MICRO FOCUS

ZENworks Mobile Workspace

Integration Overview

May 2017

Legal Notice

TABLE OF CONTENTS

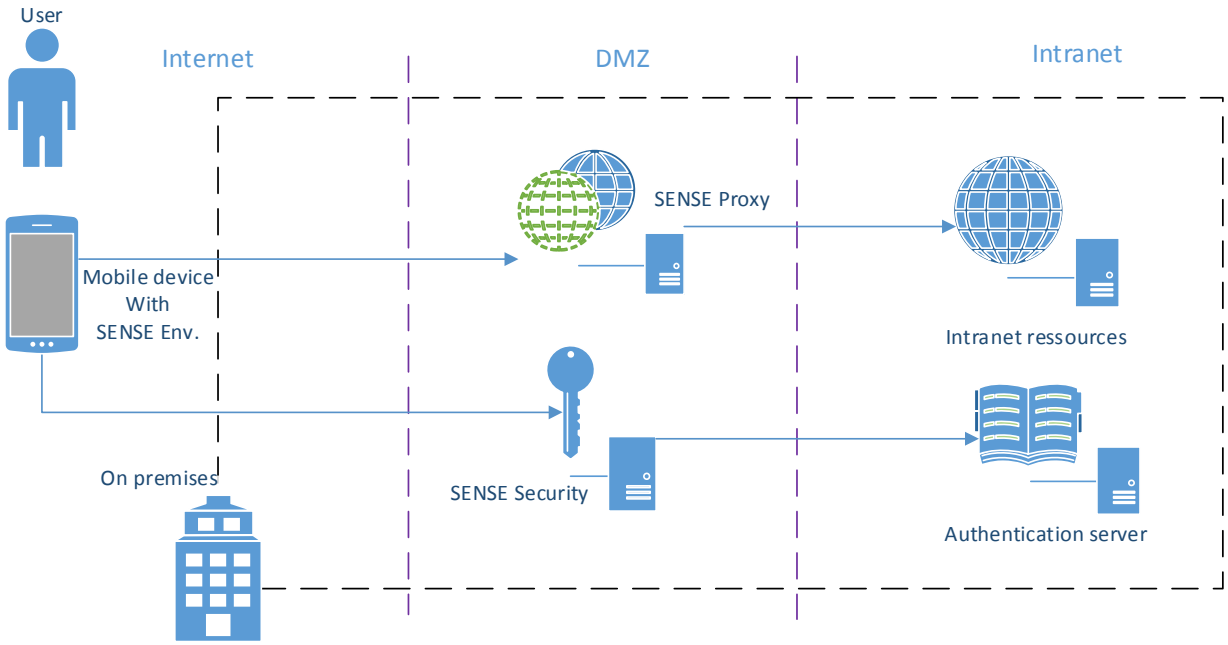
1 FOREWORD

This document aims to give an overview of the ZENworks Mobile Workspace solution to IT departments that want to deploy the application within theirs premises. It gives the minimal configuration and hardware requirements needed for a proof of concept and the back-end systems to which ZENworks Mobile Workspace can connect.

If the IT department wants to proceed to a proof of concept using a production configuration, additional steps are required.

2 OVERVIEW

The following integration diagram represents a standard deployment of ZENworks Mobile Workspace with public Internet access through a company entry point. However, a proof of concept can be conducted without an internet connection by using an internal WiFi connection.



- **User**: The user accesses his or her professional resources within the company's infrastructure from the Smartphone (running iOS or Android).
- **ZENworks Mobile Workspace Mobile / Smartphone**: The smartphone contains the ZENworks Mobile Workspace mobile application and is used to access company data through an Internet/WiFi connection.
- **ZENworks Mobile** Workspace **Security**: The ZENworks Mobile Workspace security server is installed in the customer's infrastructure and enables a centralized administration of the entire ZENworks Mobile Workspace solution.

- **SENSE Proxy**: The SENSE Proxy server allowing devices to access backend resources after authentication.
- **Authentication server**: The Active Directory / LDAP Server is a pre-installed component in the Client's infrastructure which enables the management and the authentication of users.
- **Back-end resources**: Back-end resources, such as Microsoft Exchange or IBM Lotus domino, SharePoint or OpenFire is a pre-installed component in the infrastructure which contains users' sensitive data.

3 HOSTING MACHINE

The ZENworks Mobile Workspace solution is shipped as a multi-platform installer that can be executed on a Linux or Windows operating system. In both cases, a graphics and console mode is available.

3.1 Installing ZENworks Mobile Workspace on Linux

The computer specifications to host a Linux server are the following:

- Type: virtual or physical
- Recommended resources:
  - **2000 users**: 2 x 2.2 GHz, RAM 4GB, HDD 30GB
  - **5000 users**: 4 x 2.2 GHz, RAM 8GB, HDD 50GB
- Linux version: (systemd adoption)

Linux distribution	Date added to software repository[a]	Enabled by default?	Date released as default	Can run without?
Alpine Linux	N/A (not in repository)	No	N/A	Yes
Android	N/A (not in repository)	N/A	N/A	Yes
Arch Linux	January 2012[42]	Yes	October 2012[43]	Yes[44]
CentOS	April 2014	Yes	April 2014 (7.14.04)	No
CoreOS	July 2013	Yes	October 2013 (v94.0.0)[45][46]	No
Debian	April 2012[47]	Yes	April 2015 (v8)[48]	Yes
Fedora	November 2010 (v14)[49]	Yes	May 2011 (v15)	No
Gentoo Linux[b]	July 2011[50][52][53]	No	N/A	Yes
Mageia	January 2011 (v1.0)[54]	Yes	May 2012 (v2.0)[55]	?
openSUSE	March 2011 (v11.4)[56]	Yes	September 2012 (v12.2)[57]	No
Red Hat Enterprise Linux	June 2014 (v7.0)[58]	Yes	June 2014 (v7.0)	No
Slackware	N/A (not in repository)	N/A	N/A	Yes
SUSE Linux Enterprise Server	October 2014 (v12)	Yes	October 2014 (v12)	No
Ubuntu	April 2013 (v13.04)	Yes	April 2015 (v15.04)	Yes[59]

3.2 Installing ZENworks Mobile Workspace on Windows

The computer specifications to host Windows server are the following:

- Type: Virtual or physical
- Recommended resources:
  - **2000 users**: 2 x 2.4 GHz, RAM 8GB, HDD 50GB
  - **5000 users**: 4 x 2.4 GHz, RAM 12GB, HDD 70GB
- Minimum Windows version: Windows server 2008 R2 x64

4 NETWORK CONFIGURATION

This part is linked to the data flow check list (sense_integration_check_list.pdf) that can be helpful to follow the setup of the following steps.

4.1 LDAP

The ZENworks Mobile Workspace Server can synchronize user groups with the company's LDAP directory. To achieve this, ZENworks Mobile Workspace will connect to the LDAP server and retrieve groups and users. Therefore, it is necessary to create a bind user (read only) to allow ZENworks Mobile Workspace to browse the LDAP directory.

4.1.1 Synchronization

ZENworks Mobile Workspace native LDAP connector is seeking for LDAP groups belonging to the following object class: **group, groupOfNames, groupOfUniqueNames, posixGroup**. When finding such a group, it must have at least one of the following fields set: **uid, givenName, sn, distinguishedName**. LDAP which does not match these criteria will be ignored.

When a group is selected, ZENworks Mobile Workspace will list all users belonging to that group according to the field **uniqueMember** or **member** of each user. If not defined (cf. security server manual), the default attribute used as username is the field **sAMAccountName** for Active Directory server and **cn** for other LDAP implementations. If available, the given name (field **givenName**) and the surname (field **sn**) are retrieved and displayed in the administration Web console (Helpful if the username is anonymous).

4.1.2 Authentication

ZENworks Mobile Workspace has the ability to authenticate an user on any LDAP attribute chosen as username for the synchronization. To do so, a research is done to retrieve the user distinguishedName (DN) before any authentication attempt. Therefore, the authentication process is done based on the user DN and password.

If the authentication has succeeded, the user's session is enriched with the following LDAP attributes defined for that user: **cn, displayname,description, dn, uid, sAMAccountName, userPrincipalName, mail, sn, givenName, distinguishedName**. Therefore, it will be possible to choose one of the fields as

the parameter (username) needed for backend authentication. An LDAP username used for authentication may not be usable to be used for authentication of the user against a backend server such as Exchange, SharePoint or WEB application.

However, if backend resources such as mail server (Exchange, Domino), content management system (SharePoint) or web resources need authentication, **the password used to log into SENSE must be the same as the one used for the target resources** (SSO). This is usually the case for most of standard AD/Exchange/SharePoint installations.

4.2 Firewall

ZENworks Mobile Workspace servers are listening by default on **port 8080 and 8443** for incoming HTTP(S) requests.

Firstly, you need to ensure that these ports are not blocked by the host operating system's firewall. If an external firewall is used in front of ZENworks Mobile Workspace , port translation rules can be defined like the following one:

- Internet --> **80 translated to 8080** --> ZENworks Mobile Workspace (can be even blocked to avoid connection without SSL)
- Internet --> **443 translated to 8443** --> ZENworks Mobile Workspace

It is not mandatory to translate ports but it is better to use standard HTTP ports to avoid problems with other systems/ISPs blocking nonstandard port.

4.3 Reverse Proxy

Even if SENSE ACL can prevent unauthorized access to administration console, a reverse proxy is recommended to avoid any direct access from Internet to SENSE server. To allow access to required parts of SENSE system, the following white list entries can be defined on proxy:

- **User authentication and authorization**: It will be used to enroll, authenticate and authorize the user, manage the application life cycle, check device compliance and establish a ZENworks Mobile Workspace session. The rule for this entry point is **/sense/secserver/ServletAuthentication**.
- **User application access**: It will be used to allow access to back-end system such as mail server, CMS and web application. The rule for this entry point is **/sense/appserver/Server**.
- **Application life cycle**: It will be used by the ZENworks Mobile Workspace system to provide, download and update the ZENworks Mobile Workspace mobile application. The rule for this entry point is **/sense/secserver/download/***. Or for more precise whitelist entry, the wild char * can be replaced by the following regex **[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}\.(plist|ipa|apk)** (E.g e36d3edf-c804-4720-ba95-1fd2dde38488.ipa).

- **Enterprise store**: It will be used by end users to authenticate themselves in order to get their enrollment code and download the application for the first time. The rule for this entry point is **/sense/install/***.

Reverse proxy may also be used to filter ZENworks Mobile Workspace request based on User-Agent. This may prevent any automatized attack to reach the ZENworks Mobile Workspace server.

4.4 ZENworks Mobile Workspace Administration

ZENworks Mobile Workspace administration is available through a standard Web Browser (***Minimum requirement: Google Chrome, Firefox and Safari. Some refreshing issue may happen with Internet Explorer but IE8 gives good results***):

- **/sense/secserver** : Administration of ZENworks Mobile Workspace security server:
  - Manage domains and domain admin as super admin
  - Manage security policies
  - Manage devices, users and groups
  - Manage SENSE applications
  - Manage access rights
- **/sense/pim**: Administration of DESK application
  - Manage mail server settings
  - Manage CMS server settings

For administration comfort, these consoles can be available from the intranet to avoid a remote desktop connection to access the administration Web console. Therefore, administrators can manage the solution from their preferred web browser.

4.5 TLS

Trusted TLS connection is mandatory to download and update the application on iOS 7.1. The list of trusted CAs is available here: https://support.apple.com/en-us/HT204132. Before production, the customer will be responsible to get a signed certificate from a trusted CA. During a PoC, three options are available to conduct the test:

- The application can be installed manually using Apple Configuration Utility for Windows (http://support.apple.com/kb/dl1466) or Apple Configurator for Mac (https://itunes.apple.com/ch/app/apple-configurator-2/id1037126344?l=fr&mt=12).
- Use an internal CA to sign your servers' certificates (according to the instructions present on this page https://developer.apple.com/library/ios/technotes/tn2326/_index.html - //apple_ref/doc/uid/DTS40014136) and install the CA's certificate on each iOS device (you can follow the steps described here: http://nat.guyton.net/2012/01/20/adding-trusted-root-certificate-authorities-to-ios-ipad-iphone/).

- Use Sysmosoft HTTP proxy which will provide a trusted certificate and redirect the request to your server.

5 MOBILE DEVICES

5.1 iOS devices

All iOS devices are compatible with ZENworks Mobile Workspace as long as they are running **iOS starting version 9.3.5**. Dedicated views are available for the tablet format. **Jailbroken devices are not allowed**.

The ZENworks Mobile Workspace application can only be deployed through the enterprise store. There is no available version on the public AppStore. Therefore, enterprise iOS applications must be signed with an Apple Enterprise Certificate. For PoC, Micro Focus will use its own certificate but it is mandatory to have your own to go in production. To have your own certificate, you can apply here: https://developer.apple.com/programs/ios/enterprise/ or ask Micro Focus to do it for you. The full process can takes up to 2 weeks.

5.2 Android devices

ZENworks Mobile Workspace is compatible on Android devices running from version **4.2 (Jelly Bean)**. **Rooted devices are not allowed.**

Micro Focus does not support issues caused exclusively by an operating system customization (e.g manufacturer operating system layer).

ZENworks Mobile Workspace has been tested specifically on the following devices and operating systems :

- LG Nexus 4 (operating system 5.0.1)
- LG Nexus 5 (operating system 6.0.1)
- LG Nexus 5X (operating system 7.1.2)
- Samsung Galaxy S4 mini (operating system 4.4.2)
- Samsung Galaxy S4 (operating system 5.0.1)
- Samsung Galaxy S6 (operating system 6.0.1)
- Samsung Galaxy S7 (operating system 6.0.1)
- Motorola Nexus 6 (operating system 6.0)
- Huawei Nexus 6P (operating system 7.1.1)
- Asus Nexus 7 (operating system 5.0.2)
- HTC One (operating system 5.0.1)

6 BACKEND DATA SOURCES

6.1 MS Exchange mail server

ZENworks Mobile Workspace can connect to **MS Exchange 2007, 2010, 2013, 2016 and Office365** through Exchange Web Services (EWS: http://msdn.microsoft.com/en-us/library/office/dd877012.aspx). **This requires EWS to be enabled**. To verify if EWS is enabled, go to the page http(s)://<exchange_host_name>/ews/Services.wsdl. You are prompted for a username and password. If the credentials are correct, a WSDL file is displayed.

BASIC, **DIGEST** and **NTLM** authentication are supported and ZENworks Mobile Workspace can be set to avoid NTLM if required. When using Exchange, the authentication is usually done on Active Directory.

6.2 IBM Lotus Domino server

ZENworks Mobile Workspace can connect to **IBM Lotus Domino starting version 8.5** through Domino IIOP connection (DIIOP: http://www-10.lotus.com/ldd/dominowiki.nsf/dx/DIIOP_Usage_and_Troubleshooting_Guide).

This requires DIIOP services to be enabled.

Domino connector is based on IBM remote client library (NCSO) which is incomplete. To be able to access all required features, a ZENworks Mobile Workspace Domino plugin (Domino servlet) must be deployed on the server. **This requires Domino HTTP server to be enabled**.

When using Domino, the authentication will be done on the Domino LDAP server with a username and Domino **internet password**.

6.3 Novell Groupwise

ZENworks Mobile Workspace can connect to Groupwise 2014 through SOAP Web Services (https://www.novell.com/developer/ndk/groupwise/groupwise_web_service_(soap).html). **This requires SOAP services to be enabled**. To verify if SOAP is enabled, go to the page http(s)://<groupwise_host_name>:7191/soap. You should see a HTTP 200 response page.

6.4 CMS server

6.4.1 CMIS server

ZENworks Mobile Workspace can connect to **SharePoint 2010, 2013, 2016 and any CMIS compatible CMS.** For SharePoint, connection is done through CMIS connector (SP 2013: http://msdn.microsoft.com/en-us/library/office/jj945829.aspx, SP 2010: technet.microsoft.com/en-

us/library/ff934619.aspx). **This required CMIS connector to be activated with Basic or NTLM authentication enabled**.

When using SharePoint, the authentication is usually done on Active Directory.

6.4.2 Windows share folder

ZENworks Mobile Workspace can connect to any share folder through the SMB protocol. Access rights will be the same as those defined in the Active Directory.

6.5 Internal WEB applications

The ZENworks Mobile Workspace secure browser uses ZENworks Mobile Workspace standard HTTP proxy to allow users to browse enterprise intranet. **This involves opening routes from SENSE server to such web application**.

SENSE proxy will try to do SSO on web application using HTTP authentication of type: **basic, digest, spnego, ntlm, OAuth and Kerberos**. To be able to use SSO, web application must have the same login credentials as the LDAP credentials. Otherwise, the application may display a login page to prompt the user to enter specific username and password.

Most of Web applications have not been designed for mobile devices with small screen and bad network connection. Dedicated entry point and pages may enhance user experience.