MaaS360 MEG 3.0 Migration plan

Prasad BALASUBRAMANIAN
Product Manager

Prateek FULZELE
Engineering Manager

Juan ACOSTA
System Architect

Eamonn O'MAHONY
Advisory Technical Client Success Manager

Ciaran DARCY
Client Success Manager

Agenda

- Are you impacted?
- Why MEG 3.0? Benefits
- Prepare and test changes
- Advanced configuration / Follow-up

Agenda

- *Are you impacted?*
- Why MEG 3.0? Benefits
- Prepare and test changes
- Advanced configuration / Follow-up

Customers impacted by the change

Not impacted

- ✗ Only Android or Windows devices
- ✗ Customers with iOS devices not using Mobile Enterprise Gateway
- ✗ Customers with iOS devices not using Secure Browser
- ✗ Customers with licence bundles who do not include Secure Browser and Gateway for Browser / Gateway for Apps

Impacted

Customers with <u>all</u> of these elements:

- ✓ iOS devices
- ✓ MaaS360 contract with licence including Secure Browser and Gateway for Browser
- ✓ MaaS360 Secure Browser installed on iOS devices
- ✓ Using Mobile Enterprise Gateway to retrieve web content

Agenda

- Are you impacted?
- *Why MEG 3.0? Benefits*
- Prepare and test changes
- Advanced configuration / Follow-up

Apple UI Web View vs. WK Web View

UI Web View

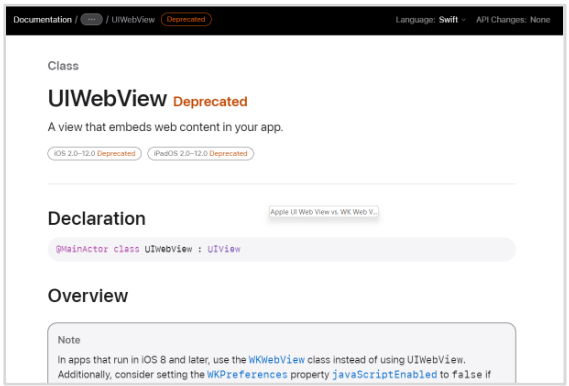
- Web browser technology used by Apple to show browser content in an app

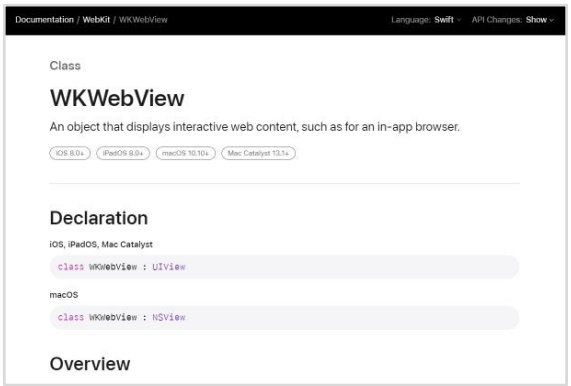
WK Web View

- New web browser technology used by Apple to replace UI Web View

MaaS360 Secure Browser

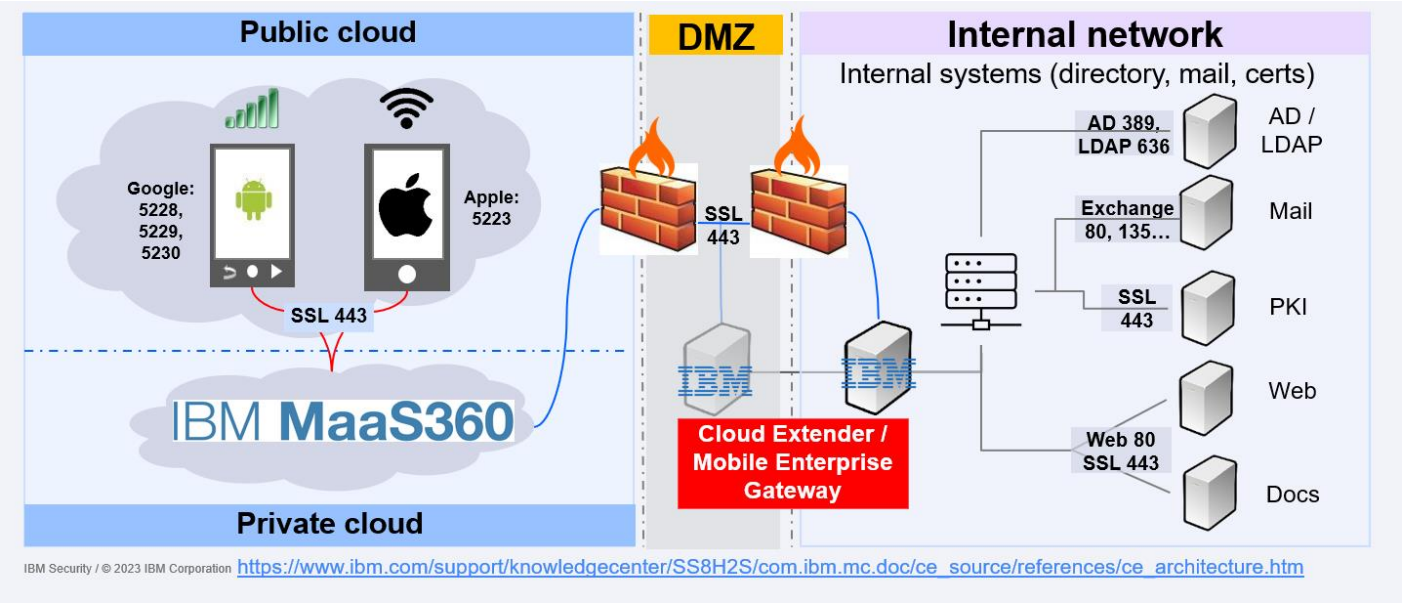
- Browser software developed by IBM for iOS and Android devices





https://developer.apple.com/documentation/uikit/uiwebview

New software support in MaaS360

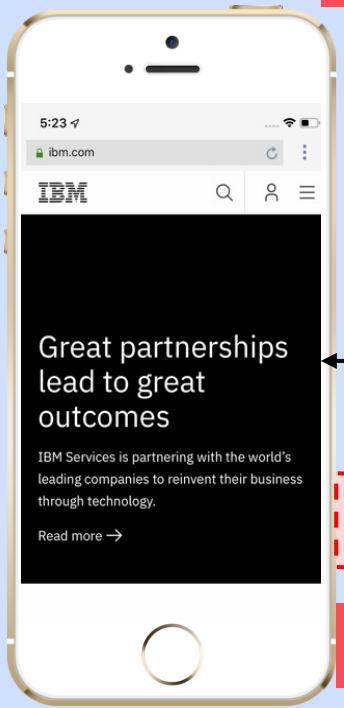


- Mobile Enterprise Gateway (MEG) connections have been re-designed
- Now we will use a VPN profile to connect to MEG
- When switching over the user is asked to accept installation of VPN profile

New approach for iOS / Secure Browser: VPN connection

Mobile device and apps

- iOS device (iPhone, iPad)
- MaaS360 core app
- MaaS360 Secure Browser
- MaaS360 MDM profile
- MaaS360 VPN profile



MEG Relay mode

DMZ

IBM MaaS360

Internal network

Cloud Extender / Mobile Enterprise Gateway

VPN

MEG Direct mode

Web and Content servers

MEG 3.0 – Improved performance

- Re-built specially for iOS devices
- MaaS360 Secure Browser “calls” the VPN connection
- Web pages render up to 20% faster
- Can work without MDM profile (MAM approach)
- Minimal configuration changes are needed to try out this newer service

Please see Appendix for further information about why these changes are being made

Agenda

- Are you impacted?
- Why MEG 3.0? Benefits
- *Prepare and test changes*
- Advanced configuration / Follow-up

Preparing for changes

Please ensure all software and network changes below are complete, or connections will not work

Device

- iOS 10.0+
- MaaS360 for iOS 10.0+
- Secure Browser for iOS 10.0+

Cloud Extender

- Minimum 2.105.200, current available 3.00.001 (see link 1 below)

Workplace policy settings

Configure allowed URL's to use MEG 3.0

Mobile Enterprise Gateway network requirements: see link no. 2 below

MEG 3.0 network requirements: see link no. 3

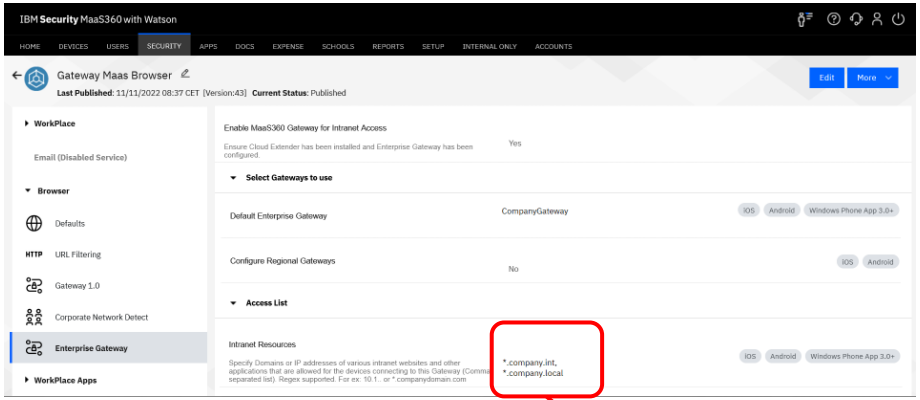
Documentation

1. MaaS360 System Requirements: https://www.ibm.com/docs/en/maas360?topic=saas-maas360-platform-system-requirements
2. Cloud Extender / MEG requirements: https://www.ibm.com/docs/en/maas360?topic=modules-mobile-enterprise-gateway-meg-module
3. MEG 3.0 requirements: https://www.ibm.com/docs/en/maas360?topic=megmsaw-enabling-mobile-enterprise-gateway-meg-support-apple-wkwebview

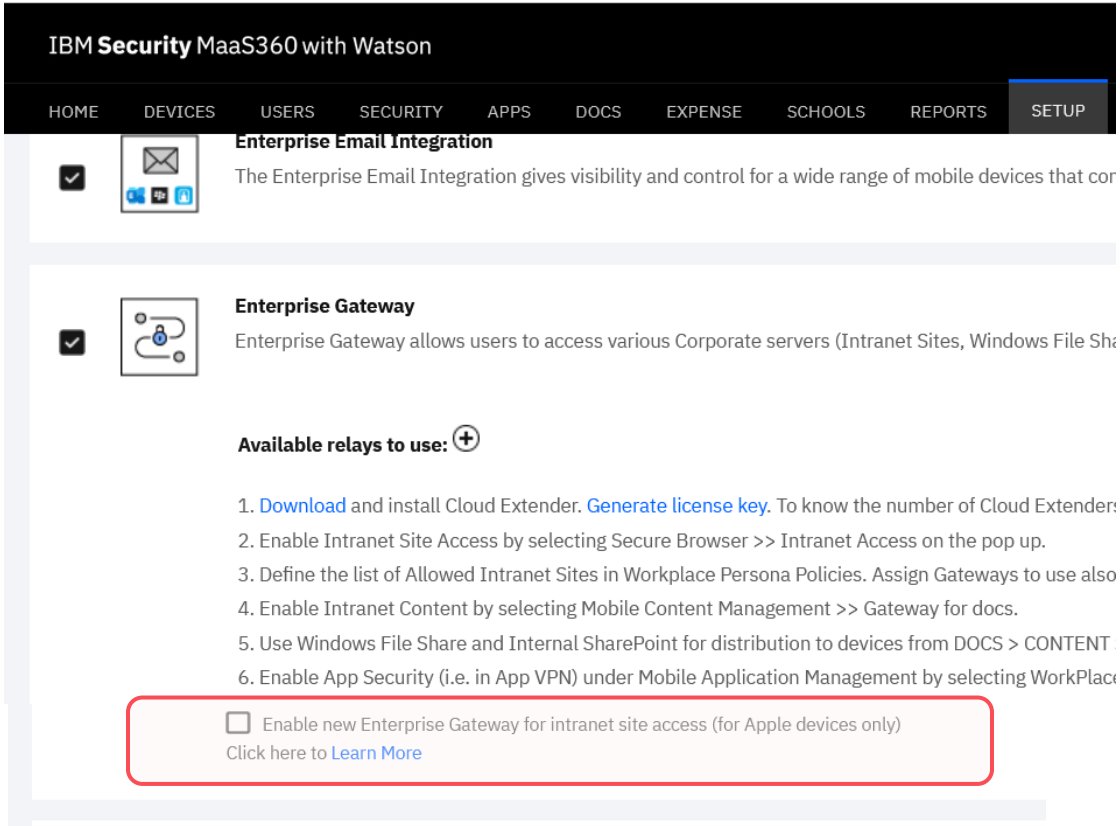
Configuration changes required?

Workplace policy – review settings – no change required

- Review existing MEG configuration in Workplace policy
- Browser > Enterprise Gateway settings

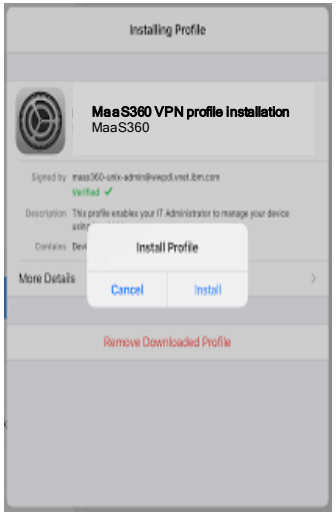


Switch on MEG 3.0



- Setup > Services
- Under Enterprise Gateway, find the section “Enable new Enterprise Gateway for intranet site access (for Apple devices only)”
- If not already checked, check the box, enter admin password, and click Submit
- Reopen Services page and verify this is now switched on

Set up your MEG 3.0 VPN configuration



User prompt: accept installation of VPN profile

- Accept > VPN configuration installed on device
- Don't accept > device will continue to prompt each time Secure Browser is opened
- VPN profile installation must be complete after switch-over date (connection will not work otherwise)

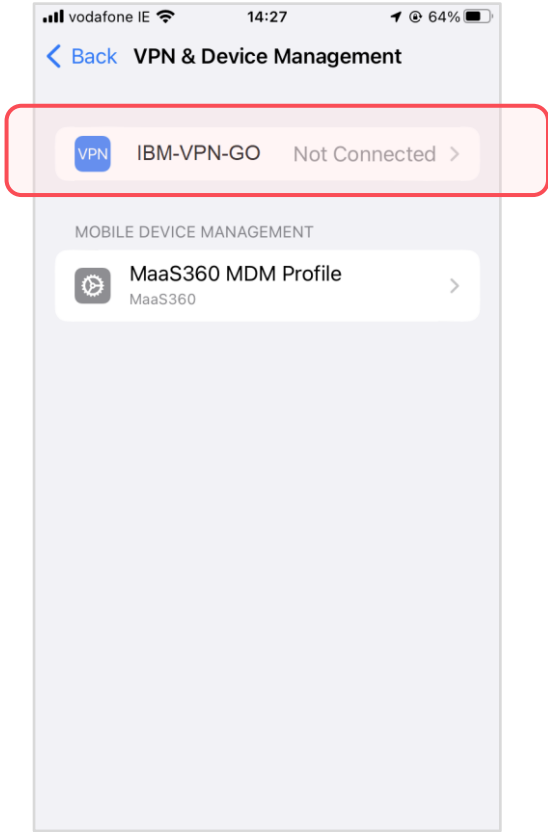
Test and confirm

Verify on device

- Confirm VPN profile installed: Settings > General > VPN & Device Management
- Verify whether VPN profile has been installed
- Open Secure Browser and try to launch one of your internal websites
- Success: now working correctly
- Not working: please report to Support for investigation

Once confirmed working

- Make changes in production device policies
- If necessary test for a small group of devices
- Confirm all functioning



Agenda

- Are you impacted?
- Why MEG 3.0? Benefits
- Prepare and test changes
- *Advanced configuration / Follow-up*

New features coming soon

– Per-App VPN configuration is coming soon!

– Please watch out on Community for when this is announced

– Will help customers who want to use multiple VPN profiles on same device

By when should we complete this?

- We are working towards a cut-over date
- We would encourage you to get started on your implementation
- We do not know when Apple will confirm the switch-over on their side meaning that the old technology will stop working at some point

How we can help

- Checklist to help you complete this step-by-step*
- Technical documentation and training*
- If further issues appear please contact Support

Checklist

Step	Item	Status
1	Is MEG v3 VPN already enabled? - If checkbox is available, please proceed to perform checks below to prepare. - If checkbox is not available, and you want to have it available, please contact Support to request “Enable Mobile Enterprise Gateway v3” - If checkbox is already checked, please proceed to make checks below to make sure all is correct and all devices will work correctly.	
2	Plan rollout timetable	
3	Verify whether working in Relay or Direct mode	
4	Checks - Relay mode customers ONLY	
5	Checks - Direct mode customers ONLY	
6	Update CE/MEG software versions	
7	Update iOS version on devices	
8	Update MaaS360 software versions on devices	
9	Test devices – make sure MEG v3 VPN is configured on devices and working	
10	Issues: please raise a ticket with Support	

* Please consult Appendix

Questions?

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube.com/ibmsecurity

Checklist

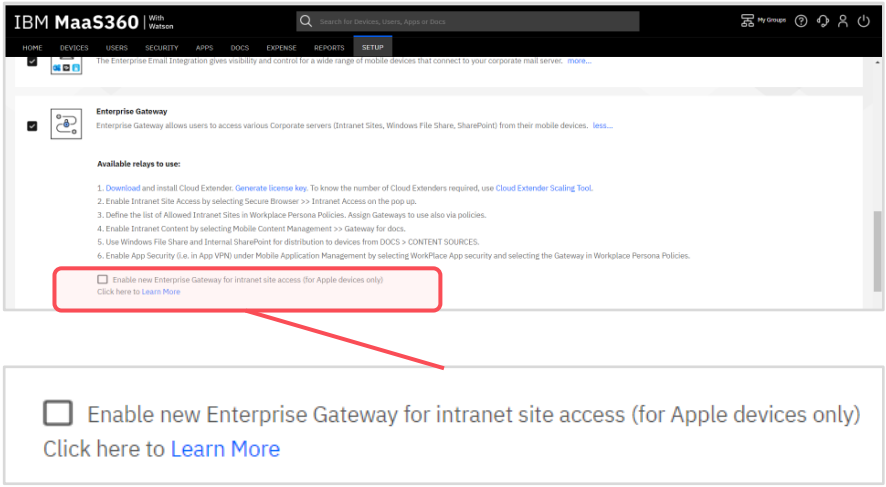
This is to help you resume the checks you have done earlier and make sure you are OK to move forward. A full detailed explanation of each step is found below.

Step	Item	Status
1	Is MEG v3 VPN already enabled? - If checkbox is available, please proceed to perform checks below to prepare. - If checkbox is not available, and you want to have it available, please contact Support to request “Enable Mobile Enterprise Gateway v3” - If checkbox is already checked, please proceed to make checks below to make sure all is correct and all devices will work correctly.	
2	Plan rollout timetable	
3	Verify whether working in Relay or Direct mode	
4	Checks - Relay mode customers ONLY	
5	Checks - Direct mode customers ONLY	
6	Update CE/MEG software versions	
7	Update iOS version on devices	
8	Update MaaS360 software versions on devices	
9	Test devices – make sure MEG v3 VPN is configured on devices and working	
10	Issues: please raise a ticket with Support	

Checklist steps – detailed description (p.1)

1. MEG v3 VPN enabled?

- Open your MaaS360 portal and go to Setup > Services
- Under *Enterprise Gateway*, click *more*
- Verify: is checkbox “Enable new Enterprise Gateway” checked?



- If checkbox is available, please proceed to perform checks below to prepare.
- If checkbox is not available, and you want to have it available, please contact Support to request “Enable Mobile Enterprise Gateway v3”
- If checkbox is already checked, please proceed to make checks below to make sure all is correct and all devices will work correctly.

Checklist steps – detailed description (p.2)

2. Plan your implementation and rollout

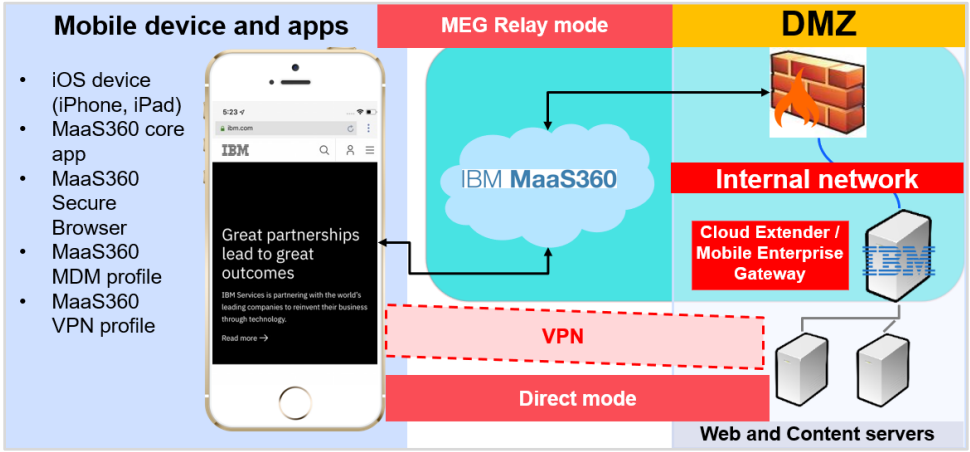
This will require some configuration and testing, you should set aside 1 hour for system checks, 1 hours for configuration and 2 hours for testing (expected 4 hours). If your use case / web content type or device types are more complex and varied, this might increase.

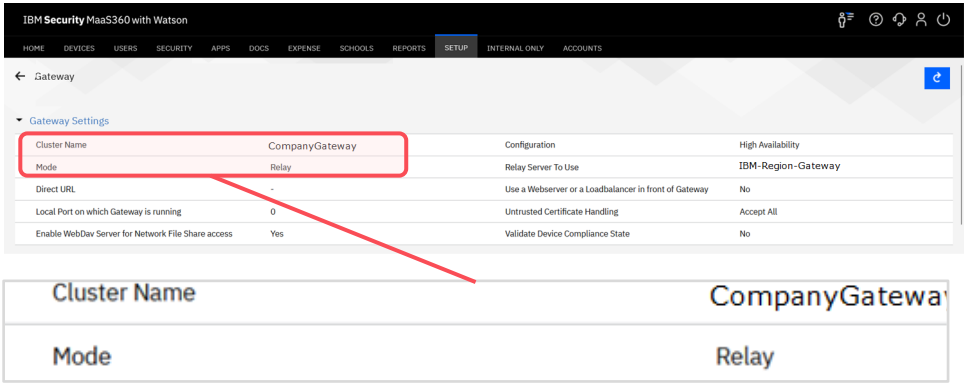
Checklist steps – detailed description (p.3)

3. Relay or Direct mode?

(please see slide 9)

- *Relay mode* – documents/web content are being retrieved from your data centre to our platform and to the device.
- *Direct mode* – where devices are retrieving content directly from your data centre without it going through our platform
- To verify go to Setup > Mobile Enterprise Gateway – look in *Mode* field on 2nd line which will tell you





Checklist steps – detailed description (p.4)

4. Relay mode customers

Confirm current OS/software versions and networking requirements:

- iOS (10.0+) (Reports > Hardware inventory)
- Cloud Extender/Mobile Enterprise Gateway software versions: (Setup > Cloud Extender > view versions at bottom)
- CE/MEG networking requirements (link no. 2 below)
- MEG v3.0 relay server (link no. 3 below)

5. Direct mode customers

Confirm current OS/software versions and networking requirements:

- iOS (10.0+) (Reports > Hardware inventory)
- Cloud Extender and Mobile Enterprise Gateway software versions: (Setup > Cloud Extender – view versions at bottom)
- CE/MEG networking requirements (link no. 2 below)
- Direct mode load balancing: see link no.4, section “Example: NGINX load balancer (or alternatives)”

If any upgrades are required please follow next steps

1. MaaS360 System Requirements: https://www.ibm.com/docs/en/maas360?topic=saas-maas360-platform-system-requirements
2. Cloud Extender / MEG requirements: https://www.ibm.com/docs/en/maas360?topic=modules-mobile-enterprise-gateway-meg-module
3. MEG 3.0 requirements: https://www.ibm.com/docs/en/maas360?topic=megmsaw-enabling-mobile-enterprise-gateway-meg-support-apple-wkwebview
4. Load balancing for direct mode: https://www.ibm.com/docs/en/maas360?topic=megmsaw-enabling-mobile-enterprise-gateway-meg-support-apple-wkwebview#concept_vtf_3wz_hnb__title__4

Checklist steps – detailed description (p.5)

6. Update software versions on CE/MEG

Instructions: https://www.ibm.com/docs/en/maas360?topic=guide-upgrading-cloud-extender-core-modules

7. Update iOS version on devices

- (from device) Settings > General > Software update – if available, connect to charger, to WiFi where possible, and start update
- (from platform) within device > Actions (top-right) > Push iOS update – choose options

8. Update MaaS360 software versions on devices

- For Supervised mode devices this should be automatic
- For Normal enrollments you can do this manually (go to App Store app on device > click on your user ‘icon’ top-right and choose Update All or Update app

Checklist steps – detailed description (p.6)

9. Test devices - ensure working

- Open Secure Browser
- You will be prompted to install the VPN profile: Accept
- Confirm VPN profile installed
- Restart device and open Secure Browser, attempt to connect to any web pages as usual

10. Contact Support for any issues

Documentation

Apple

Announcement of deprecation (sunset) of UIWebView support
https://developer.apple.com/forums/thread/678248

Deadline extension for app updates using UI Web View
https://developer.apple.com/news/?id=edwud51q

Documentation for WK Web View
https://developer.apple.com/documentation/webkit/wkwebview

Apple WebKit
https://developer.apple.com/documentation/webkit

Using WebView to view desktop or mobile web content
https://developer.apple.com/documentation/webkit/viewing_desktop_or_mobile_web_content_using_a_web_view

Acknowledgements

- iPhone image: This Photo by Unknown Author is licensed under CC BY-SA

FAQ’s (p.1)

Moving to MEG v.3

We are moving to a different way of delivering web and app content via MaaS360 Secure Browser. This is to support the changes Apple have made with their browser technology, which for iOS devices is technology that our Secure Browser relies on. We have tried to make this as straightforward as possible, with a checklist at the end to help you complete your checks.

Why is this happening?

Apple decided to move from UIWebView (a browser technology) to WKWebView, which works differently and a bit better. More importantly we have seen that this change results in a net performance increase which is significant.

When did IBM decide to work with this?

We’ve been doing this for the last 2-3 years so as we are fully expecting Apple to make the final move and ‘switch off’ the old UIWebView, and ‘switch on’ WKWebView, we want our customers to be ready. We’ve been working at implementing WKWebView in our Secure Browser, but there is also an impact on the use of Mobile Enterprise Gateway, which needs to some changes on devices and on the platform so that this can continue to work for your users.

FAQ's (p.2)

When will IBM make the change?

We've already worked on switching on the feature for some of our customers. If you want to verify whether it is already on for you, please log into your MaaS360 admin console (web browser), go to Setup / Services, and scroll down until you find Mobile Enterprise Gateway. If you click on More to the right you will find a set of information, and at the bottom there is a check-box to tell you whether this is available / already switched on / not yet configured.

When is IBM going to switch it on?

If not already enabled for you, we will turn this on by the latest on (30th June 2023???). If you want to wait until that date, OK, but you will need to take the steps indicated below to ensure that you are prepared for it.

How does it work?

In order for the new technology to work together we've changed the way that the device contacts our platform. In this case, the device will receive and install a VPN configuration which will be used every time the Secure Browser tries to connect to Mobile Enterprise Gateway. The user is asked to accept the VPN profile installation and once accepted it gets installed. If the user doesn't accept, the prompt will continue to appear until they accept it.

What happens when I switch on the MEG v3 or it gets switched on?

Once the MEG v3 VPN is activated on the Setup / Services page (Enterprise Gateway/More), the box will be checked. Once the box is checked, you know it's on now!

Why MEG 3.0 – Disadvantages of UIWebview

- UIWebview is deprecated and Apple does not allow submission of UIWebkit based apps to app-store from Dec 2020
- Using an old & unsupported technology (UIWebview) means
  - Secure Browser uses UIWebview for rendering web-pages
  - rendering issues in webpages, poor performance & security vulnerabilities in applications using it
  - with newer OS version releases we might be discovering newer & unresolved problems
  - From MaaS360 perspective, supporting older and unsupported technologies, makes it difficult to maintain our SLAs

Why MEG 3.0 – Advantages of WKWebview

- WKWebView, the new substitute for UIWebview.
- Better scalability and performance
- The WKWebView loads web pages faster and more efficiently than UIWebView, and also WKWebview doesn’t have much memory overhead
- WKWebView has higher and more efficient performance and is available to the developers all the way from iOS 8
- Secure Browser is rebuilt with WKWebview - Proactive plan to adopt WKWebview as waiting till the last minute to see UIWebview is dangerous
- Customers who haven't migrated to 3.0 will not be able to access their internal websites using MaaS360 secure browser
- The percentage of usage shows that WKWebView uses 25% CPU to render an object, whereas UIWebView uses 90% CPU for the same object
- MEG 3.0 totally supports WKWebView based secure Browser & offers better performance & flexibility to configure MaaS360 SDK, wrapped apps & 3rdparty apps