*** This guide is aimed at both End User and Technical Support audiences ***

Overview

This document is an overview of the steps required during a Disaster Recovery scenario to enable Contact Centre Agents to connect to the Marshalls RDS Web Gateway and use the Finesse Remote Agent facility to take Contact Centre calls at a remote location (e.g. home).

IS Department/Technical Support – See the rear of this document for actions that MUST be taken prior to instructing end users to follow this guide during a Disaster Recovery scenario.

Requirements & Pre-requisites

Internet Access – You must have internet connectivity, preferably via a high speed connection.

Note: Whilst lower-speed connections will not preclude these systems from working, they may seriously affect your productivity and ultimately you may lose connectivity or suffer adverse effects.

PC – This can be ANY internet connected PC (e.g. a home/family PC) running Internet Explorer.

Note: This system does not work using Chrome, Edge or any other internet browser.

Contact Centre Agent ID, Password and a Remote Agent Extension – The Agent ID and password are those that you use every day to log in to the Contact Centre.

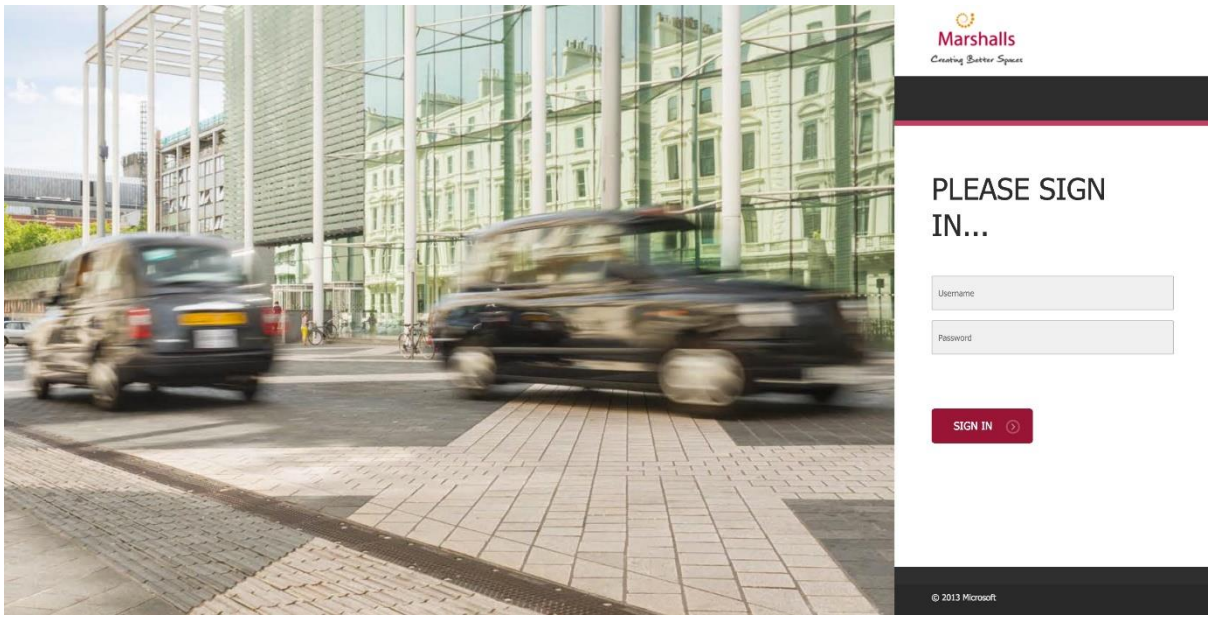
Note: A Remote Agent Extension will be assigned to you by your Team Leader, DR Co-ordinator or the Business Process Development Team.

Telephone – Access to either a mobile or a land line telephone is required, this is the line you will use to receive calls from customers. Your Team Leader will ask you for the number of the telephone you wish to use, the same telephone will also be used to verify that you are authorised to use the DR Published Desktop resource during the log in process.

Note: It is advised that any voicemail features on the designated mobile or landline telephone are turned off.

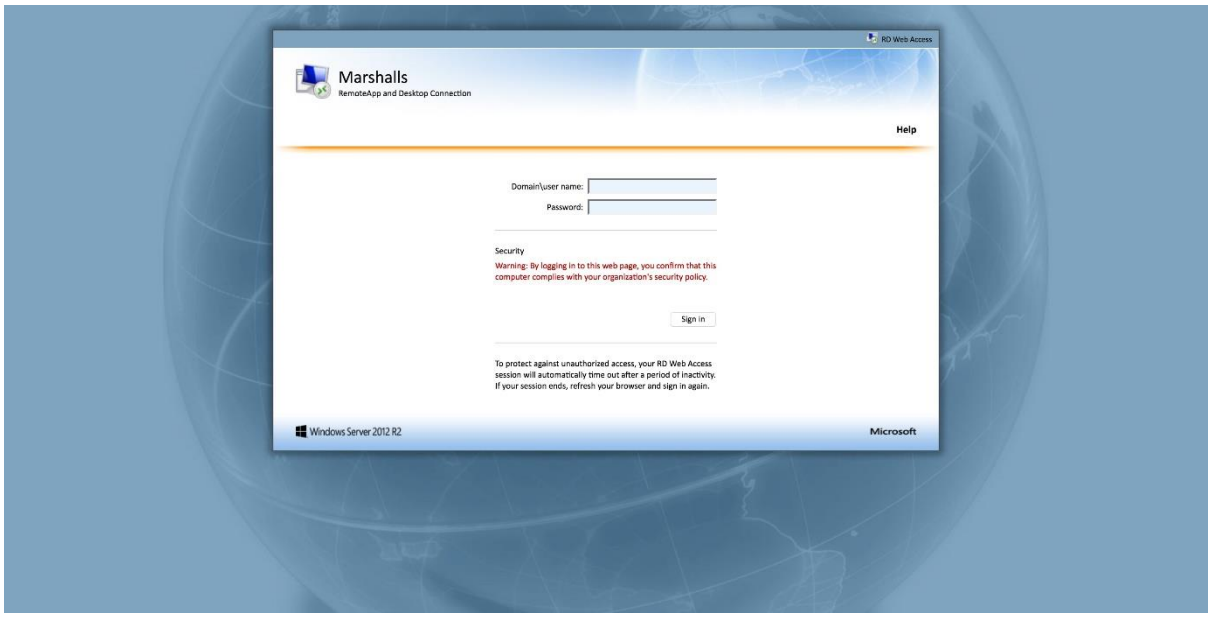
Procedure

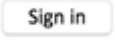
1. Using Internet Explorer, navigate to https://rdsgateway.marshalls.co.uk/rdweb. This will take you to the Marshalls connection security page:



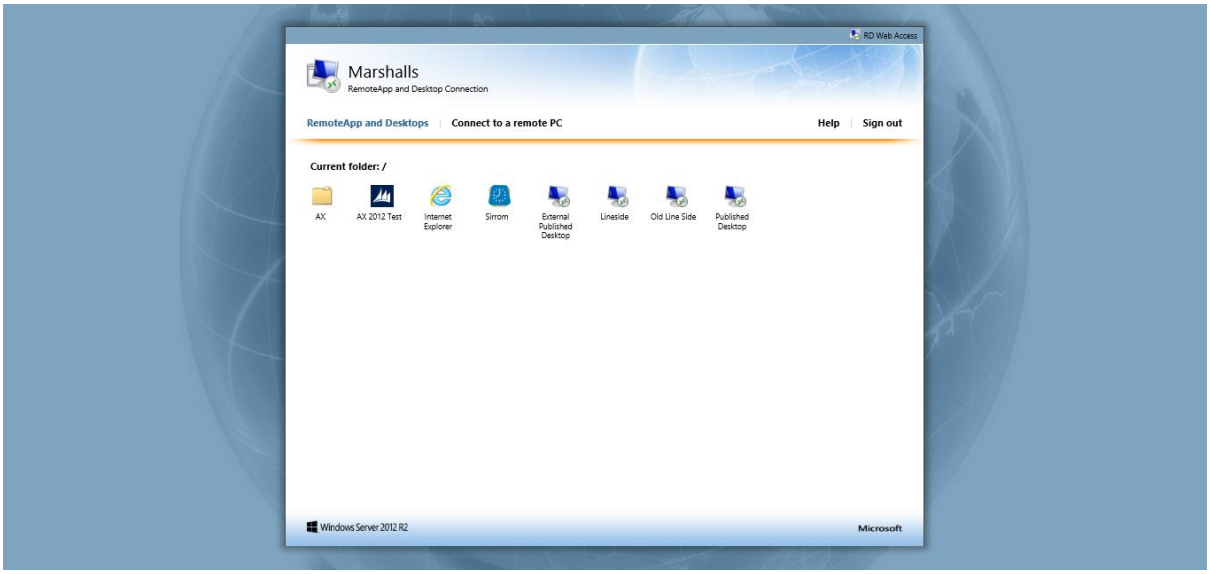
Enter your network credentials (do not use the NTSERVERS\ prefix) and click 

2. This will take you to the Gateway Login page:



Enter your network credentials (this time you need the NTSERVERS\ prefix) and click 

3. This will take you to the Remote App & Desktops page:



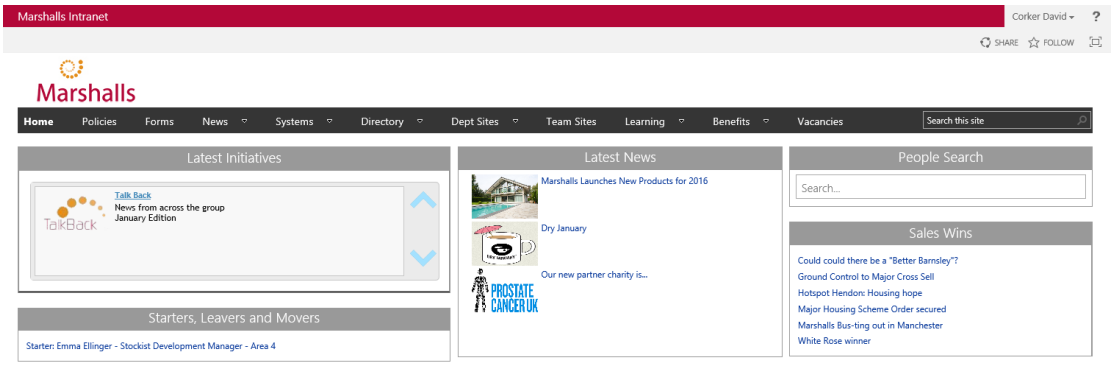
Click on the icon labelled 'External Published Desktop'. If prompted, click 'continue' when asked to '…make sure that you trust the publisher before you continue'.

When prompted, enter your network credentials (this time you need the NTSERVERS\ prefix).

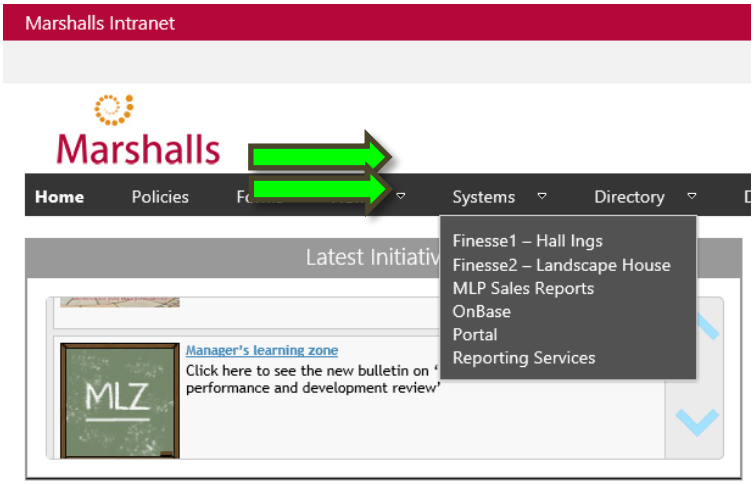
You will now receive a call on your designated telephone asking to you to 'please press the pound key to complete verification' – Press the '#' key on your telephone keypad. You should receive a message confirming that the verification has been successful. Hang up.

After a short period you will be presented with a Marshalls Windows desktop. You are now remotely connected and can use a subset of core applications just the same as you would if logged on in the office.

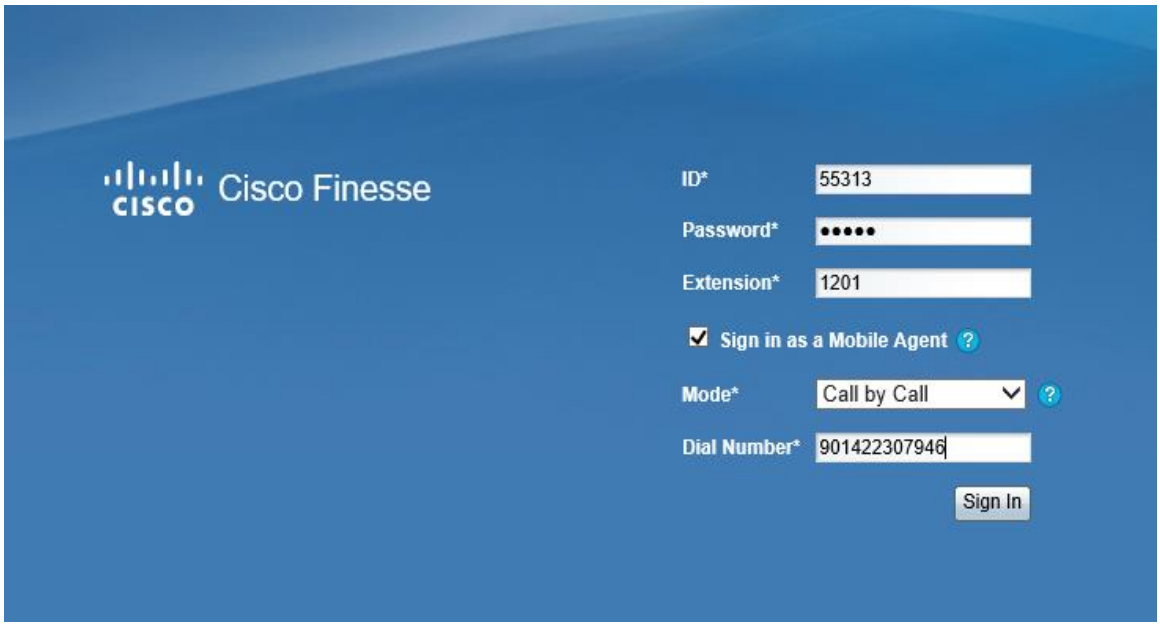
4. Once the Published Desktop has loaded, start Internet Explorer, this will load the Marshalls Intranet page by default:



5. From the Systems menu on the Marshalls Intranet homepage, select either of the Finesse links:

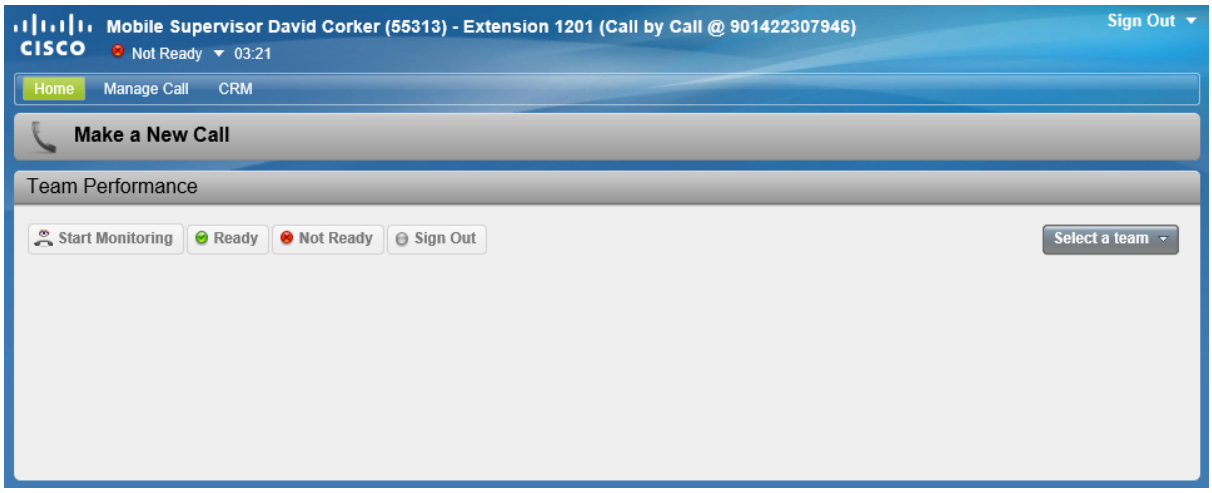


6. This will take you to the Finesse Login page:



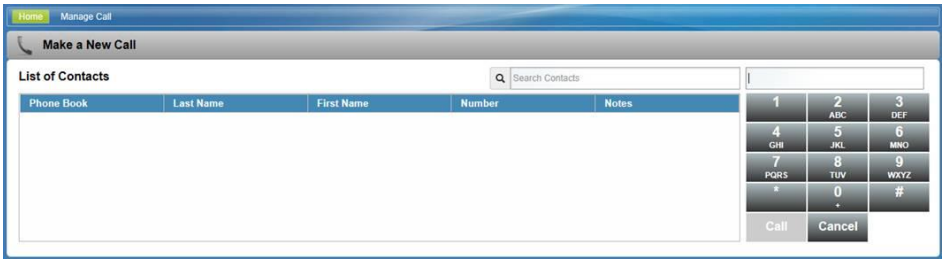
Enter your Agent ID, Password and the Remote Agent Extension provided by your Team Leader.
Tick the box adjacent to 'Sign in as a Mobile Agent'
Select the default mode of 'Call by Call'
Enter your Mobile/Landline number (with a 9 prefix) in the box labelled 'Dial Number' then click 'Sign In'.

7. This will log you into the Finesse system:



You will see that Finesse is aware that you are a Mobile Agent/Supervisor and what number you can be reached on.

8. From this point on, Finesse will work as normal – move to the Ready state and, when a customer calls, your Agent will be reserved, the telephone will make a call to your number and then connect you to the customer.
9. To make calls and to stop your home or mobile number being divulged you need to click the tab “Make a new call” in finesse. Add a 9 for external or dial the extension number. Finesse will ring your home or mobile and then put you through to the destination you requested. Marshall then pick up all costs and your numbers will not be seen by anybody else.



Caveats

Using the Finesse Remote Agent has some limitations:

Call Recording (Calabrio) – Calabrio relies on the Agent endpoint telephone being an IP phone directly connected to a Marshalls PC, within the Marshalls network. Since this is not the case, calls to Remote Agents will not be recorded.

Voicemail/Answerphones – If the mobile/landline you are using to receive calls has a voicemail/answerphone service then this needs to be switched off. If this is not done, there is a risk that Customer calls may be sent to your voicemail/answerphone.

IS Department/Technical Support

The following MUST be carried out for each Agent/Customer before they are able to take advantage of the Remote Agent facility…

- Add the user to the 'External_PD_Users' Active Directory group.
- The user designated remote telephone phone number must be added to the relevant field within the user entry on the Azure Multi Factor Authentication Server so that the user receives a call to verify their identity to allow them access to an 'External Published Desktop'.
  Tip: Ask the relevant Team Leader/Manager to supply a remote agent list and remote/temporary telephone numbers for each remote agent.
  Tip: Azuremfa > Open Multi Factor Authentication Application > Users > Import from AD > Find User > Country Code 'United Kingdom' > Insert Number > Apply
- Contact Centre/HDS1 or 2: The Agent Desk Settings for the relevant team must be enabled for 'Cisco Unified Mobile Agent' AND 'Call by Call' mobile agent mode. See a member of the Networks/Telephony team to enable.
  Tip: b-lsh-hds2 (or 1) > Administration Tools > List Tools > Agent Desk Setting List > Retrieve > <Select TEAM> > Enable Cisco Unified Mobile Agent > Mobile Agent Mode > Call by Call.
- From the range of available Remote Agent Extensions - 1201 to 1260 - distribute the appropriate number of extensions to the relevant Team Leader/DR Co-coordinator to satisfy the DR requirements of their team/site.
- Post DR - PUT EVERYTHING BACK AS IT WAS!