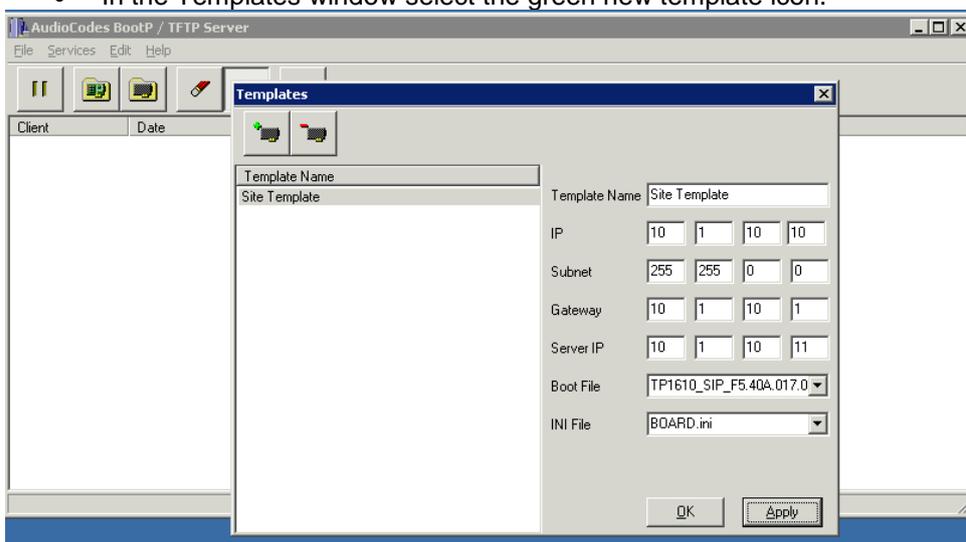
- Select Edit
- Select Preferences



- Check that the interface shows the IP address of the server running BootP (it may show the local host value 127.0.0.1)
- Use the browse icon next to the directory path to navigate to the folder where the board.ini, TMP1610,uk.dat and uk.ini files are located. It is recommended to use Program Files\Audiocodes\BootP\Data. Check that the path is has updated, it can also be set manually.
- Click okay which closes the preferences tab.

Create a new template.

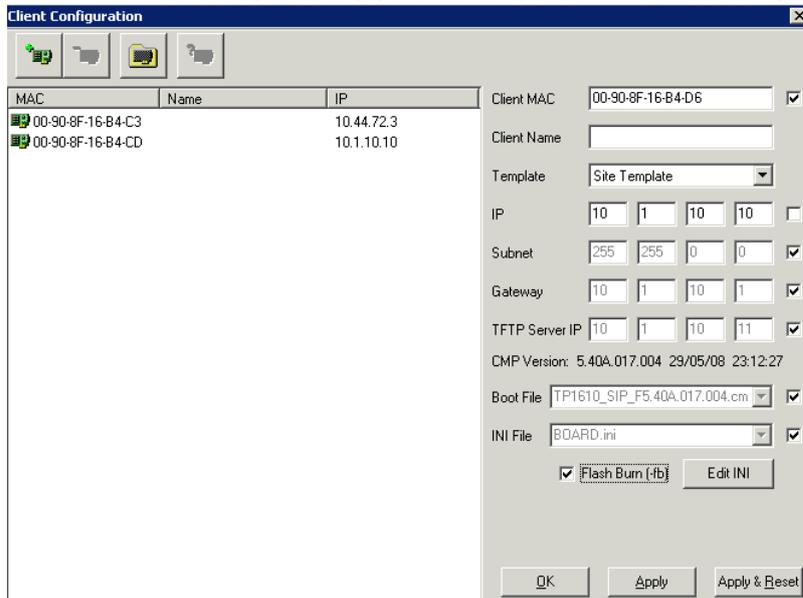
- In the AudioCodes BOOT P TFTP server window select Services and then select Templates. If the error message “Error opening TFTP directory “ is received, click okay and go back and check that the path in the template created previously is correct.
- In the Templates window select the green new template icon.



- Enter the template IP address range to be offered. If configuring locally enter the defaults values as shown.
- In the drop down box to the right of the Boot File select the P1610_SIP_F6.0a.xx.xx.cmp file.
- In the drop down box to the right of the INI File select required BOARD.ini file. Use BoardQSIG for QSIG connections or BoardEuroISDN for EuroISDN connections.
- Select OK closing the Templates window.

Creating a Client

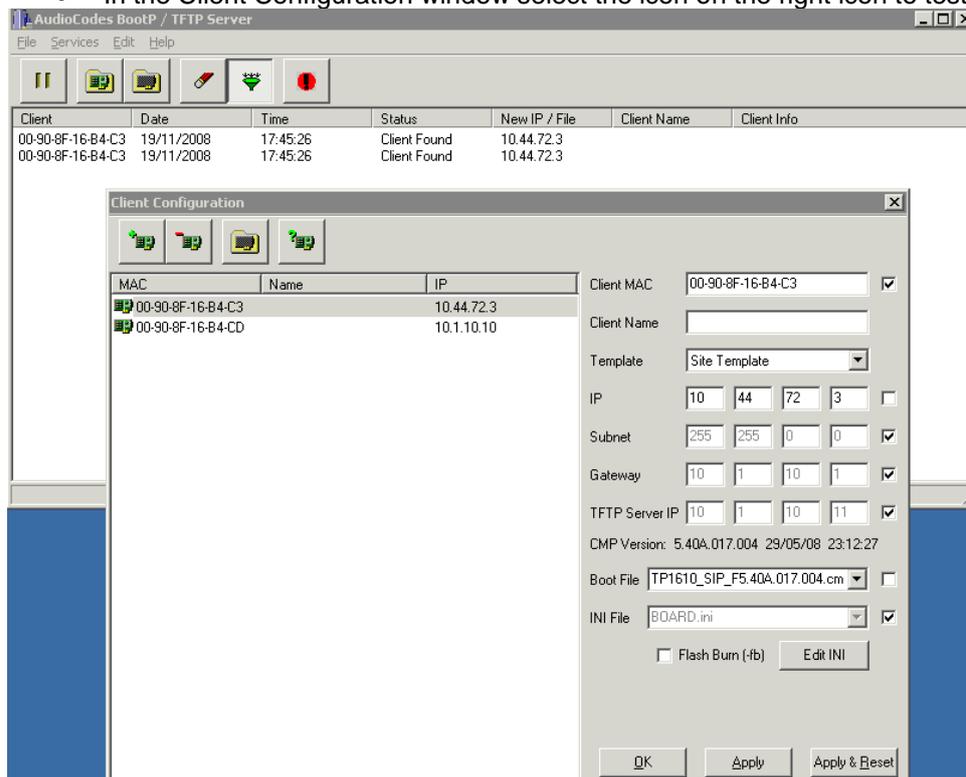
- In the AudioCodes BOOT P TFTP server window select Services and then select Clients.



- Enter the MAC address of the media gateway in the Client MAC field. It is written on the front of the gateway.
- In the drop down box to right of Templates select the template previously created.
- All the fields will be populated with the exception of the IP address. The IP address to be assigned to the device needs be added. In this example the default address has been used.
- Check the flash burn option is selected.
- Select Apply.

Check gateway can be detected.

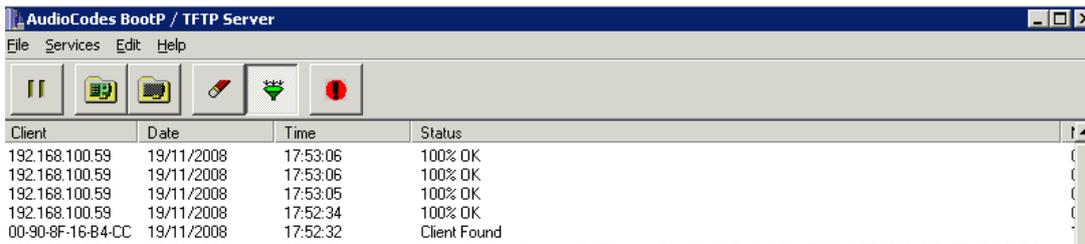
- In the Client Configuration window select the icon on the right icon to test for connection.



- When the test icon is selected the BootP software checks it can reach the MAC address. Client found should appear in the status window. If this doesn't appear check for network errors.
- Close the client window.

Uploading files to the gateway

- In the AudioCodes Boot/TFTP Server, select the line containing the MAC address of the media gateway.
- Right click on the line and select reset.



Client	Date	Time	Status
192.168.100.59	19/11/2008	17:53:06	100% OK
192.168.100.59	19/11/2008	17:53:06	100% OK
192.168.100.59	19/11/2008	17:53:05	100% OK
192.168.100.59	19/11/2008	17:52:34	100% OK
00-90-8F-16-B4-CC	19/11/2008	17:52:32	Client Found

- The gateway will restart. It will then upload the files from the BootP application to the gateway.
- Close the BootP application.

16 Appendix B – Support Numbers.

The media gateway interfaces between Microsoft Lync and a PRI trunk connecting to the PSTN or PBX. The following numbers can be used for help with in configuration of the media gateway. These numbers are for UK deployments and will be updated for International launch.

Avaya Support	0208 633 1010
Nortel Support	0800 371779
Cisco Support	01977 591706
Second Line Helpdesk BATS Incident Management	
Switch diagnostic team	0800 731 5109
Technical Support team	0800 371 779