

|  |
| --- |
| Avaya IX Workplace on iPhone iOS |
|  |

# 

# 

# Document Control

|  |  |
| --- | --- |
| **Document Title:** | Avaya IX Workplace on iPhone iOS |
| **Security Classification:** | Confidential |
| **Author:** | Paul Hrynkiw |
| **Date:** | March 2020 Update November 2022 for Avaya v10 |
| **Version:** | 1.1 |
| **Distribution:** | IPI Engineering / Customer IT |

|  |
| --- |
|  |
|  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | **Head Office / Registered Address**  IP Integration Ltd  Integration House  Turnhams Green Business Park  Pincents Lane  Reading  RG31 4UH  **T** 0118 918 4600  **F** 0118 918 4601 | **Manchester Office**  IP Integration Ltd  Holyoake House  Hanover Street  Manchester  M60 0AS  **T** 0161 241 9600  **F** 0161 241 9601 | **Philippines Office**  IP Integration Ltd  Level 26-a Rufino Pacific Tower  6784 Ayala Avenue  Makati City  Metro Manila  Philippines | | **Registered No.** 4210561 **VAT No.** 792 4208 19 | | | |  |  | | --- | | http://www.technica.nl/sites/default/files/Technica_MicrosoftgoldCertpartner.gif |   FS 557052 EMS 564375 IS 564376 |  |  |

# Overview

The Avaya Workplace application can be used remotely over the internet as your desk extension on iOS (Apple) devices.

# security

Avaya Workplace uses Mutual Transport Layer Security (TLS 1.2) to encrypt the VoIP Signalling traffic between the remote worker device and the core of the Avaya solution within Moorcroft premises / Data Centre.

Audio traffic is encrypted using Secure Real Time Protocol using Advanced Encryption Standard (AES) with 256-bit keys.

An Identity certificate is downloaded to the device during setup, which requires a password. The Identity certificate has a 2-year expiry and current certificate remoteworker730d.p12 expires 21/11/2024. IPI Support will update the certificate as part of release management of the solution.

User will log into the application using their Active Directory (AD) Windows password as they would log onto their Desktop/PC.

# Process

Below are the steps required to install and configure the Avaya Workplace application used as a Remote Worker via the internet.

# Note – All screen shots are taken from an Apple iPhone with iOS 16.

1. Install Avaya Workplace application from iOS App Store
2. Install Avaya System Manager Root Certificate into Device (only applies to new devices)
3. Configure Avaya Workplace Web Address for Auto Configuration
4. Enter Client Certificate password

Configuration & Registration now complete

# Install Avaya Workplace application

Install Avaya Workplace on iOS

Search ‘Avaya Workplace’ in the App Stores

Install the App and Accept the License Agreement

Graphical user interface, text

Description automatically generated

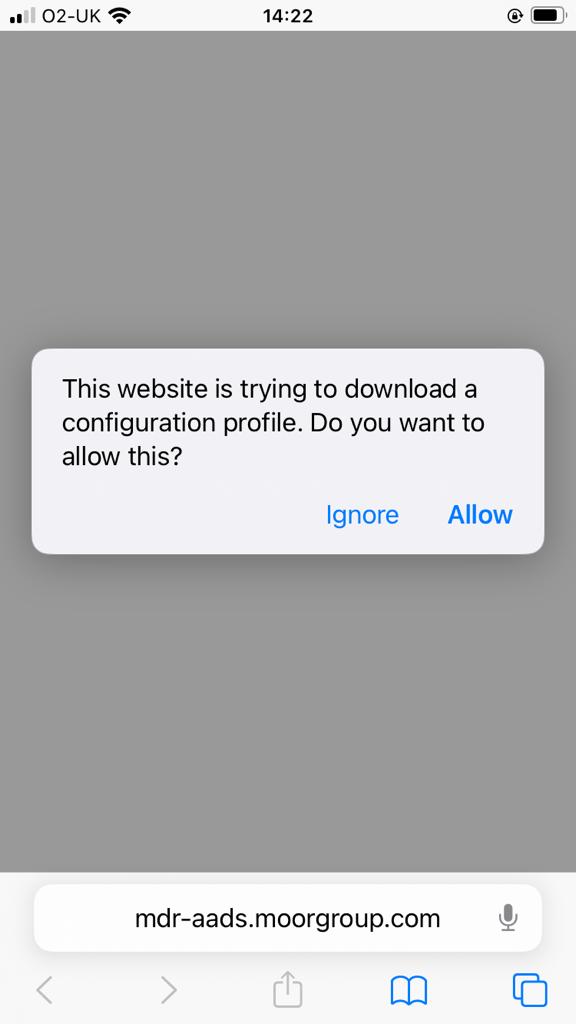
# Install Avaya System Manager Root Certificate

# Note – This only applies to new devices that have not previously been registered to the existing Remote Worker setup. If the device has previously been registered this section can be skipped.

From the iOS device browse to:

<https://mdr-aads.moorgroup.com:8443/SMGRCA.cer>

Press ‘Allow’ to download the Root Certificate



Confirmation will pop up to show the Certificate has been downloaded to Profile

Graphical user interface, text, application, chat or text message

Description automatically generated

Next from Settings > press ‘Profile Downloaded’

Graphical user interface, text, application

Description automatically generated

Press ‘System Manager CA’

Graphical user interface, text, application, chat or text message

Description automatically generated

Press ‘Install’ then you may be asked to enter your phone password (if asked)

Graphical user interface, text, application, chat or text message

Description automatically generated

Press ‘Install’ again

Graphical user interface, text, application, chat or text message

Description automatically generated

Then ‘Install’ a last time

Graphical user interface, text, application, chat or text message

Description automatically generated

The Certificate will now show as ‘Verified’

Graphical user interface, text, application, chat or text message

Description automatically generated

Now go to Settings > General > About > ‘Certificate Trust Settings’

Graphical user interface, application

Description automatically generated

Toggle the switch to on for ‘System Manager CA’ and press ‘Continue’ when the ‘Root Certificate’ pop-up is seen

Graphical user interface, text, application, chat or text message

Description automatically generated

# Configure avaya workplace

Launch Avaya Workplace

Press ‘Configure Account’

Graphical user interface, text, application, chat or text message

Description automatically generated

Press the cog icon and select ‘Use a web address’

Graphical user interface, text, application, chat or text message

Description automatically generated

Enter the following Web Address

<https://mdr-aads.moorgroup.com:8443/acs/resources/configurations?>

Graphical user interface, text, application, chat or text message

Description automatically generated

Next you will be asked to enter Workplace Credentials, this is your Moorcroft domain account and Windows password

Example:

Username : [joebloggs@moorgroup.com](mailto:joebloggs@moorgroup.com)

Password : Windows Domain password

Graphical user interface, text, application, chat or text message

Description automatically generated

If credentials are successful, you will logged in

# Note – the Remote Worker application should not be used to make Emergency Calls.

There will be a Quick Tutorial, which can be read or choose to skip

Graphical user interface, application, Teams

Description automatically generated

You will notice a red warning triangle.

Press ‘Client certificate credentials required’

Graphical user interface, application

Description automatically generated

Enter the password sent by your System Administrator

Graphical user interface, text, application, chat or text message

Description automatically generated

App has logged in successfully, no errors in top bar should be seen

Graphical user interface, application, Teams

Description automatically generated

Expiry on Identity Certificate is **21/11/2024**

To renew expiring certificate, contact IPI to regenerate the Identity then steps 3 & 4 will need to be completed to update Identity certificate on devices.

IPI will also hold this expiry in Release Management document and reviewed periodically.