KAKAPO
SYSTEMS

Unity Client: Connectivity & Protocol Overview

This document outlines the network connections and BroadWorks protocols employed by the Unity Client to provide base functionality. It describes how to configure Unity to use these protocols and provides trouble-shooting steps to common issues.

1 Connectivity

The below table outlines the connections that Unity will create to all other platforms. Please note that the port numbers given are default values which may have been changed by the Broadworks system provider. Broadworks protocols are outlined in detail in section 2 below.

It is imperative that the customer firewall allows the below outbound connections on the TCP ports stated unless changed by the system provider, otherwise Unity will not be able to connect.

Licensing & Branding

FQDN: portal.unityclient.com

Primary IP Address: 185.42.19.40

Secondary IP Address: 83.142.25.185

TCP Port 443 & 80, outbound only

IM&P, SMS Integration and Contact Center

FQDN: im.unityclient.com

Primary IP Address: 185.42.19.38

Secondary IP Address: 83.142.25.183

TCP Port 2208, outbound only

Unity Web Apps

Primary IP Address: 185.17.172.185

Secondary IP Address: 85.13.237.8

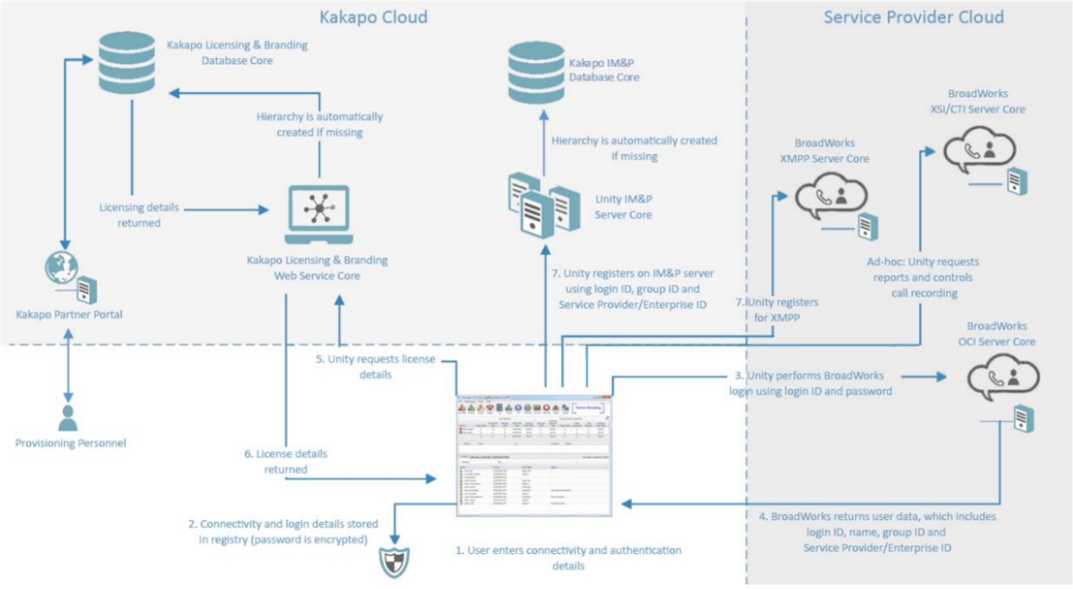
Platform/Server	Connection Type	Protocol
Broadworks OCI Server	TCP connection on port 2208 or port 2209 if TLS is in use	Open Client Interface (OCI) & Client Application Protocol (CAP)
Broadworks CTI Server	TCP connection on port 8011 or port 8012 if TLS is in use	Computer Telephony Interface (CTI). Replaces CAP for call control and BLF functionality.
Broadsoft XSI Server	All communication uses HTTPS	Xtended Services Interface (XSI)

		Standard HTTPS POST requests with embedded XML body. Used to integrate with call recording and visual voicemail, and when generating call center reports
Kakapo Licensing & Branding Platform	All communication uses HTTPS. Requests are sent to portal.unityclient.com which is a load-balanced virtual address	Encrypted XML document sent as SOAP envelope, response is received as an encrypted XML document in a SOAP envelope. Used during startup to fetch branding and license details for the system provider and user.
Kakapo IM&P Server	TCP connection on port 2208. Default FQDN is im.unityclient.com which resolves to a load balanced virtual address	Kakapo Encrypted Messaging Protocol (KEMP) consisting of an HTTP-like structure with an encrypted XML message body. Used to register on the IM&P server and send and receive messages.
XMPP Server	TCP connection on port 5222	XMPP messaging protocol as defined in IETF RFC 6120.

Unity connects to Broadworks OCI/CAP/CTI and Kakapo servers using a standard TCP/IP connection, which may or may not use TLS for secure communication depending on the Broadworks server configuration. This connection is kept open while Unity is running by sending periodic keep-alive messages. If the connection is severed unexpectedly (meaning without the user closing Unity) then Unity will attempt to reconnect every 15 seconds until the connection is re-established.

1.1 Unity Start-Up

The Unity start-up process (which illustrates when these connections are created) is outlined below.


Kakapo Cloud
Service Provider Cloud
Kakapo Licensing & Branding Database Core
Hierarchy is automatically created if missing
Licensing details returned
Kakapo Licensing & Branding Web Service Core
Kakapo Partner Portal
Provisioning Personnel
Kakapo IM&P Database Core
Hierarchy is automatically created if missing
Unity IM&P Server Core
7. Unity registers on IM&P server using login ID, group ID and Service Provider/Enterprise ID
7.1Unity registers for XMPP
BroadWorks XMPP Server Core
BroadWorks XSI/CTI Server Core
Ad-hoc: Unity requests reports and controls call recording
BroadWorks OCI Server Core
5. Unity requests license details
6. License details returned
3. Unity performs BroadWorks login using login ID and password
4. BroadWorks returns user data, which includes login ID, name, group ID and Service Provider/Enterprise ID
2. Connectivity and login details stored in registry (password is encrypted)
1. User enters connectivity and authentication details

Once the user enters the connectivity and authentications details, Unity will first fetch branding details for this user (based on the login ID), or if the user doesn't yet exist then branding details for the system provider (based on the server hostname). As well as standard branding settings, the response will include details on how Unity is to connect to the Broadworks server core (for example by using TLS or not, and which TCP port numbers to use for each protocol etc) and if CTI should be used instead of CAP, outlined in section 4 below.
Unity will then connect to the Broadworks OCI server using the branding settings returned and attempt to authenticate using the OCI protocol. The OCI server will use internal location procedures to locate the user in the correct BroadWorks Application Server cluster, if multiple AS clusters are in use.

Assuming the login succeeds, Broadworks will return the version of Broadworks that Unity has connected to as well as the user profile which includes first name, last name, extn, DDI, Broadworks Group ID and Broadworks Service Provider or Enterprise ID. The Broadworks version returned will help to determine which protocol to use in later phases.

If Unity is configured to use the CTI protocol instead CAP (as outlined in section 3.2 below) then Unity will connect to the CTI server at this point, using the connection details returned in the branding response. Please note the CTI server is often a separate physical server that uses a different TCP port to OCI, so an additional outbound firewall rule must be in place. If Broadworks if configured to use CTI and Unity can connect to the OCI server but not CTI, then the start-up procedure will stop and the user will be notified.

Once successfully connected to Broadworks, Unity will send a license request to the Kakapo licensing platform using HTTPS, the license request will include the below details:

- The server hostname (FQDN) of the Broadworks OCI server that Unity connected to. This is used to identify the Broadworks system provider in the Kakapo licensing platform. This may be the same hostname as the CTI server but in many cases it will be different.
- The login ID of the user, or the MAC address of the PC if using Unity Wallboard or Dashboard clients.
- The first and last names of the user, or the computer name if using Unity Wallboard or Dashboard clients.
- The user phone number, this is not used for Unity Wallboard or Dashboard clients.
- The Broadworks Group ID.
- The Broadworks Service Provider or Enterprise ID.

The Kakapo licensing platform will use the Service Provider/Enterprise and Group IDs to create the hierarchy in the Kakapo licensing platform if it doesn't already exist. The login ID (including the domain) is a unique identifier within a Broadworks platform, and a server hostname/FQDN can only resolve to a single Broadworks server. Therefore, by combining the login ID and server hostname as a compound key, this provides a globally unique identifier which is used to identify that user in the Kakapo partner portal.

The Kakapo licensing platform will use the login ID and first/last names to create the user account if it doesn’t already exist. The phone number is now ignored by the Kakapo licensing server as it is not required. The user/PC name will also be ignored by the server if configured for that system provider in the Kakapo portal. In this case only the login ID will be stored, this may be required to meet data protection/privacy policies.

The license response will include license details which includes if the user is configured to use Kakapo IM&P and/or XMPP for instant messaging. If Unity is permitted to connect to the Kakapo IM&P server core then the connection will be made at this point, using the connection details returned from the branding response. When registering on the Kakapo IM&P server, Unity will pass the login ID of the user, and the Group ID if the user is part of a Service Provider Group or the Enterprise ID if the user is part of an Enterprise Group. No other details are sent or used when registering the user on the IM&P platform.

If Unity is permitted to connect to the XMPP server then this connection will also be made. Rather than use connection details returned from the branding response, Unity connects to the XMPP server using the XMPP protocol (IETF RFC 6120) on port 5222, which is the industry standard for XMPP connectivity. If the “Integrated IM&P” service is assigned to the user in Broadworks, then the XMPP user ID will be included in the user profile from Broadworks after successfully logging in.
The domain from this XMPP user ID is a server FQDN which is used to connect to the server. XMPP configuration and functionality is further outlined here.

Once Unity is successfully connected to Broadworks and license details have been retrieved (and a valid license is assigned to the user), Unity will periodically connect to the Broadworks XSI server to perform ad-hoc tasks when actioned by the user, for example when fetching voicemails or when controlling (start/stop/pause/resume) call recording, or when generating call center reports.

2 Protocol Overview

There are three main protocols available when connecting to BroadWorks, as outlined below. The protocols discussed below, with the exception of XSI, are based on XML documents being sent and received over a TCP/IP) connection, the server port for the connection will differ based on the protocol being used.

2.1 Open Client Interface (OCI)

This protocol is used for service configuration as well as directory and call log integration. It is available with all BroadWorks releases, both for client-server and server-server communication. The connection for this protocol can be a standard TCP connection or a secure connection based on TLS, referred to as “OCI over TLS”. The BroadWorks OCI server must be configured to support OCI over TLS, this is not the default behaviour. Please speak to BroadSoft if you wish to implement this feature on the OCI server.

2.2 Client Application Protocol (CAP)

This protocol is available with all BroadWorks releases prior to R22. It provides call control BLF functionality and real-time call center queue updates (if applicable) to Unity. This protocol is only available for use if the Client Call Control service is assigned to the user (or call center for real-time queue updates) in BroadWorks, if this service isn’t assigned to the user logging in then Unity will alert the user and not proceed. The same connection (to the same server port) is used for OCI and CAP communication between Unity and BroadWorks (the Broadworks OCI server actually supports both OCI and CAP), therefore if the OCI connection is secured with TLS then this will implicitly apply to the CAP connection as well.

2.3 Xtended Services Interface & Client Telephony Interface (XSI & CTI)

The XSI protocol is a RESTful protocol over HTTP(s). This protocol provides all call control functionality, queue updates and BLF, but doesn’t support all the actions available in OCI, for example managing Shared Call Appearance. However, it does support voicemail retrieval and management which isn’t available through OCI, which is why it is used by Unity.

CTI is essentially the same as the XSI protocol, but over a standard TCP connection. This provides more robust connection management when connecting to the BroadWorks platform, as opposed to the XSI protocol which is more suited to web 2.0 applications and “mash-ups”. The CTI connection can also be secured using TLS, although unlike CAP this is not implicitly applied when OCI over TLS is implemented because the protocols use different server engines on different TCP ports. Therefore, the CTI server must be configured to support CTI over TLS, this is not the default behaviour. Please speak to BroadSoft if you wish to implement this feature on the CTI server.

3 Unity Support for BroadWorks Protocols

BroadWorks supports all of the above protocols, but will use them depending on the release of the BroadWorks platform that it is connect to, or configuration options in the Kakapo portal. As mentioned above the version of the Broadworks platform is determined as part of start-up, Unity supports all Broadworks releases from R17.

3.1 BroadWorks Release 20 and below

Prior to BroadWorks release 21 the XSI/CTI protocol had not been developed sufficiently for Unity to use it in place of CAP for base functionality. Therefore, Unity will always use CAP when connecting to BroadWorks R20 or below, even if the Kakapo portal has been configured to use CTI.

The OCI/CAP connection can be secured with TLS, depending on the relevant settings in the Kakapo portal, as outlined in section 4.1.

3.2 BroadWorks Release 21 (All Service Packs)

The XSI/CTI protocol was significantly enhanced in BroadWorks R21, so that all base functionality required by Unity is available. Therefore, Unity will use the branding response from the Kakapo platform (during start-up, as outlined in section 1.1 above) to connect to BroadWorks using CAP or CTI, in addition to OCI which is always used. As previously mentioned, the server ports will be different for the CTI protocol, so the customer site firewall must allow outbound connections on the server ports used by all protocols.

Both the OCI/CAP and CTI protocols can be secured with TLS, depending on the relevant settings in the Kakapo portal, as outlined in the below section. As mentioned these are separate TCP connections to different server ports, so securing one connection/protocol does not automatically secure the other.

3.3 BroadWorks Release 22 (All Service Packs)

The CAP protocol has been deprecated in R22, so that only XSI/CTI is available for call control and BLF. Therefore, Unity will always attempt to open a CTI connection to BroadWorks if the version is R22 or later, regardless of the configuration in the Kakapo portal. The CTI server port is mandatory in the Kakapo partner portal, the default value is 8011 which is the default port in BroadWorks. This portal setting will always be used when Unity connects to the CTI server (for unsecured communication). If the CTI server address is not specified in the Kakapo portal (and returned through the branding response) then Unity will attempt to connect to the same server FQDN as the OCI server.

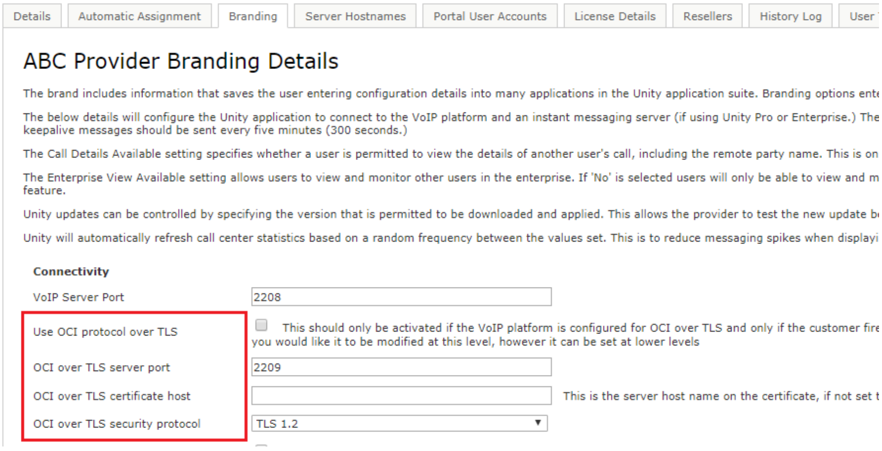
Both the OCI and CTI protocols can be secured with TLS, depending on the relevant settings in the Kakapo portal, as outlined in the below section. As mentioned these are separate TCP connections to different server ports, so securing one connection/protocol does not automatically secure the other.

4 Configurating Unity in the Kakapo Partner Portal

Unity will utilize the above BroadWorks protocols depending on version of the BroadWorks platform that it has connected to and Kakapo portal settings, as outlined below.

4.1 Activating OCI over TLS

By default, the OCI protocol does not use TLS. Once this has been activated and tested on the BroadWorks OCI server it can be activated for use by Unity, as shown below.



ABC Provider Branding Details

The brand includes information that saves the user entering configuration details into many applications in the Unity application suite. Branding options ente

The below details will configure the Unity application to connect to the VoIP platform and an instant messaging server (if using Unity Pro or Enterprise.) The keepalive messages should be sent every five minutes (300 seconds.)

The Call Details Available setting specifies whether a user is permitted to view the details of another user's call, including the remote party name. This is on

The Enterprise View Available setting allows users to view and monitor other users in the enterprise. If 'No' is selected users will only be able to view and m feature.

Unity updates can be controlled by specifying the version that is permitted to be downloaded and applied. This allows the provider to test the new update b

Unity will automatically refresh call center statistics based on a random frequency between the values set. This is to reduce messaging spikes when displayi

Connectivity

VoIP Server Port: 2208

Use OCI protocol over TLS: □ This should only be activated if the VoIP platform is configured for OCI over TLS and only if the customer fire you would like it to be modified at this level, however it can be set at lower levels

OCI over TLS server port: 2209

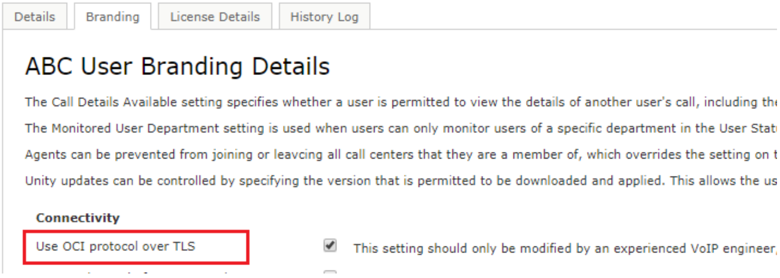
OCI over TLS certificate host: This is the server host name on the certificate, if not set t

OCI over TLS security protocol: TLS 1.2

The “Use OCI protocol over TLS” setting doesn’t need to be set at the system provider level, as it can be activated at the reseller, group or user level (for a phased rollout to customer sites or for pilot testing/rollout). However, the OCI over TLS server port must be set at the system provider level before activating the feature at any level, because Unity must know which server port to connect to for secure communication (this will be different to the non-secure VoIP server port).

If a provider does not want to allow OCI over CTI to be implemented because the Broadworks server isn’t configured, then the OCI over TLS server port should be kept blank. If the OCI server supports both unsecure and secure (TLS) connections, then the “VoIP Server Port” value should be set as 2208 and the “OCI Over TLS Server Port” value should be 2209. However, if the server supports only OCI over TLS then both the “VoIP Server Port” and “OCI Over TLS Server Port” should be set to 2209. These settings will then be included in the branding response to Unity client as part of the start-up procedure.

The certificate host name should also be set if different to the FQDN that Unity connects to. Lastly the security protocol must be explicitly set, because Unity cannot try to secure the connection using any available security protocol because the OCI server will close the connection if the wrong one is used. As with all branding settings, if this is changed then it will also update the same setting for all level below. Therefore, a ticket must be raised in the Kakapo portal to activate this setting at the system provider level, as it will impact all Unity clients. However, it can be set through the portal for a specific reseller, group or user. The below screenshot shows how to activate this setting for a user.



ABC User Branding Details

The Call Details Available setting specifies whether a user is permitted to view the details of another user's call, including th

The Monitored User Department setting is used when users can only monitor users of a specific department in the User Stat

Agents can be prevented from joining or leavcing all call centers that they are a member of, which overrides the setting on t

Unity updates can be controlled by specifying the version that is permitted to be downloaded and applied. This allows the us

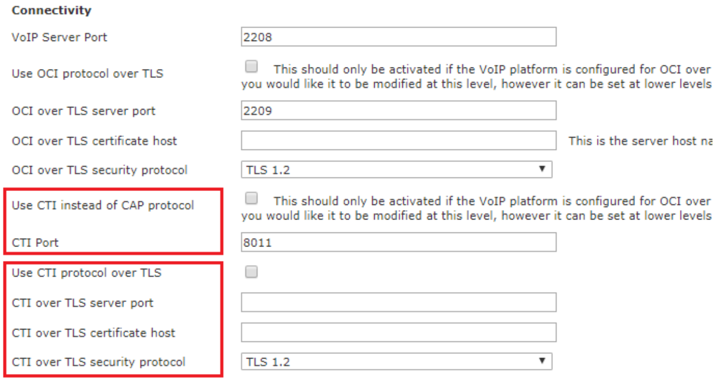
Connectivity

Use OCI protocol over TLS ☑ This setting should only be modified by an experienced VoIP engineer,

4.2 Configuring Unity to use CTI over CAP

As discussed, this setting only applies if Unity is connecting to BroadWorks release 21 (any service pack); CAP will be used for any release prior to R21 and CTI will be used for any later releases.

The below settings can be used to configure Unity to use CTI in place of CAP (BroadWorks R21 only) and whether to secure the CTI connection. The CTI Port is mandatory and will be set to 8011 by default. If the CTI server supports both unsecure and secure (TLS) connections, then the “CTI Port” value should be set as 8011 and the “CTI Over TLS Server Port” value should be 8012. However, if the server supports only CTI over TLS then both the “CTI Port” and “CTI Over TLS Server Port” should be set to 8012.

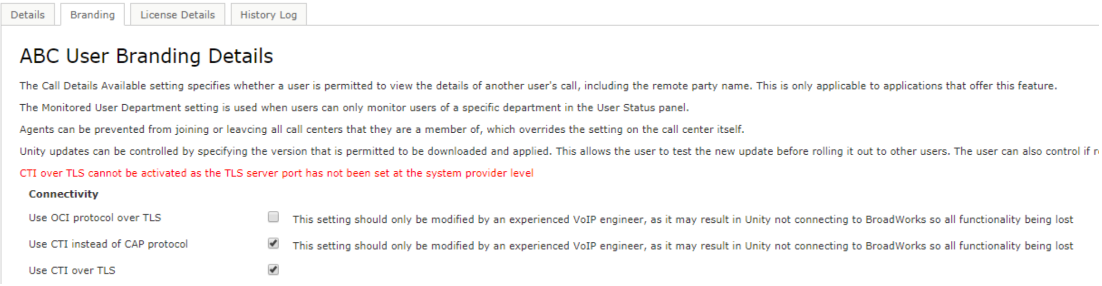


Connectivity

VoIP Server Port	2208
Use OCI protocol over TLS	☐ This should only be activated if the VoIP platform is configured for OCI over you would like it to be modified at this level, however it can be set at lower levels
OCI over TLS server port	2209
OCI over TLS certificate host	This is the server host na
OCI over TLS security protocol	TLS 1.2 ▾
Use CTI instead of CAP protocol	☐ This should only be activated if the VoIP platform is configured for OCI over you would like it to be modified at this level, however it can be set at lower levels
CTI Port	8011
Use CTI protocol over TLS	☐
CTI over TLS server port	
CTI over TLS certificate host	
CTI over TLS security protocol	TLS 1.2 ▾

Configuring CTI over TLS is similar to configuring OCI over TLS, in that the server port must be specified in order to active the feature at any level in the Kakapo portal hierarchy. As is the case with OCI, the server certificate can be set and the security protocol must be set.

The below screenshot shows configuring CTI at the user level, you can see the portal has not saved the changes because the CTI over TLS server port was not set at the system provider level.



ABC User Branding Details

The Call Details Available setting specifies whether a user is permitted to view the details of another user's call, including the remote party name. This is only applicable to applications that offer this feature.

The Monitored User Department setting is used when users can only monitor users of a specific department in the User Status panel.

Agents can be prevented from joining or leavcing all call centers that they are a member of, which overrides the setting on the call center itself.

Unity updates can be controlled by specifying the version that is permitted to be downloaded and applied. This allows the user to test the new update before rolling it out to other users. The user can also control if r

CTI over TLS cannot be activated as the TLS server port has not been set at the system provider level

Connectivity

Use OCI protocol over TLS ☐ This setting should only be modified by an experienced VoIP engineer, as it may result in Unity not connecting to BroadWorks so all functionality being lost

Use CTI instead of CAP protocol ☑ This setting should only be modified by an experienced VoIP engineer, as it may result in Unity not connecting to BroadWorks so all functionality being lost

Use CTI over TLS ☑

5 Troubleshooting

There are two common reasons why Unity is not able to connect to the BroadWorks platform using these protocols:

5.1 Firewall Access

If the customer firewall doesn’t allow outbound TCP/HTTPS connections to the relevant server then Unity will not be able to connect. This is especially relevant when introducing secure connectivity or the CTI protocol to an existing Unity business customer, either by changing settings in the Kakapo portal or by updating the BroadWorks platform to R22.

If updating the BroadWorks platform to R22 then the firewall for all existing Unity customer sites will need to be modified to allow TCP port 8011 traffic if CTI is unsecure, or another port (the default is 8012) if CTI over TLS is configured. This is because CAP is no longer supported so all clients will be forced to use CTI instead. The ConnectionLog.txt file in the Unity installation folder will help diagnose this issue, the resolution is to open the relevant firewall ports for outbound connections on the corporate firewall.

5.2 Incorrect Server Details

As mentioned above, when connecting to the CTI server Unity will use the FQDN set in the Kakapo portal branding settings, otherwise the same FQDN as the OCI server will be used, which is likely to fail because the OCI and CTI servers are usually separate physical servers with different FQDNs. Therefore, it is important to ensure the correct CTI server hostname is used when activating this connectivity feature.

Unity will first attempt to connect to BroadWorks on the server port specified through the branding response and will only attempt to secure the connection once it has been established. If the Broadworks server only supports secure connections using TLS, then the default server port must be set to the secure server port to make sure Unity can connect. If the default server port is not set to the secure port then Unity will not be able to connect to Broadworks, and the start-up procedure will stop immediately.

If the TLS certificate hostname is mismatched or the incorrect security protocol has been specified in the Kakapo portal, then securing the TCP connection may fail. In this case the server will sever the connection and Unity will alert the user that the connection failed. In most cases the TLS certificate hostname can be left blank, in which case Unity will assume the TLS certificate hostname is the same as the FQDN that Unity connected to (*.myserver.com) – if this is not the case then the TLS certificate must be set in the Kakapo portal.