

IBM MaaS360 Remote Support with TeamViewer

Efficiently provide support and control
for remote devices with TeamViewer
and the MaaS360 solution

Highlights

Connect in seconds to obtain real-world over-the-air (OTA) device views and perform remote control functions

Provide rapid IT support for devices across Apple iOS, Google Android, macOS and Microsoft Windows platforms

Remotely configure devices, provision connectivity and remediate connectivity issues

Reduce the volume of IT help desk calls and email inquiries to support staff

Increase productivity for IT administrators and users

Providing IT support for mobile devices can be time-consuming and frustrating for both the IT team and users. Whether the two parties are located in different offices or different countries, in-person support can be impractical or impossible. Even emailed instructions and help desk coaching can be confusing. Users may not understand the problem or how to resolve it and the administrator has no ability to control the device to support them. Hence, everyone's productivity suffers.

IBM MaaS360 Remote Support with TeamViewer enables IT members to remotely view users' iOS and Android mobile devices and Windows and macOS laptops and desktops exactly as if they are seeing the device interface in person. With these real-world views, IT personnel can quickly make necessary changes or guide users to change settings, add applications or remediate connectivity issues to get employees back to their jobs as quickly as possible. If there's no user at the device or the device is a kiosk, the administrator can view and control the device in an unattended mode. This solution works in tandem with the robust capabilities of the MaaS360 unified endpoint management (UEM) platform and can help organizations reduce the costs of downtime and IT support while increasing efficiencies across the enterprise.

To use IBM MaaS360 Remote Support with TeamViewer, organizations must have a MaaS360 subscription, which enables them to be one step ahead in the struggle to maintain control over disparate endpoint and mobile devices. A recent study found that 58% of employees will either be primarily home-based or will adopt a hybrid work style going forward.¹

MaaS360 users can take advantage of its numerous UEM features—including centralized management and monitoring and strong security controls across administrators, devices, applications and content—to support smartphone, tablet, laptop and Internet of Things (IoT) deployments.

OTA configuration capabilities enable administrators to provide the profiles, credentials and settings employees need from essentially anywhere.

MaaS360 capabilities

- Quick OTA enrollment of endpoints and mobile devices
- Setup email, contacts, calendar, VPN and wifi profiles
- Access corporate docs and content, including internal and public applications
- Approve or quarantine of new mobile devices that access the network
- Restrict access to apps and features, such as screen capture and cloud backup
- Enable device sharing and kiosk mode features

With IBM MaaS360 Remote Support with TeamViewer, IT personnel can capitalize on all these capabilities, connect to a remote device in seconds, gain full visibility into the user's interface and use remote control capabilities to resolve issues.



Gain full visibility into user devices

IBM MaaS360 Remote Support with TeamViewer can be used to visualize the problems users are experiencing and provide them with remote guidance. Administrators can demonstrate an applications functionality, can directly access a device for troubleshooting and support, and can make required changes, such as:

- Configuring security policies
- Dragging and dropping applications or retrieving application data
- Performing functions required to bring a device back into compliance

Within TeamViewer, administrators and users can send instant messages to each other. If needed, administrators can also record the remote session as it occurs within the application or transfer files to the user as needed.

Count on robust remote device security



The MaaS360 solution includes a range of enterprise-grade endpoint security features, including including secure content containers, identity management, threat management and cloud security. TeamViewer security features include:

- RSA-2048 private and public key exchange and AES 256-bit session encryption, including full client-to-data encryption
- Access protection with a unique session code for every remote session
- New device confirmation at sign-in through a trusted devices list

9 steps to get started with IBM MaaS360 Remote Support with TeamViewer

1. Obtain a MaaS360 subscription.
2. Create a TeamViewer profile on TeamViewer.com.
3. Activate TeamViewer on the MaaS360 solution.
4. Download TeamViewer for remote support.
5. Select an endpoint from the device inventory in the MaaS360 solution.
6. TeamViewer will send a request for remote connectivity to the user through the MaaS360 solution.
7. The user can accept the request by clicking a link on the device. New users will need to download the TeamViewer application first.
8. Within seconds, the IBM MaaS360 Remote Support with TeamViewer interface launches on the user's device.
9. The IT administrator then has a complete view of the connected device's interface for full remote control capabilities.

Why the MaaS360 solution?

Thousands of organizations of all sizes across all industries trust the MaaS360 solution as the foundation for their digital transformation with mobile. With IBM Watson®, the MaaS360 solution delivers UEM, powered by AI, with strong security controls across users, devices, applications and content to support basically any endpoint or mobile deployment. With IBM MaaS360 Remote Support with TeamViewer, organizations can obtain the real-world device views they need to increase productivity and reduce the costs of IT support and employee downtime.

For more information

To learn more about IBM MaaS360 Remote Support with TeamViewer, contact your IBM representative or IBM Business Partner, or visit ibm.com/maas360.

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit ibm.com/financing.

© Copyright IBM Corporation 2022

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
January 2022

IBM, the IBM logo, IBM Security, IBM Watson, MaaS360, and with Watson are trademarks or registered trademarks of International Business Machines Corporation, in the United States and/or other countries. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on ibm.com/trademark.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs. THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

¹ Future of Work – How Long-Term Digital Workplace Strategies and Business Priorities Have Changed, Omdia, August 2021

