

Telstra Business Connect CGA Provisioning Guide

Conventions used in this guide



The following typographical conventions are used in this guide for simplicity and readability:

Web addresses, e-mail addresses and hyperlinks are shown in **bold italics**, for example

www.telstra.com.au

Button names and titles/features on your computer screen are shown in *italics*.

User input is shown in **bolded** font.

Telstra Business Connect, Provisioning Guide, July 2018

[©] Telstra Corporation Limited (ABN 33 051 775 556) 2013. All rights reserved.

This work is copyright. Apart from any use as permitted under the Copyright Act 1968, information contained within this manual cannot be used for any other purpose other than the purpose for which it was released. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the written permission of Telstra Corporation Limited.

Document purpose

This guide outlines the manual steps required for a CGA to configure a user to use Telstra Business Connect on their TIPT service. An automated tool is available for PC users that completes the steps contained within this document for one or more users at a time. It is available https://ucone.tipt.telstra.com/cga

Recommended settings

Provisioning a user

If you are using the Telstra Business Connect mobile or desktop clients, please refer to the Customer Detailed Integration Guide on the TIPT Online Resource Centre at https://www.telstra.com.au/business-enterprise/download/document/business-tipt-customer-detailed-integration-guide.pdf for required network settings.

Step 1: Ensure relevant services packs are assigned to a group and a user

When provisioning Telstra Business Connect for a user (Desktop and/or Mobile) ensure the TIPT Executive or Standard Pack v10 service packs are assigned to the group and the relevant service pack is assigned to the user.

Telstra Business Connect licences are not available in the Basic pack.

For users that have the Executive pack assigned to them, they also have the option of having the Telstra Business Connect iPad licence assigned to them. The BTBC v1 licence needs to be assigned to Executive pack users for them to be able to utilise the dedicated iPad Telstra Business Connect client.

Step 2.1: Adding shared call appearance (SCA)

The **Telstra Business Connect** client can be used as Primary Device or SCA on the TIPT primary number. The mobile Telstra Business Connect client and the Desktop client will require a Primary or SCA user each – additional SCA users must be created if the user requires both Telstra Business Connect clients.

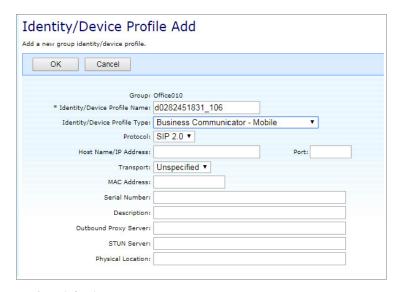
Each SCA is assigned appropriate *Identity/Device Profile Type:* either the Business Communicator – *Mobile*, Business Communicator – *Tablet* device or Business Communicator – *PC* device.

To add SCA

- 1. Login to Commpilot and search for the user.
- 2. Go back to the group level of the User.
- 3. Click on to the Resources and then Identity/Device Profiles.

If there are existing SCA's configured, ensure the next numeral in the number range is entered, i.e. [phone_number]_01, [phone_number]_02, [phone_number]_03

Provisioning a user



- 4. Search for the user.
- 5. Click on the user that requires Shared Call Appearance to be added.
- 6. From the Options menu.
- 7. Click on Call Control option.



Recommended settings

Provisioning a user

8. Click on the Shared Call Appearance.

Options:	Call Control	
Profile	Call Control	
Incoming Calls	Basic	Advanced
Outgoing Calls	Barge-in Exempt - On	BroadWorks Anywhere
Call Control	Block barge-in attempts from other users with Directed Call Pickup with Barge-in	Configure the fixed and mobile phones you would like to link to this account
Calling Plans	Call Waiting - On Answer a call while already on another call.	Hoteling Guest - Off Allows a user to associate their service profile with a host user and use the
Client Applications	Customer Originated Trace	Push to Talk
Messaging	Issue a trace to your service provider for your last incoming call by using a feature access code.	Make and selectively receive Push to Talk calls.
Utilities	Directed Call Pickup Pick up a call using a feature access code and an extension.	Remote Office - Off Use the full CommPilot Call Manager functionality from another phone.
	Diversion Inhibitor	Shared Call Appearance
	Inhibit the remote party's redirecting services	Display alternate calling identity/device profiles or lines assigned to you.
	Directed Call Pickup with Barge-in	
	Pick up or barge-in on a call using a feature access code and an extension.	

- 9. Check Allow Call Retrieve from another location.
- 10. Select Multiple Call Arrangement Off.



- 11. Click Add.
- 12. Enter the information detailed below to the **Shared Call Appearance Add** page. Be sure you add in the correct information for the device type.

For Mobile Clients

Field name	Field value		
Identity/Device Profile Name	New Identity/Device Profile (Group)		
Line/ Port	p[phone_number]_01		

Provisioning a user



13. Click OK.

For PC Clients

1. Add the Identity/Device Profile from the group level.

If there are existing SCA's configured, ensure another number is entered, i.e. [phone_number]_01, [phone_number]_02, [phone_number]_03.

It is irrelevant what number is used, so long as the number is unique and hasn't been used previously.



- 2. Select the Allow Call Retrieve from another location checkbox.
- 3. Select Multiple Call Arrangement Off.
- 4. Click Add.
- 5. Enter the information detailed below to the **Shared Call Appearance Add** page. Be sure you add in the correct information for the Identity/device type.

Provisioning a user



Field name	Field value	
Identity/Device Profile Name	New Identity/Device Profile (Group)	
Identity/Device Profile Type	Business Communicator – PC	

6. Click OK.

The SCA page will display the users you have just added, one for each client they will be using.



7. Click OK.

Provisioning a user

Step 2.2: Adding Telstra Business Connect as primary device (optional)

- 1. Go to the **Group Level** of the User.
- 2. Click on to Resources and then Identity/Device Profiles.
- 3. Add the Identity/Device Profile.

If there are SCA's configured, ensure unique number is entered in **Identity/Device Profile name**. It is irrelevant what number is used, so long as the number is unique and hasn't been used previously.

dentity/Device Profile Add						
dd a new group identity/device profile.						
OK Cancel						
Group:	Office010					
* Identity/Device Profile Name:	d0282451832					
Identity/Device Profile Type:	Business Communicator - PC	•				
Protocol:	SIP 2.0 ▼					
Host Name/IP Address:		Port:				
Transport:	Unspecified ▼					
MAC Address:						
Serial Number:						
Description:						
Outbound Proxy Server:						
STUN Server:						
Physical Location:						
-Authentication -						
 Use Identity/Device Profile Ty 	Use Identity/Device Profile Type Credentials					
Use Custom Credentials						
* Device Access User Name	2:					
* Device Access Password	d:					
* Re-type Device Access Password	d:					

- 4. Go to the User and Click on the Addresses.
- 5. Choose the Identity/Device Profile Radio Button.

Provisioning a user

6. Choose the right Identity/Profile Name, it was created earlier and add the unique Line/Port and click on Apply.

OK	Apply Cancel	
Phone Number	0282451832 ▼ Activated	
Extension	203	
Identity/Det	vice Profile Trunking None	
-Identity/De		
Identity/Dev	ce Profile Name: d0282451832 (Group)	T
	* Line/Port: p028451832	
diases: sip: 02	82451832@digitalbusiness	
sip:		digitalbusiness ▼
sip:		
sin		@ digitalbusiness ▼
sip:		

7. Click on Configure Identity/Device Profile in Addresses.

Phone Number: 0282451832 ▼ Activated					
Extension: 203					
Identity/Device Profile					
Identity/Device Profile Name:	D0282451832 (Group)	Y	Configure Identity/Device Profile		
* Line/Port: p0282451832 @ digitalbusiness ▼ AdvancedSettings					
!					

Provisioning a user

8. Under Authentication, choose Use Customer Credentials.

dify or delete an existing group identity, aved	device pror	ile.					
OK Apply D	elete	Canc	el				
Profile			User	s			
Identity/Device Profile Name: D							
Identity/Device Profile Type: B Device Type URL: ht				a com:443/c	lms/uc-one	/pc/	
Device Type OKE. III		ingicalous	illessiteisti.	a.com: 440/c	inis, de one,	pu	
Protocol:	SIP 2.0 ▼						
Host Name/IP Address:					Port:		
Transport:	Jnspecifie	d ▼					
MAC Address:			1				
Serial Number:			J				
Description:						_	
Outbound Proxy Server:						-	
STUN Server:							
Physical Location:	1000000000000						
Lines/Ports: U Assigned Lines/Ports: 1	nlimited						
Unassigned Lines/Ports: U	nlimited						
Version:							_
-Authentication -							7
Use Identity/Device Profile Ty	pe Credentia	els					Ш
Use Custom Credentials	222245						Ш
* Device Access User Name		1832					Ш
* Device Access Password							. 11

Provisioning a user

Step 3: Setting device passwords for the SCA users

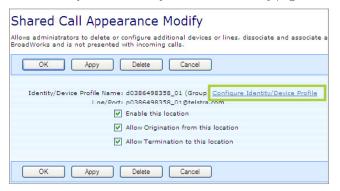
1. Following on from the steps above click **Edit** Business Communicator **Mobile** from Shared Call Appearance screen.

Delete	Identity/Device Profile Type	Identity/Device Profile Name_	Line/Port_
	Business Communicator - Mobile	d0282451831_102 (Group)	p0282451831_102@di
	Business Communicator - PC	d0282451831_104 (Group)	p0282451831_104@di
	Business Communicator - Tablet	d0282451831_103 (Group)	p0282451831_103@di

Note: This step has to be repeated for each SCA user created as a part of provisioning Telstra Business Connect client(s), i.e. Mobile, Tablet and PC client.

2. Click Configure Identity/Device Profile.

This will take you to the Identity/Device Profile Modify page.



Provisioning a user

3. In the Authentication section select Use Custom Credentials and enter the Device Access User name and Password.

The username corresponds to the SCA username.

The default authentication password is the web access password.

The "Device authentication user" is automatically updated by Broadworks.

Profile	Configure	Users	Files	Custom Tags	
Identity/Device Profile Name: Identity/Device Profile Type: Device Type URL:		om: 443/dms/uc-one/mobile/			
Protocol:	SIP 2.0 ▼				
Host Name/IP Address:		Port:			
Transport:	Unspecified				
MAC Address:					
Serial Number:					
Description:					
Outbound Proxy Server:					
STUN Server:					
Physical Location:					
Lines/Ports: Assigned Lines/Ports:	1				
* Device Access Passw * Re-type Device Access Passw	Type Credentials me: 0386320416@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx				
OK Apply	Delete Cancel				

- 4. Click Apply and OK.
- 5. Repeat the above steps 1-4 above for the Business Communicator-PC SCA configuration.

Conventions used in this guide Document purpose

Provisioning a user

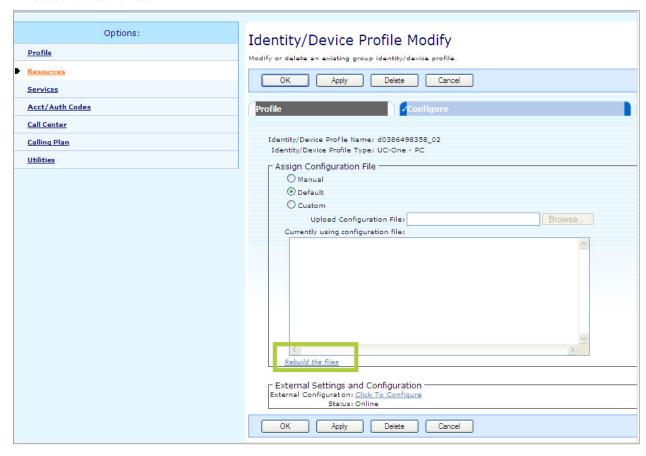
- Step 1: Ensure relevant services packs are assigned to a group and a user
- Step 2.1: Adding shared call appearance (SCA)
- Step 2.2: Adding Telstra Business Connect as primary device (optional)
- Step 3: Setting device passwords for the SCA users
- Step 4: Rebuilding configuration files

Recommended settings

Provisioning a user

Step 4: Rebuilding configuration files

- 1. Click on the **Configure** tab.
- 2. Select Rebuild the files.



- 3. Click OK.
- 4. Repeat this step to rebuild the files for the Business Communicator desktop device type created.

Conventions used in this guide

Document purpose

Provisioning a user

- Step 1: Ensure relevant services packs are assigned to a group and a user
- Step 2.1: Adding shared call appearance (SCA)
- Step 2.2: Adding Telstra Business Connect as primary device (optional)
- Step 3: Setting device passwords for the SCA users
- Step 4: Rebuilding configuration files

Recommended settings

Recommended settings

The Telstra Business Connect client supports the following TIPT features. These services can be turned on or off using the preferences window.

- Changing any of the recommended settings may impact expected functionality.
- Settings can be configured on you mobile device or configured in Commpilot.
- The following table lists recommended settings and how to configure the settings on your iOS or Android mobile client.
- When setting up your initial settings prior to making a call, it is recommended that the Always Ask option is selected from your Settings>Call Settings field.
- For Android users the "Enable video calls" setting should also be enabled to be able to view video calls. The following settings are recommended for initial setup in the Mobile client.

Changing the recommended settings may impact the expected performance.

Setting	Telstra Business Connect Client	Reason for setting
Call Forwarding No Answer	On	If you can't answer the call on your TIPT desk phone the call will arrive at the configured number after the set number of rings
Call Forwarding Always	Off	If turned on the call will not go to the client, as calls will always be diverted to the configured number
Do Not Disturb	Off	If you turn Do Not Disturb on, calls will not arrive on your Telstra Business Connect client
Remote Office	Off	If you turn Remote Office On with your mobile number configured as the remote device, calls made to your TIPT desk phone will arrive at your mobile, not your Telstra Business Connect client
TIPT Anywhere	Feature can be On, Enabled location — Off	If you turn TIPT Anywhere On and you have your mobile number listed as a location, both your mobile and the Telstra Business Connect client will ring at the same time when a call arrives through the Telstra Business Connect client. So this does not happen you must have TIPT Anywhere mobile location disabled
Simultaneous Ring Personal	Off	If you have your mobile number in your Simultaneous Ring list, both your mobile and the Telstra Business Connect client will ring at the same time when a call arrives through the Telstra Business Connect client if this features is turned On

Conventions used in this guide

Document purpose

Provisioning a user

- Step 1: Ensure relevant services packs are assigned to a group and a user
- Step 2.1: Adding shared call appearance (SCA)
- Step 2.2: Adding Telstra Business Connect as primary device (optional)
- Step 3: Setting device passwords for the SCA users
- Step 4: Rebuilding configuration files

Recommended settings

Recommended settings

The following User settings are recommended for initial setup in Commpilot.

Setting	Compilot	Reason for setting
Connected Line Identification Restriction	On*	
External Calling Line ID Delivery	On*	
Internal Calling Line ID Delivery	On*	
Call Waiting	Off	If turned on, it will affect the active call and place it on hold automatically. This is default behaviour of your mobile device not Telstra Business Connect.

^{*} Note: If you don't want your CLID name and number to be displayed ensure Internal and External Calling Line ID Delivery is turned Off.