



Access Manager Mobile Users QuickStart

Your company has provided you with the ability to access corporate applications through your mobile device by providing a link to a login page to access these resource. Use the following information to install, configure, or remove the MobileAccess App.

Installing the MobileAccess App

There is an app for iOS and Android devices.

To install the MobileAccess app on a mobile device:

- 1 Access the login page URL for your company on your device.
- 2 Click the bar at the top of the login page to access the App Store on your device.
- 3 Locate the NetIQ MobileAccess app.
- 4 Tap **Install**.

To use the app, you must register your device with your company. For more information, see [Registering Your iOS Devices with Your Company](#) or [Registering Your Android Devices with Your Company](#).

Registering Your iOS Devices with Your Company

You must register your device with your company to use the app. The first time you launch the app you might be prompted to set a **PIN number**. A PIN number allows you access the app without having to enter your credentials each time you open the app.

There are two different ways to register your device. The method you use depends on how your company implemented the solution.

REGISTERING YOUR IOS DEVICE USING A URL LINK

To use this method, your company sends you an email with a link that automatically populates your company's information.

To register your iOS device:

- 1 (Optional) Create a PIN for your account the first time you launch the app.

- 2 Open the email on your iOS device.

- 3 Tap the link in the email.

The link launches the application with the **Provider** value filled in.

- 4 Tap **Sign in** to begin the registration process.

- 5 Log in with your corporate credentials or your PIN number.

Your device is now registered.

REGISTERING YOUR IOS DEVICE MANUALLY

To us this method, your company sends you an email with a URL that you must manually enter to register your device.

To manually register your iOS device:

- 1 (Optional) Create a PIN for your account the first time you launch the app.

- 2 Launch the app.

- 3 Tap **Accounts**, then tap **Plus (+)** to add a new account.

- 4 In the **Provider URL** field, type the URL sent to you in the email from your company.

- 5 Tap **Sign in** to begin the registration process.

- 6 Log in with your corporate credentials or your PIN number.

Your device is now registered.

VERIFYING THE IOS REGISTRATION

To verify the registration process worked:

- 1 After logging in to the app, at the bottom of the app window, tap **Accounts**.

- 2 Look under **Devices**. If the registration process worked, you will see your device along with the time of registration.

Registering Your Android Devices with Your Company

You must register your device with your company to use the app. The first time you launch the app you might be prompted to set a **PIN number**. A PIN number allows you access the app without having to enter your credentials each time you open the app.

REGISTERING YOUR ANDROID DEVICE

Your company sends you an email with a the URL you must enter to register your device with your company.

To register your Android device:

- 1 (Conditional) If this is the first time you open the app, you are presented with the MobileAccess License Agreement. You must read the agreement, then tap **Accept** to continue.
- 2 (Optional) After accepting the license, if this is the first time you launch the app, create a PIN for your account.
- 3 Tap the **Tools** icon, then tap **Accounts > Add Accounts**.
- 4 Type the URL your company sent you in the email.
- 5 Tap **Sign in** to start the registration process.
- 6 Log in with your corporate credentials or your PIN number.

Your device is now registered.

VERIFYING THE ANDROID REGISTRATION

To verify the registration process worked:

- 1 After logging in to the app, tap the **Tools** icon to view the Settings page.
- 2 Tap **Manage Devices**.
- 3 Look under **Devices**. If the registration process worked, you will see your device along with the time of registration.

Configuring the iOS MobileAccess App

There are different options you can configure in the app.

Tapping the **All Apps** icon displays the icons for configured applications. This page is empty until the administrator configures applications to be accessible from mobile devices.

Tapping the **Favorites** icon displays the icons for apps that you chose as your favorites. This page is empty until you add apps from the All Apps page to the Favorites page.

To add an app to Favorites:

- 1 On the All Apps page, long-press any app until all of the apps begin to shake.
- 2 Select the **X** on an app to add it to Favorites.
- 3 Tap **Home** to end the selection process.

After you add the apps to Favorites, MobileAccess opens to the Favorites page. You can view all applications by tapping **All Apps**.

Deregistering Your Device

You can deregister your device at any time.

DEREGISTERING YOUR IOS DEVICE

To deregister your iOS device:

- 1 Log in to the app.
 - 2 Tap **Accounts** at the bottom of the app window.
 - 3 Under **Devices**, the swipe left on the device name to expose the **Delete** option.
 - 4 Tap **Delete**.
- Your device is deregistered.

DEREGISTERING YOUR ANDROID DEVICE

To deregister your Android device:

- 1 Log in to the app.
 - 2 Tap the **Tools** icon to view the Settings page.
 - 3 Under **Accounts**, tap **Remove account**.
- Your device is deregistered.

DEREGISTERING YOUR DEVICE FROM A WORKSTATION

To deregister mobile devices from the Devices page:

- 1 Log in to your company's login page from a workstation.
- 2 Specify your login credentials when prompted.
- 3 In the upper right, by your name, click the arrow.
- 4 Click **My devices**.
- 5 Click the **Delete** icon next to the device you want to deregister, then click **OK** on the confirmation message.

Uninstalling the MobileAccess App

You can uninstall the MobileAccess app at any time. Also, at times you might need to uninstall the app and then reinstall an updated app when a new app is available.

To uninstall and reinstall the MobileAccess app on a device:

- 1 Follow the instructions to uninstall the MobileAccess app:
 - ♦ **iOS:** (http://www.apple.com/support/iphone/assistant/application/#section_5)
 - ♦ **Android:** (<https://support.google.com/googleplay/answer/2521768?hl=en>)
- 2 Reinstall the MobileAccess app. For more information, see "Installing the MobileAccess App" on page 1.

Installing a Self-Signed Certificate on the iOS Device

This procedure is required only if you receive an email from your company explaining that you need to add a certificate to your iOS device.

To install a self-signed certificate on your iOS device:

- 1 Open the email (or web/FTP site) your company sent you on the mobile device, then tap the certificate attachment.
- 2 In the Install Profile window, tap **Install**.
- 3 Read the warning and then tap **Install**.
- 4 Verify that the certificate says "Trusted" with a green check mark in the Profile Installed window.
- 5 (Conditional) If the certificate is not trusted, something is wrong with the certificate and the MobileAccess application will not work. Contact the person at the company that sent the email with the certificate.
- 6 Tap **Done**.
- 7 Verify that this procedure worked by entering the appliance DNS name in the Safari address bar and ensuring that there is no warning about an untrusted certificate.

NOTE: This step does not currently work in Chrome.

This certificate is installed in the **Settings > General > Profiles** page on the iOS device and can be removed from that location on the device.

Legal Notice: THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

© 2015 NetIQ Corporation. All Rights Reserved.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

Check Point, FireWall-1, VPN-1, Provider-1, and SiteManager-1 are trademarks or registered trademarks of Check Point Software Technologies Ltd.

Access Manager, ActiveAudit, ActiveView, Aegis, AppManager, Change Administrator, Change Guardian, Cloud Manager, Compliance Suite, the cube logo design, Directory and Resource Administrator, Directory Security Administrator, Domain Migration Administrator, Exchange Administrator, File Security Administrator, Group Policy Administrator, Group Policy Guardian, Group Policy Suite, IntelliPolicy, Knowledge Scripts, NetConnect, NetIQ, the NetIQ logo, PlateSpin, PlateSpin Recon, Privileged User Manager, PSAudit, PSDetect, PSPasswordManager, PSSecure, Secure Configuration Manager, Security Administration Suite, Security Manager, Server Consolidator, VigilEnt, and Vivinet are trademarks or registered trademarks of NetIQ Corporation or its affiliates in the USA. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.