KAKAPO SYSTEMS

Unity Client: BroadWorks Protocol Overview

This document outlines the 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 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.

1.1 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.

1.2 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, therefore if the OCI connection is secured with TLS then this will implicitly apply to the CAP connection as well.

1.3 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.

CTI is essentially the same as the XSI protocol, but over a 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. 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.

2 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.

2.1 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 the below section.

2.2 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 relevant settings in the Kakapo portal to connect to BroadWorks using CAP or CTI, in addition to OCI which is also used. 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.

2.3 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).

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.

3 Configurating Unity in the Kakapo Partner Portal

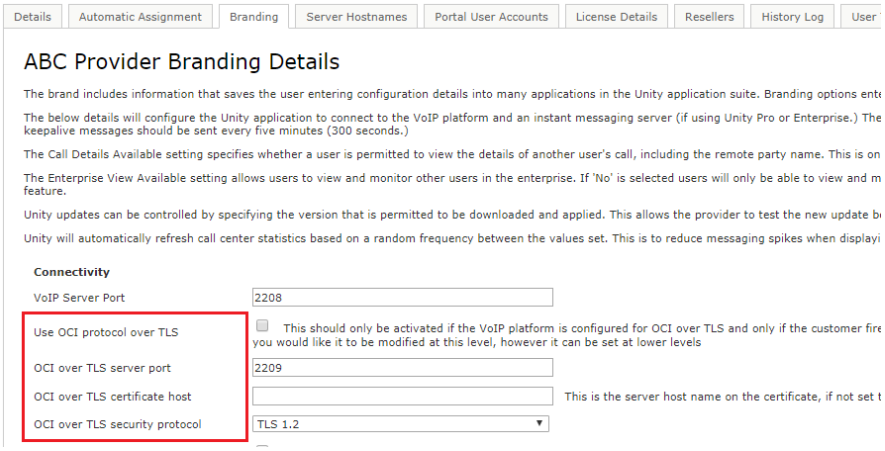
As mentioned above, Unity will utilize the above BroadWorks protocols depending on the BroadWorks platform that it has connected to and Kakapo portal settings, as outlined below.

3.1 Activating OCI over TLS

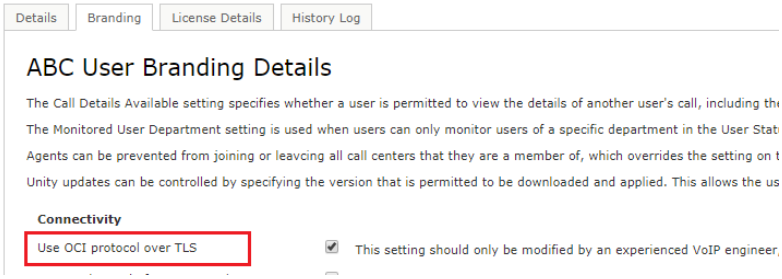
By default, the OCI protocol does not use TLS. Once this has been activated and tested on the BroadWorks OCI server it can be activated for use by Unity, as shown below.

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, the OCI over TLS server port should be kept blank.

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 security protocol as the OCI server will close the connection if the wrong one is used.



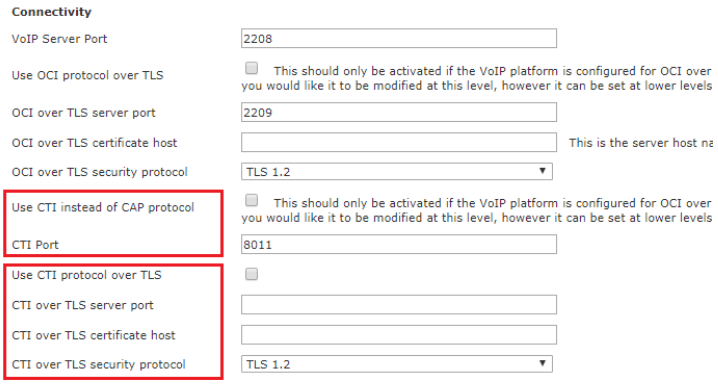
As with all branding settings, if this is changed then it will also update the same setting for all level below. Therefore, a ticket must be raised in the Kakapo portal to activate this setting at the provider level, as it will impact all Unity clients. However, it can be set through the portal for a specific reseller, group or user. The below screenshot shows how to activate this setting for a user.



3.2 Configuring Unity to use CTI over CAP

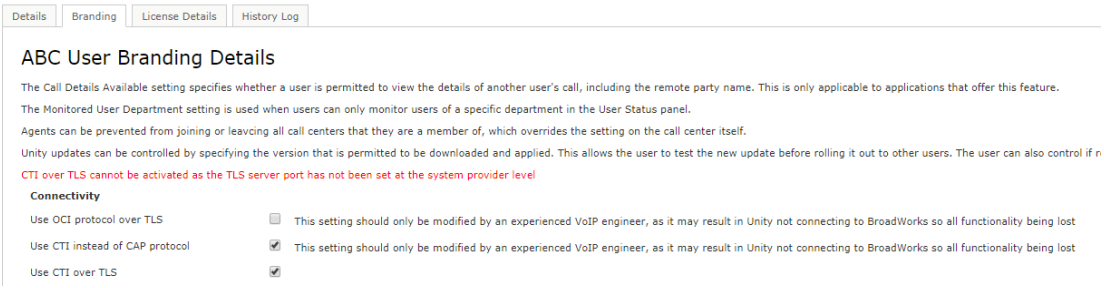
As discussed, this setting only applies if Unity is connecting to BroadWorks release 21 (any service pack); CAP will be used for any release prior to R21 and CTI will be used for any later releases.

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 (BroadWorks R21 and later). The CTI Port is mandatory and will be set to 8011 by default.



Configuring CTI over TLS is similar to configuring OCI over TLS, in that the server portal must be specified in order to active the feature at any level. The server certificate can be set, 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.



4 Troubleshooting

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

4.1 Firewall Access

If the customer firewall doesn't allow outbound TCP connections to the relevant BroadWorks 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 site will need to be configured to allow TCP port 8011 traffic if CTI is unsecure, or another port (the default is 8012) for CTI over TLS. 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.

4.2 Incorrect TLS Configuration

Unity will first attempt to connect to BroadWorks on the server port specified and will only attempt to secure the connection once it has been established. If the certificate hostname is mismatched or the incorrect security protocol has been specified in the Kakapo portal, then securing the connection may fail. In this case the server will sever the connection, Unity will not be able to communicate over a non-secure connection.