ZENworks Mobile Workspace

Security Server Guide

Version 3.18.1 - November 2018

Table of Contents

Overview

This user guide provides instruction on how to administrate the ZENworks Mobile Workspace security server.

The administration console allows to configure the whole product from a single web application.

Minimum requirement: Google Chrome, Firefox and Safari. Some refreshing issues may occur with Internet Explorer, but IE8 works well or IE in compatibility view IE8.

Roles

Roles have been defined in order to tailor the permissions associated with login credentials according to a user's responsibilities and the tasks they perform. Three roles have been predefined:

1. **Superadmin:** Responsible for the Technical configuration. He has to set the generic server configuration sections and manage domains and domain's administrators. The superadmin can setup a domain, but cannot manage it.
2. **Administrator:** Responsible for the Business and Security configuration. He has to manage all security aspects belongs to the domain and the ZENworks Mobile Workspace components configuration. Administrator credentials should only be given to individuals who have a high security level.
3. **Provisioner:** Responsible for the Users operational management. He has to assign applications to groups and enable users for enrollment. This role has been created to allow an administrator to delegate low responsibility tasks.

Multiple roles can be endorsed at once. This is generally the case for a domain **administrator** which is also a **provisioner** (as the default admin).

Login

To access to the administration console, open a web browser and navigate to `http://<server name or ip>:8080/sense/secserver` or `https://<server name or ip>:8443/sense/secserver`. The login page will display in order to give your credentials.

Enter the username and password assigned to you by your administrator and click `Login`.

If the server has just been installed, use one of the following default credentials (<username>/<password>):
- **superadmin/superadmin** (as superadmin role)
- **admin/admin.** (as administrator role)

You should change the passwords for these default accounts after your first login (cf: Edit an admin).

If you have entered the right credentials you will be redirect to the home page of the administration console. Apart from the welcome message, you will find in the top-right corner some information about your account and the `Logout` button:

- **Domain:** The domain you are about to configure (if you are logged as superadmin, that one is hidden).
- **Username:** Your username.
- **Roles:** The role(s) you have (cf. Roles).

Technical configuration

You have to log in as `superadmin` and will see the three main menus:

- HOME
- DOMAINS
- SERVER

DOMAINS

ZENworks Mobile Workspace security server supports a multitenant environment and thus is able to manage multiple domains or sites by connecting to the respective resources of various remote sites. Each domain is defined by a DNS name and a proxy address. It is linked to a synchronization source and processes authentication against its own authentication provider.

All the existing domains are listed here. At this point, you are able to Create a new domain and to Edit an existing domain or Delete an existing domain.

Create a new domain

Click on the `plus` icon in the last column table header. First, you have to give the General configuration of the domain. Once done, new configuration panels are available: Identities | PIM | Documents | Administrators

General

- **Name:** A display name.
- **DNS name or identifier:** A unique identifier for your domain.
- **Proxy URL:** When a user has been authenticated, he will be able to gain access to backend resources via the proxy server. As the resources may be different per domain (in multitenant situations), the security server will send the URL of the proxy server back to the workspace application to use at user's login.
- **Enable analytics:** ZENworks Mobile Workspace embeds a search and analytics engine allowing administrator to analyses user's behavior. If enabled, any data related to user and application activity are collected and stored in a dedicated local database.

Identities

Here are gathered the authentication and synchronization settings. Depending on the selections, some fields are displayed or hidden.

- **Users authentication and synchronization method:** Select how users and groups are retrieved through the LDAP server.

LDAP parameters:

- **URL/Path:** The URL to the LDAP server with the base name.
- **Username:** The username of the root user that has the rights to access the root group and all sub-groups. It is also used to find the DN of users.
- **Password:** The password of the root user that has the rights to access the root group and all sub-groups. It is also used to find the DN of users.
- **LDAP attribute to use as username:** The attribute for the username (example: "userPrincipalName") (default: “sAMAccountName” on AD or “cn” on LDAP).
- **Relative context:** The relative context to the groups (example: "ou=sysmosoft-groups") (default: "root").
- **Search filter:** Used to filter group name (example: “*sysmosoft*”).
- **Synchronize all users to a single group:** This enables to work with some third-party LDAP implementations that don’t support groups, or simplify the configuration for organizations that just want to quickly enable all users without modifying the LDAP server.

Synchronization parameters:

- **Custom class name:** Custom synchronization connector class name.
- **Enable auto synchronization:** When a user has been added to your identity source (such as LDAP server), an administrator must authorize the user by manually synchronizing the linked ZENworks Mobile Workspace group. You can automate this synchronization by checking this box and setting a synchronization interval.
- **Sychronization interval [m]:** The time between two synchronizations. Avoid values that are too low (less than 10 minutes), as it may take more time to synchronize than the interval duration.

Admin users authentication parameters:

- **LDAP URL:** If you would like to authenticate administrators against you LDAP server, just enter the LDAP server URL. Therefore, you still must create the user but the password will be validated directly against your LDAP server.

Custom JAAS authentication:

- **Context name:** Name of the application policy as defined in the file "$ZENworksMobileWorkspace_HOME/conf/jaas.conf".
- **Custom callback handler class name:** Name of the Java class used to handle custom credentials.

GroupWise authentication parameters:

- **Server address:** The Groupwise server hostname.
- **Server SOAP port:** The Groupwise server port number (default is "7191").
- **Connect using TLS ?:** Check this if ZENworks Mobile Workspace must use SSL to establish a connection to the Groupwise server.

PIM

The PIM (Personal Information Manager) panel allows to configure the mail server.

- **Server type:** Select what type of mail server you use.

Microsoft Exchange:

- **Server address:** The exchange server hostname.
- **Server prefix:** The server prefix to use to access the server (If you do not know, use “exchange”).
- **Connect using SSL ?:** Check this if ZENworks Mobile Workspace must use SSL to establish a connection to the Exchange server.
- **Disable NTLM ?:** Check this if the server should not use NTLM authentication scheme.

Lotus Domino 8.5.x:

- **Server address:** The Domino server hostname.
- **Connect using SSL ?:** Check this if ZENworks Mobile Workspace must use SSL to establish a connection to the Domino server.
- **Use DB name automatic resolution:** The db name of the user will be resolved from the Domino Session.
- **LDAP field name to find DB file name:** If the server cannot resolve the DB name, use this field to tell ZENworks Mobile Workspace in which LDAP field this information can be found (If you do not know, use “mailfile”).

Micro Focus GroupWise:

- **Server address:** URL of the Micro Focus GroupWise server host.
- **Server SOAP port:** Port on which the GroupWise server is listening to. The default is normally **7191**.
- **Connect using SSL ?:** Select this checkbox if ZENworks Mobile Workspace must use SSL to establish a connection with the Exchange server.

LDAP settings:

- **Attribute to use as username:** It is mandatory to define which LDAP field contains the user account name to establish a session. Most of the time, the field “sAMAcountName” is used for MS Exchange and “cn” for IBM Lotus Domino.

- **Email address attribute name:** It is mandatory to define which LDAP field contains the mailbox name. This is used to set the sender when sending a message. Most of the time, the field “mail” is used.

Documents

Document parameters allow to set CMS (content management system) server.

- **LDAP attribute to use as username:** It is mandatory to define which LDAP field contains the user account name in order to establish a session. Most of the time, the field “sAMAcountName” is used.
- **Server implementation:** Select your backend content management system:
  - **Content Management Interoperability Services (CMIS):** CMS with Content Management Interoperability Services available (like: Alfresco, Documentum, ...). Services URL should look like this: `http://alfresco.sysmosoft.local:9080/alfresco/api/-default-/public/cmis/versions/1.0/atom`.
  - **Microsoft SharePoint:** Even when, on SharePoint 2013, CMIS is also available, you must choose this option dedicated to SharePoint. To enable CMIS services on SharePoint, please follow instructions in the appropriate Microsoft documentation: MS SharePoint 2010 or MS SharePoint 2013. Services URL should look like this:
    - 2010: `http://<server>/_vti_bin/cmis/rest/<library GUID >?getrepositoryinfo`
    - 2013: `http://<server>/_vti_bin/cmis/rest?getrepositories`
  - **Windows network share (SMBv1 / CIFS):** Windows share folder access is based on SMB protocol. Services URL should look like this: `smb://sysmosoft.lan/DATA/`.

    

    Starting from Windows Server 2012, SMBv1 is disabled by default. Using SMBv1 is not recommended as it is a security issue.
  - **Windows network share (SMBv2):** Access Windows share folder usin SMBv2 protocol. Services URL should look like this: `smb://sysmosoft.lan/DATA/`.

    

    DFS support is broken. If DFS support is required in your environment, you must use the SMBv1 implementation.
- **CMIS AtomPub REST services URL:** The CMIS or MS SharePoint services URL.
- **CIFS smb:// root URL:** The Windows share folder access services URL.

Administrators

This section allows you to give access to other users who need to administrate the server.

Create an admin

- **Role:** The role(s) to assign to the user (at least one must be selected). Most of the time, administrators are set with both Administrator and Provisioner roles (cf: Roles).
- **First name:** The first name of the user. This field is for information only and will not be used

for authentication or when logging user action.

- **Last name:** The last name of the user. This field is for information only and will not be used for authentication or when logging user action.
- **Username:** The user name that the user must enter when prompted for login credentials. This field is also used when logging a user action.
- **Domain:** This is a read-only field to indicate on which domain you are currently creating (or editing).
- **Authentication mode:** Define if you want to use a ZENworks Mobile Workspace managed password (Password) or LDAP managed password (LDAP). LDAP server URL must be defined at domain creation to have the LDAP option.
- **Password:** The password that the user must enter when prompted for login credentials (minimum length is to 6 characters).
- **LDAP username** The username field use to bind the ZENworks Mobile Workspace user to the LDAP user.

Edit an admin

By clicking on the `pencil` icon, you will see the edition panel. Only four fields can be updated: the **Role(s)**, the **First name**, the **Last name** and the **Password**.

To change the password, you have to click the `Change password` button. Then, you will be prompted to enter the **Old password**, a **New password** and **Confirm new password**.

When logged in as an administrator, you will able to edit your own password.

Delete an admin

By clicking on the `cross` icon, you will ask to confirm your willingness to delete the admin. Then, clicking on `OK` will permanently remove that administrator.

Edit an existing domain

Click on the `pencil` icon. Then, you will find all the same configuration panels as for the domain creation, Refer to them for more information: General, Identities, PIM, Documents, Administrators.

Delete an existing domain

Click on the `cross` icon. Then, all domain related entities are listed and you are asked to confirm that you really want to delete that domain. If you click `OK`, all these related entities will be also deleted.

Once deleted, there is no way to recover deleted domain information (excepted by restoring a databse backup).

SERVER

Basic server parameters are located here: ACL | License | Geolocation | TLS errors | Trusted certificates | Logs | Superadmin

ACL

ACL (Access Control List) allows the Superadmin to define explicitly which computer(s) can access the web console (other than localhost). And as other entities, you can create, edit or delete by clicking respectively on the `plus`, `pencil` or `cross` icon.

Each access control is defined with a regular expression and a description:

- **Regex:** This is a regular expression (regex) that will be tested against the IP of an accessing remote computer. If the IP does not match the regex, the request will be dropped. More information about regex can be found on the web site: http://www.regular-expressions.info/ and can be tested on: http://www.fileformat.info/tool/regex.htm.
- **Description:** An information field to describe effects of the regex or to identify which computer will be allowed to access the web console.

Here are some examples and their effects:

- **.*** → All access
- **198\.168\..*** → All computers with an IP that start with 198.168.
- **192\.168\.1\.20** → Only the computer with the IP 192.168.1.20

Deleting an access control immediately renders the web console unusable. Users logged into the console will instantly no longer be able to use it.

If the server has just been installed, the web console can be accessed **from anywhere.**

License

A license must be uploaded to allow your company and its employees to use ZENworks Mobile Workspace. Without a valid license, you will be able to administrate the server, but you cannot enroll or enable security users. Moreover, the server will not create a new security session when a security user is trying to access the security server.

If the server has just been installed, ZENworks Mobile Workspace can be used during a period of 60 days without a valid license.

Once your license has been uploaded, you will see the following license information:

- **Max users:** The maximum number of users that can be enabled or connected at the same time.
- **Licenses left:** The number of available licenses that can be assigned to new users.
- **Days left:** How many more day(s) the license is valid.

- **Expiration date:** Beyond this date, security users will be unable to connect to the server.
- **File name:** The name of the license file that is currently in use.
- **File:** The license to upload. The license file must be a valid license provided by Sysmosoft SA with a Sysmosoft SA customer license (.scl) extension. **The license file has been generated exclusively for your company and cannot be shared**.

A table summarize how the licenses are used across the configured domain(s). It is particularly useful when you are providing ZENworks Mobile Workspace as a service for multiple entities in your organization, you can see how many licenses are being used per domain.

Geolocation

Geolocation is based on the detected device IP address. The IP is then compared with a list of IP ranges and the respective country in which they are delivered. Download a current IP-to-Country file from http://software77.net/geo-ip/ → Download → IPV4 CSV (zip). Extract the archive to obtain the (.csv) file and upload it. ONce done, the following information will be printed:

- **File name:** The name of the file that is currently in use.
- **Creation date:** The date when you uploaded a file for the first time.
- **Last upload date:** The date of the last uploaded file.
- **File:** The file to upload. It must be in a comma separated values format (.csv extension).

Sometime the downloaded file raise an error when trying to upload it. The reason is because at any time, new data which is not recognized by ZENworks Mobile Workspace can be created (eg: a new country). In a such case, please contact us at: support@sysmosoft.com.

TLS errors

Analyzing and identifying clearly SSL/TLS errors can be fastidious, so in addition to the trusted certificates feature, the server has a dedicated error reporting view that allows to manage the SSL/TLS errors:

The view reports the **hostname**, **port** and the **error message** as well as the **last occurrence** the error was reported. It reports also the **domain** affected which can be useful in multi-domain environments.

Errors can be acknowledged once the it has been fixed (eg: the certificate has been added, or the back-end server's configuration has been fixed). The connection is retried and the error is automatically removed from the error list if is doesn't occur anymore. Click the `retry` icon (a circular arrow in clockwise direction) to perform retry.

Errors can be ignored, allowing the application to bypass SSL/TLS checks for a given hostname/port. This is not recommended, but can help IT administrators enable a temporary workaround for back-end servers that are not configured properly. Click the `bypass` icon (two arrows crossing each other from left to right) to ignore.

Trusted certificates

It is possible to add and remove dynamically SSL/TLS certificates, avoiding complex maintenance operations. It allows to:

- Have a clear overview of custom certificates that are to be trusted by the server.
- Check expiration dates in order to anticipate problems due to certificate expiration.
- Avoid downtime and risky operations since certificates can be added without requiring a server restart.

To trust a new certificate, simply click the `plus` icon and choose a certificate file on you file system. Here are the authorized format:

- **.pem:** (Privacy-enhanced Electronic Mail) Base64 encoded DER (Distinguished Encoding Rules) certificate.
- **.cer, .crt, .der:** Usually in binary DER (Distinguished Encoding Rules) form, but Base64-encoded certificates are common too (see .pem above).
- **.p7b:** PKCS#7 SignedData structure without data, just certificate(s) or Certificate revocation list.

You can view the full details of an uploaded certificate by clicking the `pencil` icon.

If you don't want to trust a certificate anymore, click on the `cross` icon and confirm your willingness to delete it. **This takes effect immediately**.

Logs

This section allows you to access and download all log files generated by the application server that runs ZENworks Mobile Workspace. Here are the main files generated by ZENworks Mobile Workspace and its components:

- **analytics.log** contains the logs generated by the analytics engine that analyses the users behavior.
- **appserver.log:** contains the logs generated by the proxy server.
- **install.log:** contains the logs generated by the distribution server.
- **pimserver.log:** contains the logs generated by the connectors which execute the requests to the backend servers.
- **secserver.log:** contains the logs generated by the security server including those of the administration console.

All of these files have also an associated file (postfixed with "**-errors**") gathering only the errors.

In addition to these files, the Tomcat logs containing access logs and standard output logs will be available here as well. Please note that while most third-party libraries are logging to their respective module files, some may log to the standard output.

To see a specific file, click on his name and it will be directly opened in you browser.

Once a log file is open in your browser, if you refresh the page you will be able to see the last statements that have arrived since the opening (as if you were live).

To download one or several files, check the left-box in front of each wanted files and click the `Download selected files` button. Then, you will able to save a (.zip) file containing all the checked file.

Superadmin

Here you can change the password of the Superadmin. As a "regular" administrator, you have to enter your **Old password**, the **New password** and **Confirm new password**. As indicated in the confirmation message, the change will takes effect at your next login, which means that you will not disconnected from the current session (no force-logout).

Business and Security configuration

You have to log in as an `administrator` and will see the five main menus:

- HOME
- GENERAL
- APPLICATIONS
- DOMAIN
- WORKSPACE

GENERAL

Here you will find several tabs: Groups | Security settings | Contextual rules

Groups

The Security Groups are designed to prevent administrators from having to define Security settings for every user. Every group can be synchronized with an LDAP (by default) group (cf: Identities). This puts access control in the hands of the authentication server administrator. If access is disabled within the company, this state will propagated to the ZENworks Mobile Workspace platform.

To define a new group you must give the following parameters:

- **Name:** The name of the group.
- **Security settings:** Select which security rules will be applied to this group (cf: Security settings).
- **Workspace settings:** Select which workspace parameters will be applied to this group (cf: Workspace settings).
- **Sync group:** Select from a list of groups returned by the synchronization manager. In cases where the server has been configured to use the default connector, groups will be those contained in the ZENworks Mobile Workspace LDAP root group. Select the group from which

users will be imported into the ZENworks Mobile Workspace platform. If an importation has already been done, a synchronization will occur.

- **Members:** Found users have a symbol in front of his name indicating his status:
  - `green plus:` The user will be imported in the group.
  - `check in a green circle:` The user has already been synchronized.
  - `question mark in a red circle:` The user has already been synchronized in another group. He will not be added twice. Ask your LDAP administrator to remove it from one group.
  - `cross in a red circle:` The user is no longer in the LDAP group, and will be removed from the ZENworks Mobile Workspace group.

Security settings

Every Groups must use ZENworks Mobile Workspace in conformity with the security rules that have been defined for him.

Security settings are applied when the user open a session. To ensure the new settings are as soon as possible used after any modification, **the server closes every opened session linked to the modified security settings**. End users will have to login again after such modifications.

A security settings currently used by a security group cannot be deleted.

Security settings creation (same for edition) is divided into several sections:

- **Name:** A unique Name for the set of rules you are defining.

Authentication and session settings:

- **Maximum formal authentication tries (>=3):** Set how many times a user can enter a wrong password before having his/her account blocked. The account can then only be reactivated by an administrator.
- **Allow users to change their password ?:** If checked, users are allowed to update their password from the mobile application. This feature is only available for LDAP authentication and requires a TLS connection to the LDAP server.
- **User inactivity timeout [s]:** Set the time the user can remain inactive on the workspace application before he/she is required to re-enter login credentials. The session will be updated once the user re-enters the credentials.
- **Session inactivity timeout [m]:** Set the time the workspace session can remain inactive on the application side or the server side (no request received) before the user is required to re-enter login credentials. The user will need to start a new session after this timeout.
- **Enable application execution in background ?:** If checked, the session remains active on the workspace application even when it is sent to the background.
- **Secret key duration (>0) [h]:** Set how long the secret key can be used to establish session keys before becoming obsolete. The renewal process is transparent to the user, but the app start can be slower.

- **Enable strong encryption on the secret key ?:** If checked, the user password will be used to encrypt the secret key on the device. Otherwise, only OS security mechanisms will be used. This greatly increases the security, however, if the user password changes, explicit change action must be performed on the application side requiring the old password.
- **Require location ?:** If checked, the app has to send GPS coordinates in each business request. The session will be closed if the app cannot retrieve coordinates. **Be aware that this feature can increase battery consumption**.

Enrollment settings:

- **Enrollment code length (>0):** Set length of enrollment codes whose will be generated when activating enrollment for a user.
- **Enrollment code duration (>0) [h]:** Time after which the enrollment code will not be valid anymore.
- **Allow users to generate enrollment codes themselves ?:** If checked, the users are allowed to generate enrollment codes from the enterprise store.

Storage settings:

- **Enable local storage ?:** If checked, the security storage will be used on the workspace application. This should be disabled for high security.
- **Disable key update process ?:** If checked, the keys for storage encryption will never be renewed.
- **Delay until the client's storage key is refreshed (>0) [h]:** Set the time for a storage key to expire and be refreshed. This will generate new keys for the encryption of the smartphone local data.

Offline access settings:

- **Enable offline access ?:** If checked, the user will be allowed to access sensitive data without a connection to the server.
- **Offline access authorization validity (>0) [h]** Set how long a user can operate in offline mode after the last connection to the server.

Push settings:

- **Enable push notifications ?:** If checked, this enables push notification for iOS devices through the Apple Push Notification service (APNs). This establishes a persistent connection with iOS devices, which accommodates real time notifications. The tradeoff is decreased battery life. If disabled, actions such as remote wipe or push mail will not function.

Rules package:

- **Enable rules execution ?** You must check the box and then select one rule in order to assign a unique Contextual rules to the security settings.

Contextual rules

ZENworks Mobile Workspace uses Drools as business rule management system (BRMS). Since it is an open source project from JBoss all the documentation is available online ⇒ Drools 5.5.0.Final. A rule is defined by:

- **Name:** The name of the rule.
- **Version:** The version of the rule.
- **File name:** The file name of the already uploaded rule.
- **Uploaded date:** The date when the rule file has been uploaded.
- **File:** Upload a file to add a new rule or to update an existing one.

Different rules can be defined (time based, location based, etc...), but only one rule can be assigned for each Security settings.

An rule assigned to a security settings cannot be deleted.

APPLICATIONS

The Applications view allows the domain administrator to deploy different kinds of applications and each application can be loaded for the iOS and/or Android platforms. To add an application, press the `plus` icon and choose what kind of application you would like to add: In-house application or Public Store Application.

An application can be deleted only if it is not assigned to a Groups.

In-house application

In-house applications are customer dedicated applications that need to be managed and deployed to employees. These applications have been developed by the customer or third party developers and are not available on public stores such as the Apple App Store or the Google Play Store.

When you add a new in-house application, you have to provide a **Name** and a **Description** (optional). Then, you must at least **Upload an iOS binary (ipa)** and/or **Upload an Android binary (apk)**.

When you edit an existing in-house application, you can edit the name and the description, configure push notifications (cf: Push configuration) and upload a new application version. To do that, simply click the `plus` icon corresponding to the application platform (iOS or Android) and select the binary file on your file system.

You cannot upload an application with exactly the same version.

As the application itself, a version can be deleted only if it is not assigned to a Groups.

Public Store Application

Public store applications are applications published on an official public store such as the Apple App Store or the Google Play Store.

When you add a new public store application, you have to provide some information:

- **Name:** The name of the application (could be different than those used on the public store).
- **Description:** The application description (optional).
- **Link to the application on the App Store:** The URL that target the wanted application on the Apple App Store.
- **Link to the application on the Play Store:** The URL that target the wanted application on the Google Play Store.
- **Is your application secured with the SDK?:** An application based on the ZENworks Mobile Workspace development kit needs to be identified by the ZENworks Mobile Workspace server and then use the application unique identifier to do it. ZENworks Mobile Workspace can also be used just to distribute applications (without the ZENworks Mobile Workspace security enabled).
- **Bundle Id (iOS):** The iOS application unique identifier.
- **Package name (Android):** The Android application unique identifier.

When you edit an existing public store application, you can update the name and the description and configure push notifications (cf: Push configuration).

Push configuration

On the edit screen of any kind of application, you can configure the services to send push notifications. For iOS, two services are provided: Apple Push Notification Service or Novell Push Notification Service. For Android, only Firebase Cloud Messaging is provided.

Apple Push Notification Service

The Apple Push Notification Service (APNs) requires a **Key file** in `p8` format as well as a **Key ID** and a **Team ID**. These data can be obtained through the Apple developer account.

Novell Push Notification Service

The Novell Push Notification Service (NPNS) requires a **Key file** in `pem` format, a **NPNS certificate file** in `crt` format and also a **Service ID** which must be set to `ZMWAPP` for the ZENworks Mobile Workspace. These data can be obtained through the Micro Focus Certificate Portal.

Firebase Cloud Messaging

For Android, the Firebase Cloud Messaging (FCM) requires a **Firebase Admin SDK private key file** and a **Google Services configuration file** both in `json` format. These data can be obtained through the Firebase console.

Create a new project, then add an Android application and enter `com.microfocus.zenworksmobileworkspace` as *Android package name*, then click the *Register app*

button and download the `google-services.json` file by clicking on the button. Then go to the end of the wizard and click the *Skip this step* link on the *Run your app to verify installation* step. Next go to the *Project settings* and then the *Service accounts* tab. Select the *Firebase Admin SDK* and click the *Generate new private key* button, and then confirm again by clicking on the *Generate key* button. This will download the JSON key file.

DOMAIN

Here you will find several tabs: Status | Allowed URLs | Administrators

Status

The server status gives you information about connected security users and provides tools for remote control and messaging (only available when push is enabled).

- **Close all sessions:** The icon representing `two devices with a power button` will close all existing sessions. This can be use when a server reboot is needed or when a ghost session remains. A ghost session can occur if a user switches off his mobile phone abruptly and the session remains after the user is no longer connected. This remote control will affect all connected users.
- **Close a single user's session** The `power button` icon will end the user's session. The application on the mobile phone will instantly display the lock screen.
- **Send a message to all users:** Send a message to all users. This can be used to inform users of server maintenance periods or to send news (new application versions, features, etc.). You cannot send a message to an individual user.

Allowed URLs

Simple HTTP requests sent via the ZENworks Mobile Workspace application are automatically wrapped and sent through the ZENWorks proxy. For these applications, ZENworks Mobile Workspace is acting as a VPN, allowing the ZENworks Mobile Workspace app to make HTTP requests as if it were within the internal network. To avoid unauthorized access from outside, the ZENWorks proxy allows access to backend resources based on an ordered white list (first matching URL is used). Using the `First`, `Last`, `Up`, and `Down` buttons, the URLs can be ranked by priority.

You can also test a manually entered URL against the rules list to check which rule is applied to any given URL, or simply to check if an URL is allowed or not.

Click on the `plus` icon to add a URL at the list.

- **Rank:** A new URL is automatically added at the end of the white list.
- **Name:** The name of the rule.
- **Regex:** This is a regular expression (regex) that will be tested against the URL a user wants to access from the ZENworks Mobile Workspace app. If the URL does not match the regex, an html error 403 will be returned. More information about regex can be found on the web site: http://www.regular-expressions.info/ and can be tested on: http://www.fileformat.info/tool/regex.htm.
- **Auto login:** If checked, the proxy will attempt to inject user's credentials into the forwarded

http request. Otherwise, the proxy will return the result as an anonymous request. **Caution: Auto login will enrich requests with user credentials only if requested by targeted web resources. This should not be used when accessing internet resources**. Therefore, Form-based authentication is not supported. Supported scheme are:

  - Basic
  - Digest
  - Negotiate (NTLM and MS-SFU)

- **LDAP attribute to use as username (optional):** It is possible to define which LDAP field contains the user account name to establish a session. If not set, the ZENworks Mobile Workspace Users's username is used.
- **Enrich HTTP requests:** Allow the proxy to enrich client HTTP requests with the following headers:
  - **x-sense-client-ip-country:** The country name based on the IP seen by ZENworks Mobile Workspace.
  - **x-sense-client-ip-address:** The IP address of the client seen by ZENworks Mobile Workspace.
  - **x-sense-client-location:** The GPS coordinates and precision of the device.
  - **x-sense-client-time:** The date/time of the device.
  - **x-sense-identity-domain:** The user's domain.
  - **x-sense-identity-name:** The user's username.
  - **x-sense-identity-group:** The name of the group to which the user belongs.

Administrators

That section is exactly the same as described in the Technical configuration → Administrators.

When logged in as an administrator, you will not able to delete yourself.

WORKSPACE

Here are the ZENworks Mobile Workspace components settings. One of them must be assigned to each security group.

Workspace settings

The first created workspace settings will be take as default. Which means that every next created workspace settings will be copied from the first one.

A workspace settings currently used by a security group cannot be deleted. As well as the default workspace settings cannot be deleted.

Workspace settings creation (same for edition) is divided into several tabs representing the configurable ZENworks Mobile Workspace components: General | Mail | Calendar | Contacts |

Web browser | Document

General

This part is not directly linked to a ZENworks Mobile Workspace components but to the workspace it-self.

- **Allow users to remember their password in the mobile application to enable fast biometric authentication:** The administrator can authorize users to store their password on the device in order to retrieve it when opening a session with the device biometric authentication.

Mail

- **Mails to synchronize:** For security concern, an administrator can restrict the list of emails displayed on the user device by setting a range of date **since today**. Restricted options are:
  - User choice: Let the user to choose what he want (with same next options).
  - All
  - 1 day
  - 3 days
  - 1 week
  - 2 weeks
  - 1 month
- **Mail's footer:** A footer to add at the end of each email sent by the ZENworks Mobile Workspace **(the user will not be able to remove it)**.
- **Maximum file size of attachments [bytes]:** For security reason, an administrator can limit the size of mail's attachments.
- **Allowed attachment extensions:** To increase the security, users will be unable to download an attachment unless an administrator explicitly authorizes that type of attachment file. Add (`plus` icon) a new attachment type by giving an **Extension** and a **Description** and edit (`pencil` icon) or delete (`cross` icon) one.

Calendar

This synchronization allows users to import personal meetings into ZENworks Mobile Workspace and export professional meetings into the native application. Imported and exported items are read only. Imported items will never be synchronized with the remote server. **When activated, this feature must be also be enabled by the user**.

While importation retrieves all information from native applications, exportation is controlled. Meetings will be anonymized before exportation. The subject of the meeting will be "Professional meeting" and only the meeting date and time will be exported.

Contacts

This synchronization allows users to import personal contacts into ZENworks Mobile Workspace and export professional contacts into the native application. Imported and exported items are read only. Imported items will never be synchronized with remote server. **When activated, this feature must be also be enabled by the user**.

While importation retrieves all information from native applications, exportation is controlled. Only exported fields will be authorized. The name of the exported contact will be created from first name and last name or company name. If none of these fields are available, “Professional Contact” will be used instead.

Web browser

- **Home page:** The initial web page that must be opened when a user launches the Browser application.
- **Web applications:** Allow users to quickly access to web applications. Webapps are displayed at the bottom of the dashboard.

Document

The list of repositories used for the Document application component. If none is set, all found at the configured root URL (by the Superadmin: Documents) will be returned to the user.

Users operational management

You have to log in as a `Provisioner` and will see the two main menus:

- HOME
- GENERAL

GENERAL

Browser

The browser gives an overview of all security groups created and the security users in each group. It provides an easy way to quickly manage them.

When you select a user item, you will find the user’s details as described under Users.

When you select a group item, you will be able to define the applications and versions the users belonging to that group will be allowed to use. **Don’t forget to click on the `Update` button to validate your changes**.

Users

Security users are the end users of the ZENworks Mobile Workspace platform. To be permitted to access the resources ZENworks Mobile Workspace provides, every user must be added via a group

synchronization manager. **Users cannot be added or removed directly**. By clicking the `pencil` icon, you can manage a user and see information about his applications usage.

Here are the user information:

- **Group:** The security group to which the user belongs.
- **First name:** The user's first name.
- **Last name:** The user's last name.
- **User ID:** The unique user identifier. The user has to enter as **username** it in the ZENworks Mobile Workspace mobile application on the enrollment screen.
- **Client logging level:** Select the granularity of the logs that should be retrieved from the devices. Logging level modification should be confirmed by clicking on **Update** button. This change will be applied on the devices at the next login.

Logs are not sent to the server at real-time but only when a new session is established.

iOS apps handle a single logging level. When not **DISABLED**, all logs will be retrieved.

- **Enrollment code:** The one time code used for the enrollement phase. The user has to enter it in the ZENworks Mobile Workspace mobile application on the enrollment screen. This field is only set if an enrollment is in progress, empty otherwise.
- **Status:** It is the current status of the user. Possible values are:
  - **Enabled:** The user is already enrolled on an application.
  - **Never been enabled:** The user was disabled by default at the time of importation because he/she never enrolled.
  - **Maximum authentication attempts reached:** The user has attempted to log in with the wrong password too many times.
  - **Disabled by an administrator:** An administrator has locked the user.

Four actions are possible on a security user (two by two exclusive):

- **Lock user:** Although the access can be disabled through the authentication server, this provides a way for the ZENworks Mobile Workspace administrator to disable a user's access as well. All active sessions belonging to that user will be killed immediately.
- **Unlock user:** Counter part of the "Lock user" action, this will re-enable a disabled user.
- **Enable enrollment:** If your server has been configured to use the secure activation, this button allow an administrator to generate an enrollment code for the user. Therefore, this enrollment code is displayed just above and in the user's download portal as well.
- **Disable enrollment:** Counter part of the "Enable enrollment" action, this will cancel the enrollment code.

Below the user information, you can see a list with all applications that have been enrolled. By

clicking on the `question mark` icon in front of each row, you can see more details.

- **Device:** Some information about the device that runs the application.
- **Server time:** The server date/time at which the login (or last request) has been made.
- **Client time:** The device date/time at which the login (or last request) has been made.
- **IP address:** The IP address from which the server received the last login request (or last business request). The country (or network) related to the IP address is shown in parentheses.
- **Geolocation:** A button that allows to show on Google Maps the user's last known location. Based on the GPS coordinates sent by the mobile application, this button appears only if the "Require location ?" is set (cf: Security settings).
- **Download client logs:** This button appears if the device has sent logs or crash reports. An archive file containing all logs and crash reports is downloaded. Logs and crash reports are automatically deleted after 30 days.

From the list, you can also disable and/or disenroll one or several applications at once:

- **Disable an application:** Un-check the box under the `power` icon.
- **Disenroll an application:** Check the box under the `cross` icon.

When you have finished to edit the applications checkboxes, **don't forget to click on the `Apply` button to validate your changes**.