MICRO FOCUS

Data Sheet
ZENworks Mobile Workspace

ZENworks Mobile Workspace

Almost every end user wants mobile access to valuable company resources. But some of these resources are full of sensitive information: contacts, attachments, appointment details, and more. Regardless of how sensitive this data is, users want access without giving complete control of their mobile devices to the company. With Micro Focus® ZENworks® Mobile Workspace, you can strike the right balance. Companies can allow mobile access to corporate applications through a company-controlled workspace while users retain control of their devices and personal data.

Product Highlights

ZENworks Mobile Workspace is a simple, highly secure mobile application management (MAM) solution for companies that want to enable mobile device use for their internal or external workforce. Users can access sensitive data through a mobile workspace that uses unique, independent security mechanisms that the company controls. As a result, business assets stay protected—whatever the configuration or ownership of the device. And users get to keep their mobile habits, apps, and privacy without suffering from frustrating device restrictions.

Key Features and Benefits

Business Workflows

ZENworks Mobile Workspace enables end users to access professional resources from their mobile devices:

Access corporate documents: Provide convenient access to a corporate collaboration repository or file repository, allowing users to easily access their data from the workspace.

Read documents: A built-in viewer for Office and PDF files enables users to review items they receive in their email or that are accessible via their documents repository.

Browse intranet: When using the browser built into the workspace, users are always browsing through the secure gateway. This feature eliminates inadvertent browsing through the corporate VPN. Additionally, the administrator can control which websites are accessible from within the workspace.

Browse web applications: Users can readily add links to their internal web applications for quick and easy access within the workspace.

Easy Management

Users will be happy to have mobile access, while IT personnel will like that ZENworks Mobile Workspace is easy to manage:

Workspace management: Centrally managing the resources available to users and devices allows you to limit the workspace to only the capabilities that a user needs.

Apps management: Implement a simple landing page where users can download the applications that the corporation supports, without the need for intrusive management agents.

User and group management: Use your corporate directory (Active Directory or eDirectory™) to leverage your current users, passwords, and groups.

ZENworks Mobile Workspace at a Glance:

- Enable mobile access to corporate resources.
- Ensure that resources are protected through a secure workspace.
- Easily manage and configure the mobile workspace.

www.microfocus.com

Web-based administration: Manage devices from anywhere by using the web-based management console.

Over-the-air configuration: Users can enroll the device with the workspace server and gain access with nothing more than an email that includes the enrollment URL.

Independent Security

There's no need to enforce policies that control entire devices to secure your corporate data. ZENworks Mobile Workspace uses its own keystore and encryption to remove potential vulnerabilities:

Sensitive data isolation: All corporate data remains in the secure workspace, so when users access it, they know they're entering a corporate data island. And because the data is encrypted, you can be sure it's secure.

Dedicated encryption: The workspace doesn't rely on the underlying OS for encryption. Instead, it uses dedicated, banking-grade encryption for local storage.

Data in-transit protection: All communication between the agent and the server is encrypted, both at the data level and over the HTTPS transport.

Data at-rest encryption: The workspace uses banking-grade encryption to secure all of the local data in the workspace.

Strong two-factor authentication: Use Java Authentication and Authorization Service (JAAS) to implement two-factor authentication with access management systems such as NetIQ® Access Manager™ and Active Directory Federation Services (ADFS). Built-in two-factor enrollment is also available.

Secure user activation: Depending on the level of security you need, you can allow the user to request access or require an administrator to manually enable user enrollment.

Device integrity control: Implement rules to control access to the workspace based on hours and days, location, jailbreak status, and more.

Threat Prevention

From unauthorized data sharing to jailbreaking, prevent risky activity within the workspace with policies you set:

Data sharing: Control whether users can share data outside of the workspace. You can include restrictions such as preventing screenshots, sharing calendars and contacts, and copying and pasting outside of the container.

Unsecure caches: Control whether the workspace provides online only or offline access. Securely encrypt the local data store with banking-grade encryption.

Data theft on lost devices: In the event that an employee loses a device or leaves the company, you can wipe just the workspace and prevent access to your sensitive data.

Jailbreak: If a user jailbreaks his or her device, you can restrict access to the workspace.

Micro Focus
UK Headquarters
United Kingdom
+44 (0) 1635 565200

U.S. Headquarters
Rockville, Maryland
301 838 5000
877 772 4450

Additional contact information and office locations:
www.microfocus.com