ZENworks Mobile Workspace

Security Server Guide

June 2017

Legal Notice

TABLE OF CONTENTS

1 OVERVIEW

This user guide provides instructions on how to administer the ZENworks Mobile Workspace security server. The administration tools have been categorized in three main sections:

Settings (Users' settings): Define security settings according to the company's security policies, synchronize security groups with your already set LDAP or custom groups, and define accesses. Device integrity rules and contextual rules can also be defined in this section.

Applications (MAM): Manage in-house and public store applications.

Server (Server administration): Super administrator can define who can administrate domains and access control, set basic parameters needed for resources access (application server, LDAP), upload your license and manage domains. A domain administrator can only see the list of users connected.

Administrator 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. Currently, three roles have been predefined:

- **Administrator:** (domain administrator) Can access all sections of his or her domain, except the definition of the domain itself.
- **Provisioner:** Can only access security user management.
- **Super administrator:** Can access only the security server to manage domains and create a domain administrator.

2 LOGIN

To access the web console, open a web browser* and navigate to:

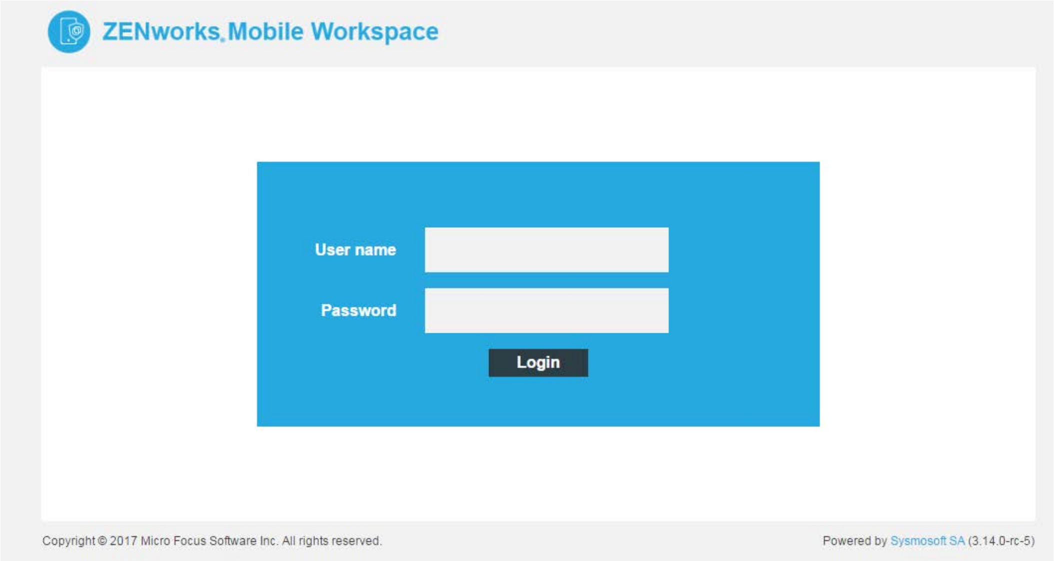
http://<server name or ip>:8080/sense/secserver or

https://<server name or ip>:8443/sense/secserver *

** 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.*

Tip: *If the server has just been installed,* ***the web console can be accessed from anywhere.*** *(See also, 3.3 Manage ACL.)*

The login page is displayed.



Copyright © 2017 Micro Focus Software Inc. All rights reserved.

Powered by Sysmosoft SA (3.14.0-rc-5)

You must give credentials to access the server web console. Enter the user name and password assigned to you by your administrator and click "Login".

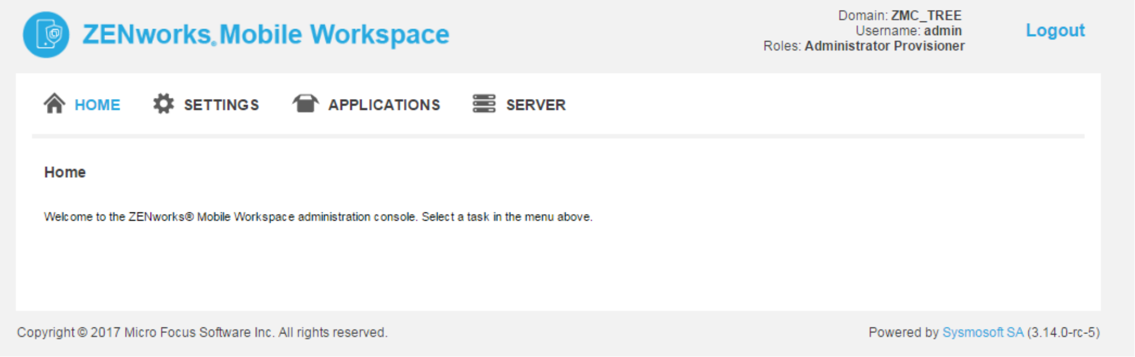
Tip: If the server has just been installed, enter the web console with one of the following default credentials (you may eventually want to change the passwords for these default logins):

- *Super Admin:* ***the user name "superadmin" and the default password "superadmin".***
- *Default Domain Admin:* ***the user name "admin" and the default password "admin".***

If an error message displays, either your credentials are wrong or someone is already logged in with the same credentials.

2.1 Main view

If you have entered the right credentials and no one else is logged in with the same user name, you will be redirected to the home page of the web console.



Domain: ZMC_TREE
Username: admin
Roles: Administrator Provisioner

Home

Welcome to the ZENworks® Mobile Workspace administration console. Select a task in the menu above.

Copyright © 2017 Micro Focus Software Inc. All rights reserved.

Powered by Sysmosoft SA (3.14.0-rc-5)

Tip: *The login info shows the username followed by the role(s) assigned to the user.*

The message panel is used to display confirmation, warning, or error messages. These messages are displayed when an administrator has created, updated or deleted information.

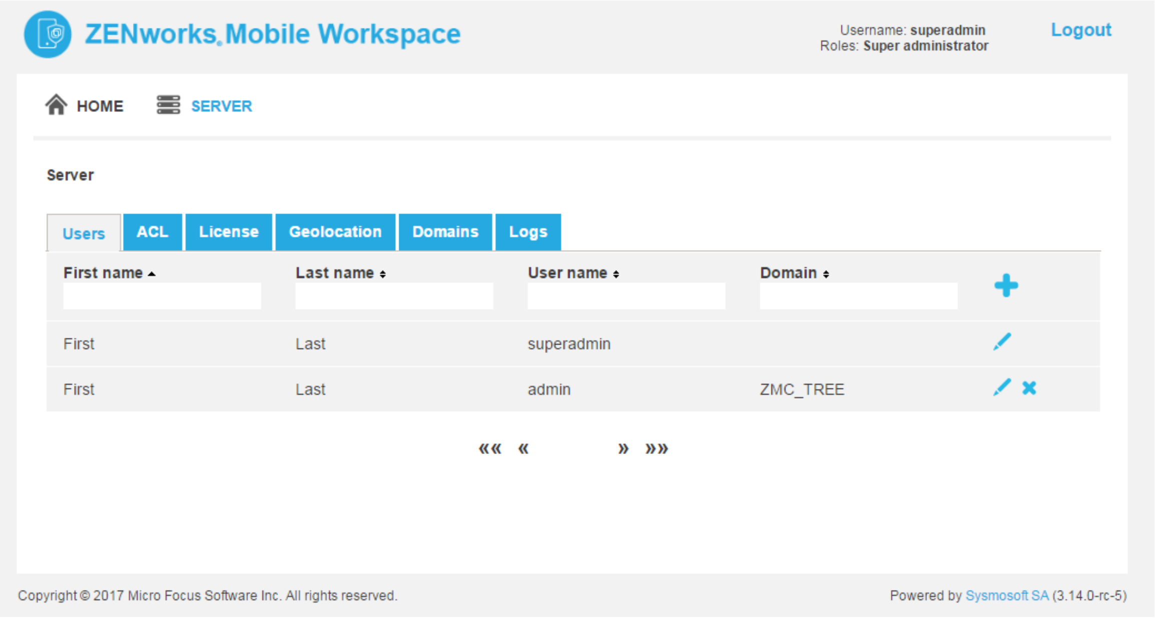
3 MANAGE SERVER

Basic server parameters are located under the main menu option labeled ***Server***.

To access the parameters you must have either **Super Administrator** or **Domain Administrator** credentials. Domain administrators can access only two of the *Server* menu sub-sections (***Users*** and ***Status***.) You must use superadmin credentials to access the rest of the sub-sections.

The ***Server*** menu sub-sections are listed below *(green text indicates superadmin access only)*:

- **Users** (administrator management): This is the only option available via either a domain admin or superadmin login. When logged in as a domain admin, the option is labeled *Users*. It allows you to create login credentials for users who must access the web console and to determine which permissions they are granted. The super administrator will be able to create domain administrators. Domain administrators can create other domain administrator or provisioner credentials for the domain in which they are working.
- **Status** (server status): Lists which security users are connected and provides tools for remote control. *This section is not available to the superadmin since only a domain administrator should be able to access end user information.*
- **ACL** (access control list): Defines which computer(s) can access the web console.
- **License** (ZENworks Mobile Workspace customer license): Uploads the license given by Micro Focus to enable access to the server.
- **Geolocation**: Defines which IP addresses are delivered from which countries.
- **Domains** (management of domains): Manages your domains and setup authentication and synchronization parameters.
- **Logs** (logs access): Display server logs and download them to assist with diagnosing issues.
- **Parameters:** All server parameters have been regrouped in the file /SENSE/lib/sense-server-config.properties.



First name ▴	Last name ⬍	User name ⬍	Domain ⬍
First	Last	superadmin	
First	Last	admin	ZMC_TREE

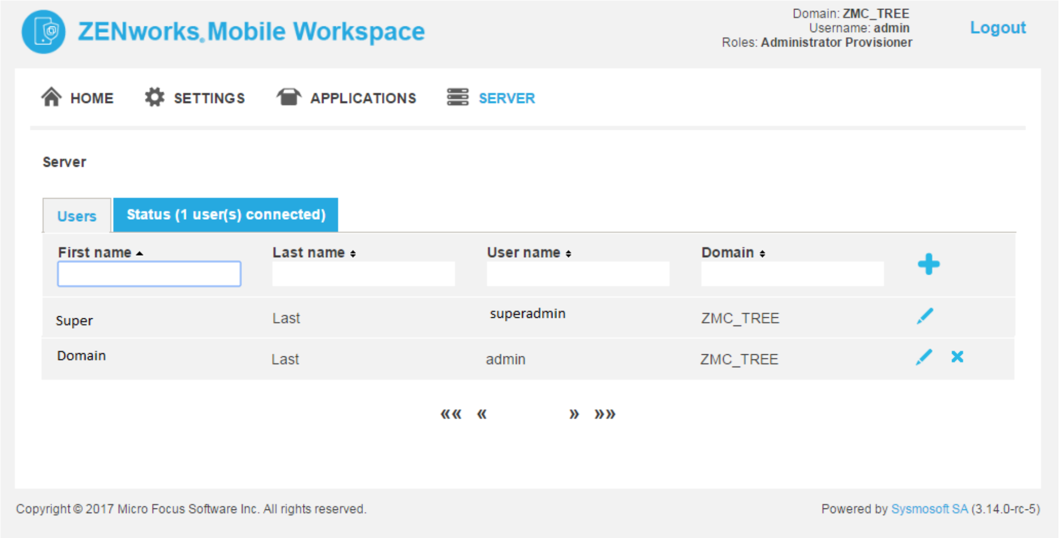
Copyright © 2017 Micro Focus Software Inc. All rights reserved.

Powered by Sysmosoft SA (3.14.0-rc-5)

3.1 Manage Users

This section allows you to give access to other users who need to administrate the server. On the security server, three roles have been defined:

- **Domain administrator:** Can access all sections related to his/her defined domain. Administrators have access to critical areas where security settings can be modified. They can give access to end users (referred to as security users) and determine the level of permissions they are granted. Administrator credentials should only be given to individuals who have a high security level.
- **Provisioner:** Can access only the device management sections (*Settings tree* and *Security users*). This role has been created to allow an administrator to delegate low responsibility tasks. A provisioner will see information related to his or her domain only.
- **Super administrator:** Can access generic server configuration sections and manage domains and domain admins. A super administrator can setup a domain, but cannot manage it.



First name	Last name	User name	Domain
Super	Last	superadmin	ZMC_TREE
Domain	Last	admin	ZMC_TREE

Copyright © 2017 Micro Focus Software Inc. All rights reserved.

Powered by Sysmosoft SA (3.14.0-rc-5)

The root administrator cannot be deleted, even by another administrator, thus the delete icon (X) does not appear against the Super Admin row. You can, however, change the password of the Super Admin.

Create a new user account

User credentials can be added by clicking the plus (+) icon and filling in the administrator form:

First name (Required): The first name of the user. This field is for information only and will not be used for authentication or when logging a user action.

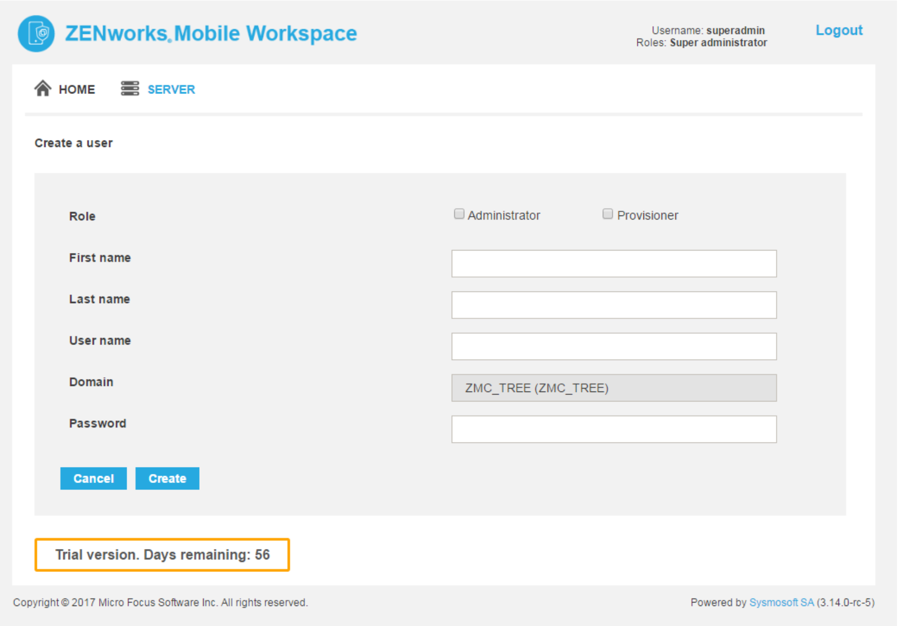
Last name (Required): The last name of the user. This field is for information only and will not be used for authentication or when logging a user action.

User name: (Required, min length = 6): The user name that the user must enter when prompted for login credentials. This field is used when logging a user action. **Role (Required):** The role that will be assigned to the user. At least one must be selected. Most of the time, domain administrators are set with both *Administrator* and *Provisioner* roles to allow access to the device management sections (*Settings tree* and *Security users*).

Domain: (This field is only required when you are logged in as Super Administrator) Select which domain this user will be allowed to manage. If you are logged in as a Domain Administrator, this parameter is hidden because you can only create a new administrator for your defined Domain.

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.

- **LDAP username:** The username field used to bind the ZENworks Mobile Workspace user to the LDAP user.
- **Password (Required, min length = 6):** The password that the user must enter when prompted for login credentials.



Username: superadmin
Roles: Super administrator

Create a user

Role	□ Administrator □ Provisioner
First name	
Last name	
User name	
Domain	ZMC_TREE (ZMC_TREE)
Password	

Trial version. Days remaining: 56

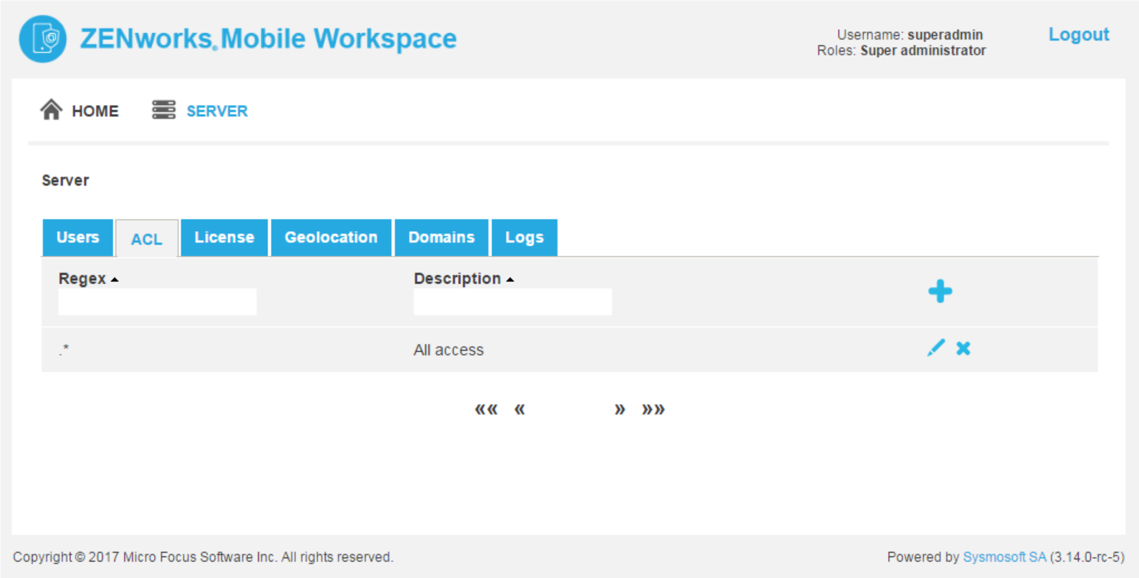
Copyright © 2017 Micro Focus Software Inc. All rights reserved.

Powered by Sysmosoft SA (3.14.0-rc-5)

3.2 Manage ACL

(Super admin access only)

ACL (Access Control List) allows the Super Administrator to define explicitly which computer(s) can access the web console (other than the localhost).



Regex ▴	Description ▴
.*	All access

Copyright © 2017 Micro Focus Software Inc. All rights reserved.

Powered by Sysmosoft SA (3.14.0-rc-5)

Deleting an access control immediately renders the web console unusable. Instantly, users logged into the console will no longer be able to see it.

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

Each access control is defined with an IP and a description:

IP: This is not exactly an IP, but to give more control you have to enter 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 this website: http://www.fileformat.info/tool/regex.htm.

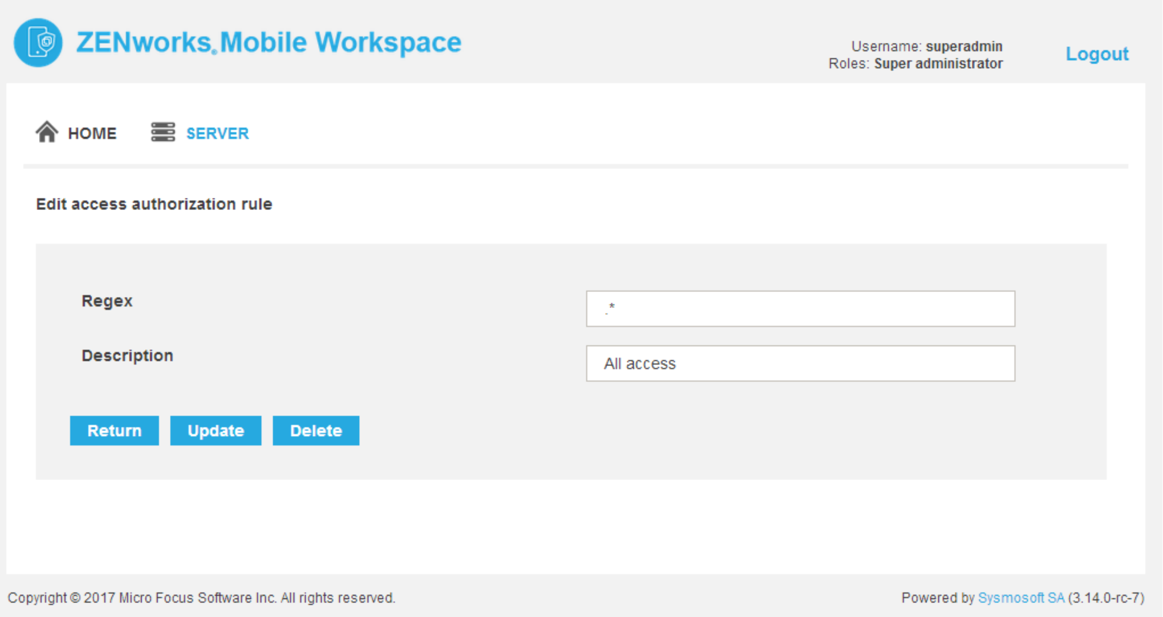
Here are some simple regex examples and their effects:

.* -> All access

198\.168\..* -> All computers with an IP that contains 198.168.

192\.168\.1\.20 -> Only a computer with the 192.168.1.20 IP.

Description: An information field to describe the effects of the regex or to identify which computer will be allowed to access the web console.



Edit access authorization rule

Regex: .*

Description: All access

Copyright © 2017 Micro Focus Software Inc. All rights reserved.

Powered by Sysmosoft SA (3.14.0-rc-7)

3.3 License

(Super admin access only)

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 (See also section 5.3 Manage Security Users). Moreover, the server will not create a new security session when a security user is trying to access the security server.

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

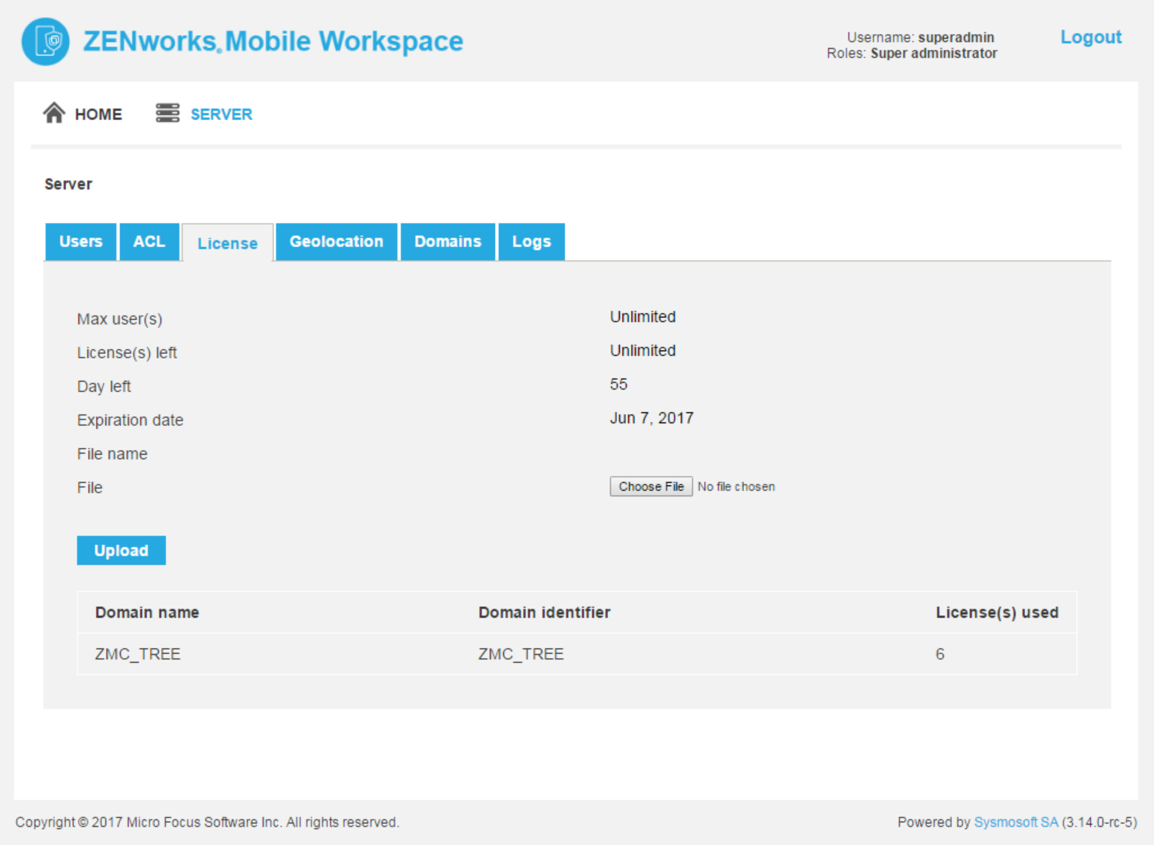
Max user: The maximum number of users that can be enabled or connected at the same time.

Licenses(s) 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: The license to upload. The license file must be a valid license provided by ZENworks Mobile Workspace with a ZENworks Mobile Workspace customer license (.scl) extension. **The license file has been generated exclusively for your company and cannot be shared.**



Max user(s)	Unlimited
License(s) left	Unlimited
Day left	55
Expiration date	Jun 7, 2017
File name	
File	

Domain name	Domain identifier	License(s) used
ZMC_TREE	ZMC_TREE	6

Copyright © 2017 Micro Focus Software Inc. All rights reserved.

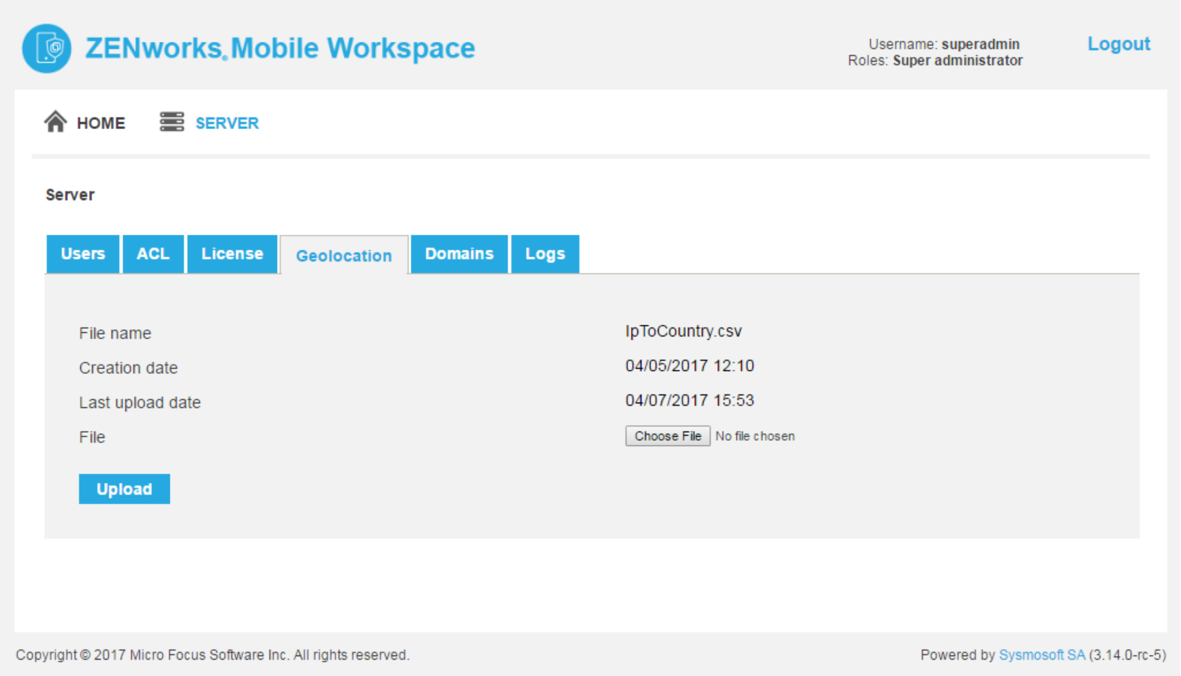
Powered by Sysmosoft SA (3.14.0-rc-5)

If 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.

3.4 IP Geolocation

(Super admin access only)

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.



File name IpToCountry.csv
Creation date 04/05/2017 12:10
Last upload date 04/07/2017 15:53
File No file chosen

Copyright © 2017 Micro Focus Software Inc. All rights reserved.
Powered by Sysmosoft SA (3.14.0-rc-5)

Download a current *IP-to-Country* file from http://software77.net/geo-ip/ -> Download -> IPV4 CSV (zip).

3.5 Server Status

(Domain admin access only)

The server status gives you information about connected security users and provides tools for remote control and messaging. The remote controls are as follows:

Close all sessions: This button will close **all** existing sessions. This can be used when a server reboot is needed or when a ghost session remains. A ghost session can occur if a user switches off his or her mobile phone abruptly and the session remains after the user is no longer connected. This remote control will affect **all** connected users.

Some remote controls affect only a selected user. On the user list, you will see each user's login name and the device that he or she is using. The remote control icons available for the user appear to the far right:

Close a single user's session: (only available when push is enabled) This action ends the user's session. The workspace application on the mobile phone will instantly display the lock screen.

3.6 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. Only a Super Administrator can create domains. Each domain is associated with an Administrator who will be responsible for managing the domain.

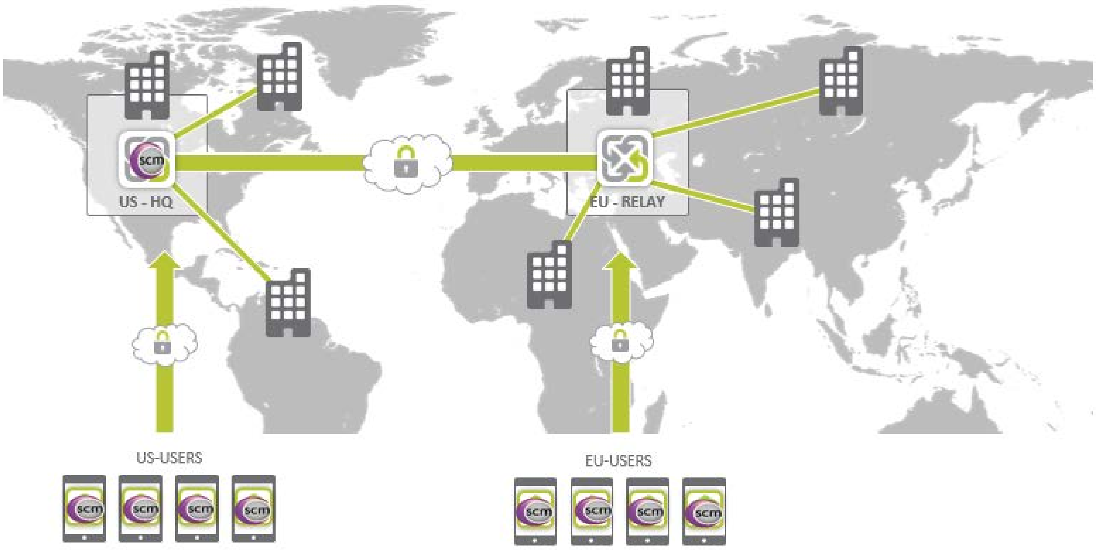


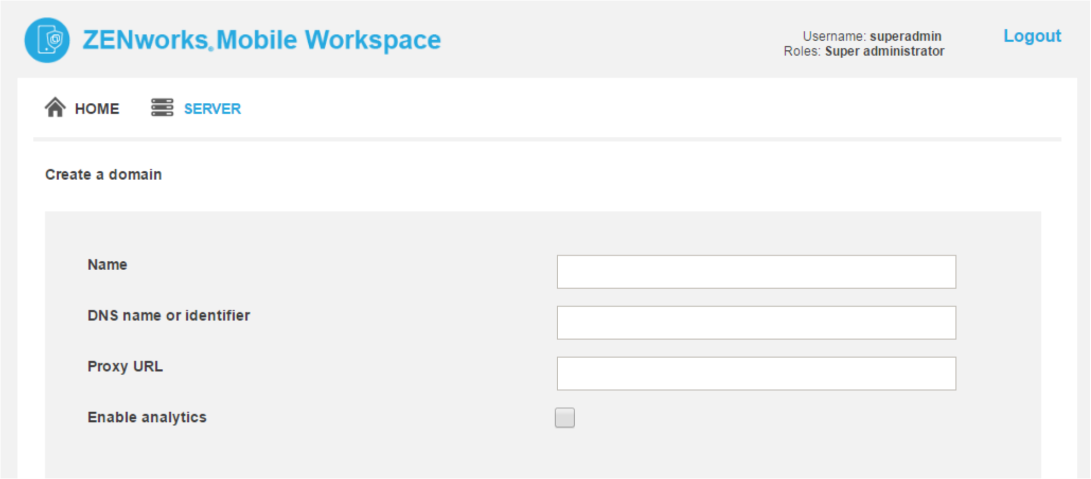
Figure 10: Federation schema

3.6.1 Domain Creation

Each domain is defined by a proxy address and parameters to authenticate and synchronize users.

Proxy URL

When a user has been authenticated, he or she 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.



Create a domain

Name

DNS name or identifier

Proxy URL

Enable analytics □

Public store version of ZENworks Mobile Workspace will also use this parameter to change the security server URL requested the first time the user installation the application. This is very useful if infrastructure changes happened such as hostname modification or HTTP to HTTPS migration.

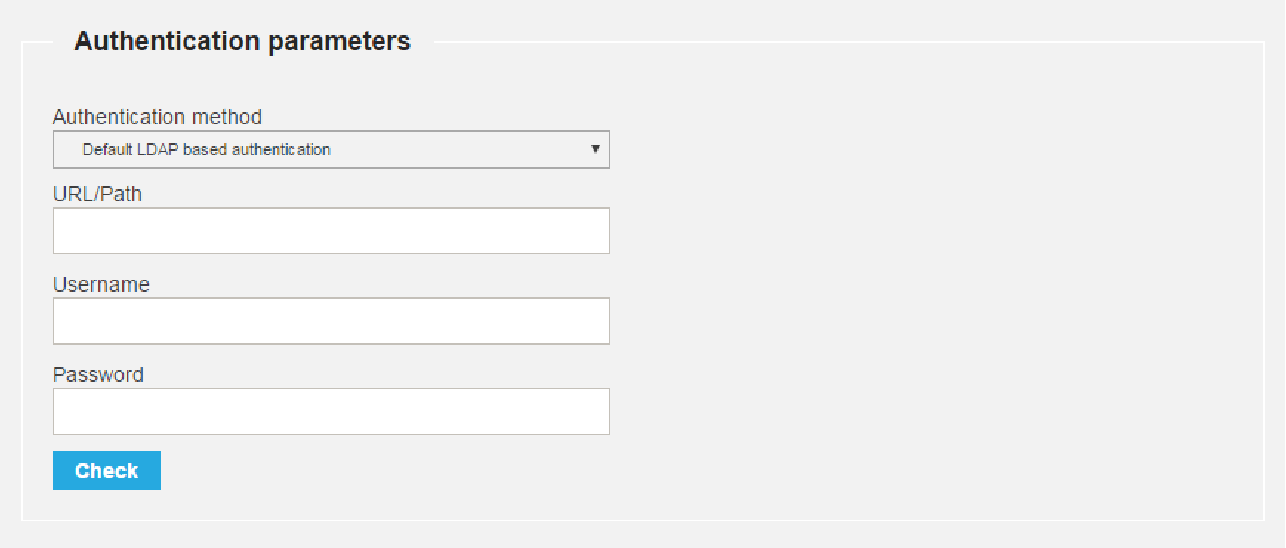
Authentication & Synchronization

The ZENworks Mobile Workspace solution utilizes the authentication and synchronization mechanisms already implemented within the enterprise. By default, ZENworks Mobile Workspace uses an LDAP JAAS connector for authentication and a proprietary LDAP connector for group synchronization. This LDAP connector can be used for authentication and synchronization against OpenLDAP, MS Active Directory, IBM Lotus Domino or all other server matching LDAP protocol.

To enable ZENworks Mobile Workspace to use these connectors the following information must be given:

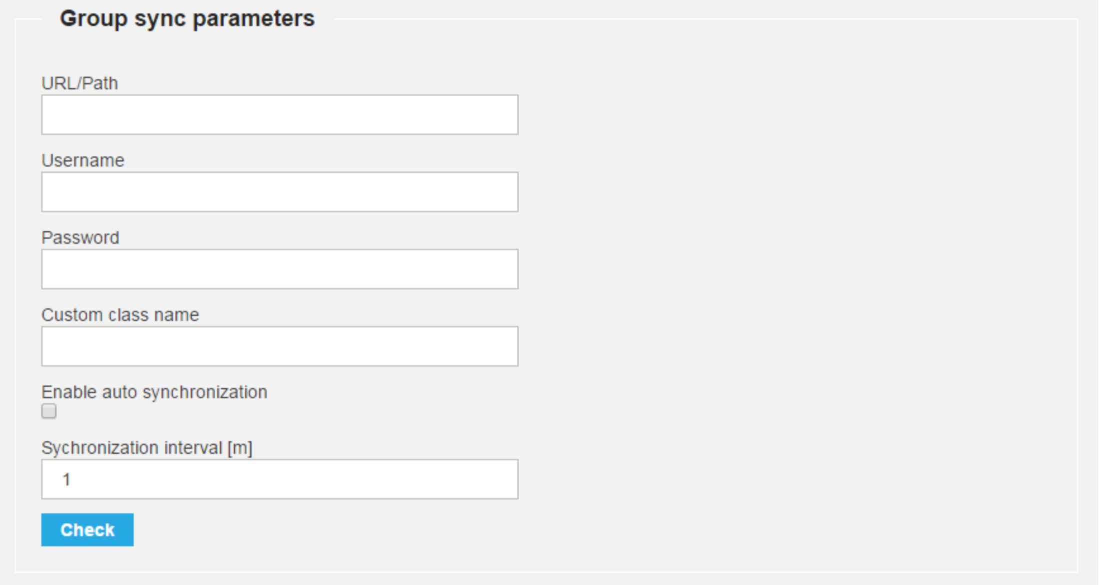
Authentication

- <u>Default LDAP based authentication</u>
    - **URL/Path**: The URL to the LDAP server with the base name.
    - **Username**: The user name used to find the DN of a ZENworks Mobile Workspace user.
    - **Password**: The password used to find the DN of a ZENworks Mobile Workspace user.
- <u>Custom JAAS based authentication</u>
  (See the ZENworks Mobile Workspace Servers SDK document for further information)
    - **Custom JAAS context name**: Name of the application policy as defined in the file SENSE_HOME/conf/jaas.conf
    - **Custom JAAS callback handler class name**: Name of the Java class used to handle custom credentials.



Authentication method: Default LDAP based authentication

Synchronization



Enable auto synchronization ☐

Sychronization interval [m]: 1

- **URL/Path**: The URL to the LDAP server with the base name. Additional parameters can be added separated with semi-colon (;):
  - Second parameter sets the relative context to the groups.
    Example: ou=microfocus-groups (Default: root)
  - Third parameter sets the attribute for the username.
    Example: userPrincipalName. (Default, "**sAMAccountName**" on LDAP AD or "**cn**" on ldap)
  - Fourth parameter is used to trim the domain contained in the username in cases where the username is the email address.
    Example: If username is username@domain.com and this parameter is set to "@," the result will be username.

        - Fifth parameter is used to filter group name.
          Example: "*microfocus*"

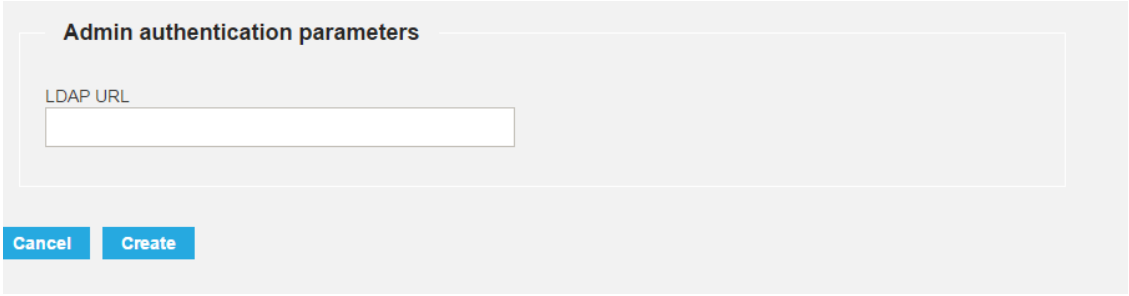
    Common usage may be similar to the following:
    ldap://ad.company.local:389/DC=microfocus,DC=com;OU=microfocus-groups;userPrincipalName;@;*microfocus*

- **Username**: Username of the root user that has the rights to access the root group and all sub-groups.
- **Password**: Password of the root user that has the rights to access the root group and all sub-groups.
- **Custom class name**: Custom synchronization connector class name. See the ZENworks Mobile Workspace Server SDK document for further information.
- **Enable auto synchronization**: When a user has been added to your identity source (such as LDAP server), a domain 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.
- **Synchronization interval:** 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.

To check whether or not the correct parameters have been set, use the ***Check*** button to validate them.

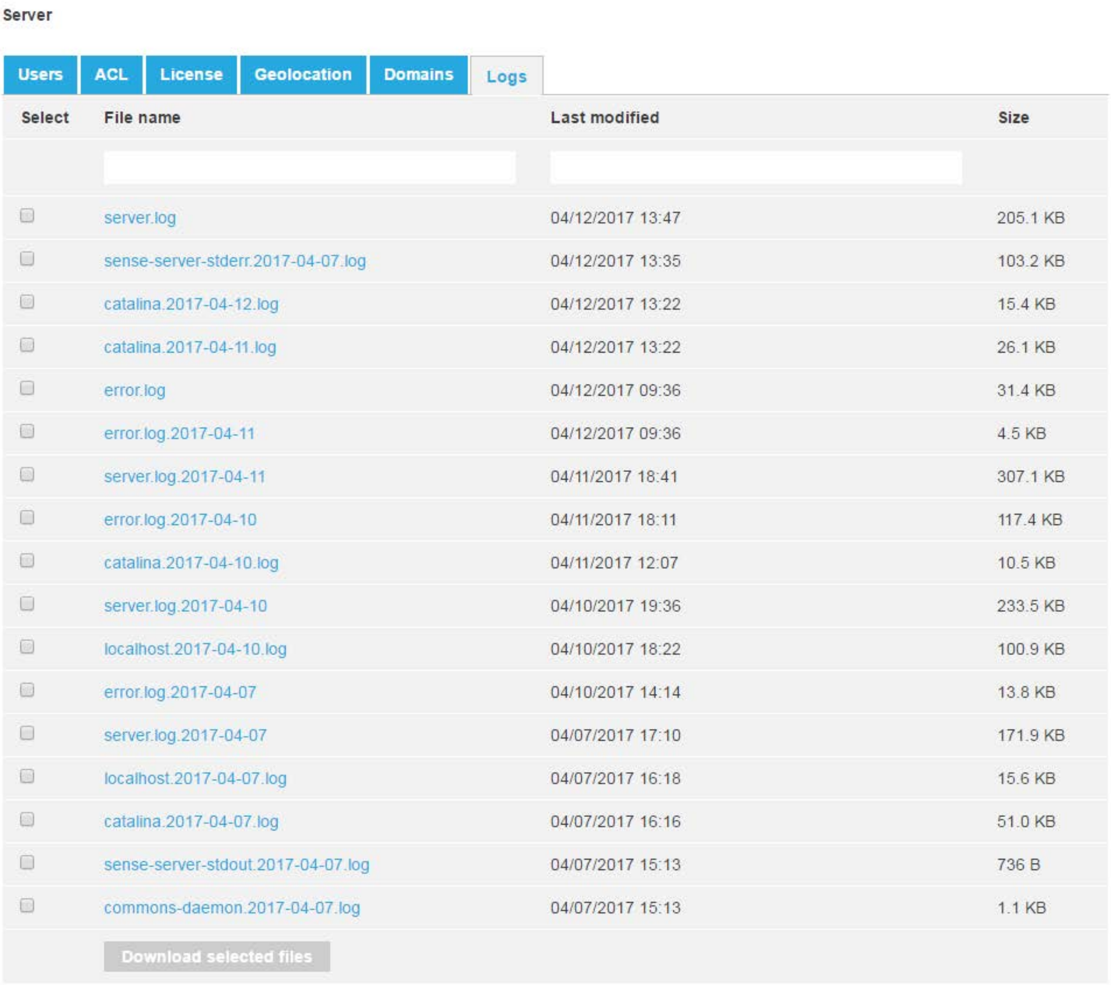
- **LDAP Admin authentication**

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



3.7 Logs

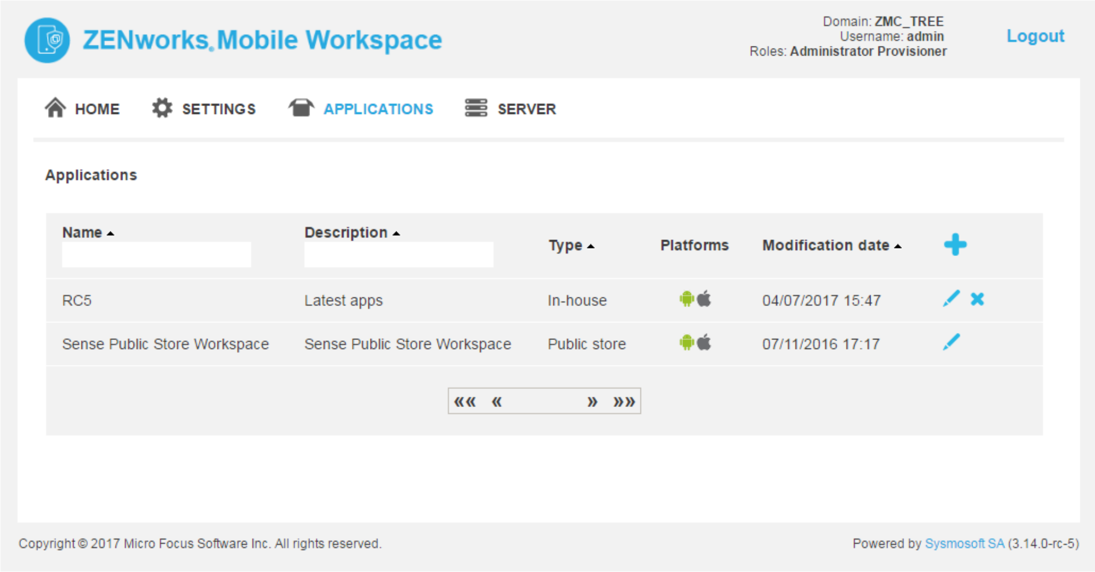
This section allows you to access and download all log files generated by the application server that runs ZENworks Mobile Workspace. In addition to logs from the security server, logs from any module or custom library will be available here as well.



Select	File name	Last modified	Size
□	server.log	04/12/2017 13:47	205.1 KB
□	sense-server-stderr.2017-04-07.log	04/12/2017 13:35	103.2 KB
□	catalina.2017-04-12.log	04/12/2017 13:22	15.4 KB
□	catalina.2017-04-11.log	04/12/2017 13:22	26.1 KB
□	error.log	04/12/2017 09:36	31.4 KB
□	error.log.2017-04-11	04/12/2017 09:36	4.5 KB
□	server.log.2017-04-11	04/11/2017 18:41	307.1 KB
□	error.log.2017-04-10	04/11/2017 18:11	117.4 KB
□	catalina.2017-04-10.log	04/11/2017 12:07	10.5 KB
□	server.log.2017-04-10	04/10/2017 19:36	233.5 KB
□	localhost.2017-04-10.log	04/10/2017 18:22	100.9 KB
□	error.log.2017-04-07	04/10/2017 14:14	13.8 KB
□	server.log.2017-04-07	04/07/2017 17:10	171.9 KB
□	localhost.2017-04-07.log	04/07/2017 16:18	15.6 KB
□	catalina.2017-04-07.log	04/07/2017 16:16	51.0 KB
□	sense-server-stdout.2017-04-07.log	04/07/2017 15:13	736 B
□	commons-daemon.2017-04-07.log	04/07/2017 15:13	1.1 KB

4 MANAGE APPLICATIONS

The **Applications** view allows the domain administrator to deploy different kinds of applications.



Applications

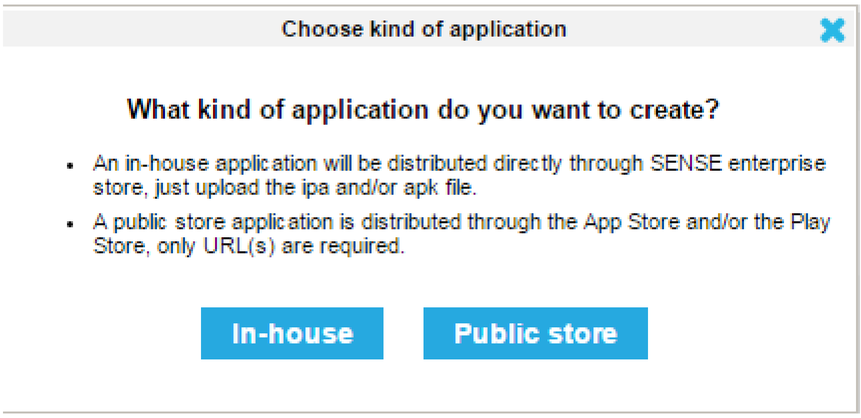
Name ▴	Description ▴	Type ▴	Platforms	Modification date ▴	+
RC5	Latest apps	In-house	🤖	04/07/2017 15:47	✎ ✖
Sense Public Store Workspace	Sense Public Store Workspace	Public store	🤖	07/11/2016 17:17	✎

Copyright © 2017 Micro Focus Software Inc. All rights reserved.

Powered by Sysmosoft SA (3.14.0-rc-5)

To add an application, click the '+' icon. Choose what kind of application you would like to add: **In-house** or **Public store.**

Each application can be uploaded for the iOS and/or Android platforms.



Choose kind of application

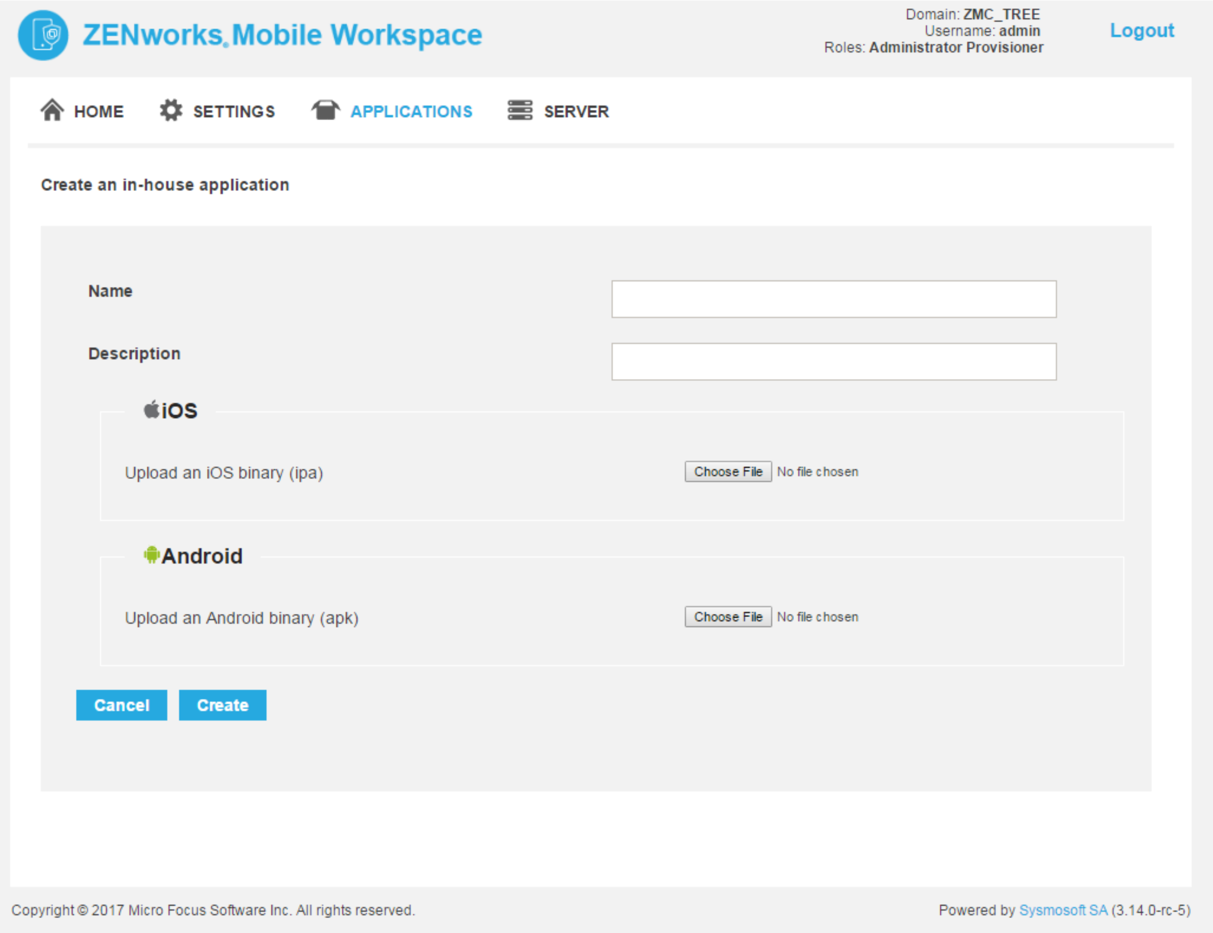
What kind of application do you want to create?

- An in-house application will be distributed directly through SENSE enterprise store, just upload the ipa and/or apk file.
- A public store application is distributed through the App Store and/or the Play Store, only URL(s) are required.

4.1 In-house Applications

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 Google Play Store.

4.1.1 Add new in-house applications



Create an in-house application

Name

Description

iOS

Upload an iOS binary (ipa) Choose File No file chosen

Android

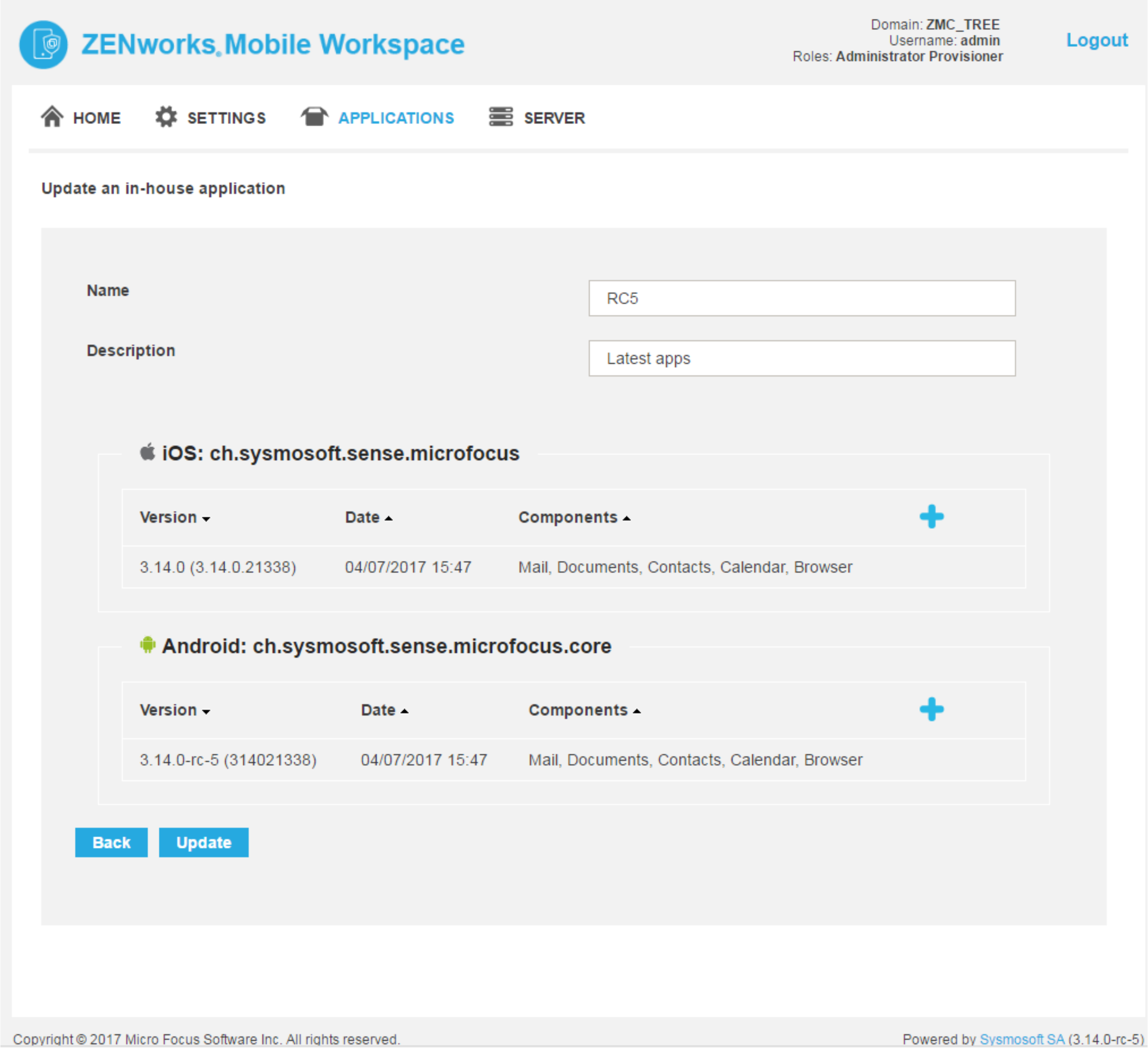
Upload an Android binary (apk) Choose File No file chosen

Copyright © 2017 Micro Focus Software Inc. All rights reserved.

Powered by Sysmosoft SA (3.14.0-rc-5)

4.1.2 Edit in-house applications

Click the edit icon beside the app you want to update. You can edit the name and description or upload a new application version. As with public stores, **you cannot upload an application with exactly the same version**.



Domain: ZMC_TREE
Username: admin
Roles: Administrator Provisioner

Update an in-house application

Name: RC5

Description: Latest apps

iOS: ch.sysmosoft.sense.microfocus

Version	Date	Components
3.14.0 (3.14.0.21338)	04/07/2017 15:47	Mail, Documents, Contacts, Calendar, Browser

Android: ch.sysmosoft.sense.microfocus.core

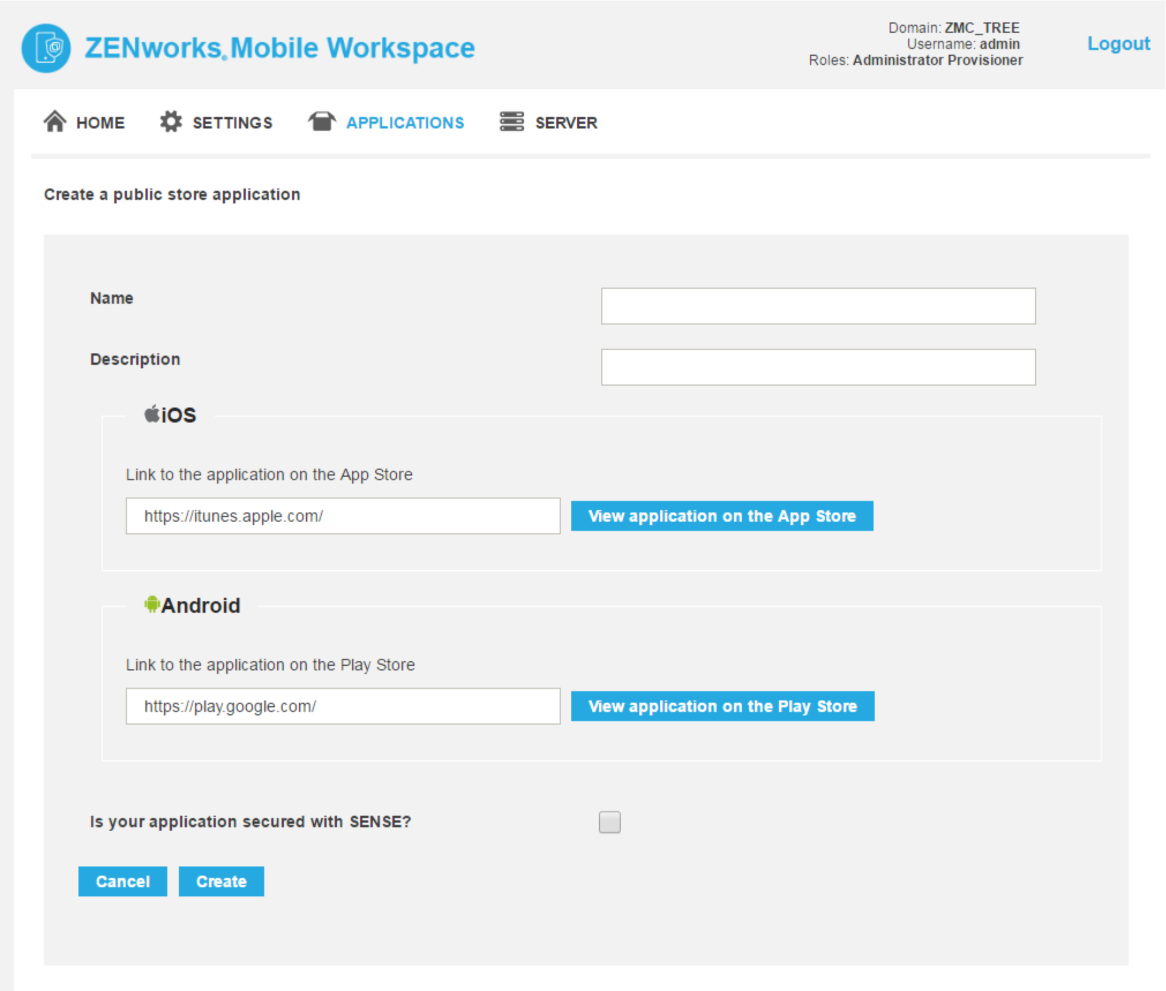
Version	Date	Components
3.14.0-rc-5 (314021338)	04/07/2017 15:47	Mail, Documents, Contacts, Calendar, Browser

Copyright © 2017 Micro Focus Software Inc. All rights reserved.

Powered by Sysmosoft SA (3.14.0-rc-5)

Click on the "+" icon to upload a new In-house version. A popup is displayed allowing you to upload the new version.

4.2 Public Store Applications


ZENworks Mobile Workspace
Domain: ZMC_TREE
Username: admin
Roles: Administrator Provisioner
Logout
HOME
SETTINGS
APPLICATIONS
SERVER

Create a public store application

Name

Description

iOS

Link to the application on the App Store

https://itunes.apple.com/

View application on the App Store

Android

Link to the application on the Play Store

https://play.google.com/

View application on the Play Store

Is your application secured with SENSE? □

5 MANAGE SETTINGS

The *Settings* menu option is an operational view of the security server. This section allows you to define and edit security groups and users, define group members, and identify which devices security users are using.

To manage these settings, click on the ***Settings*** menu option. This option is only accessible with administrator login credentials and is composed of the following sub-sections:

Settings tree: An overview and quick access to the *Security users* and *Security groups* sections.

Security users: Security user management. Once a group has been added and synchronized, you can edit security users who are part of the group and their mobile devices.

Security groups: Security group creation and synchronization. Add, remove, update, and synchronize security groups.

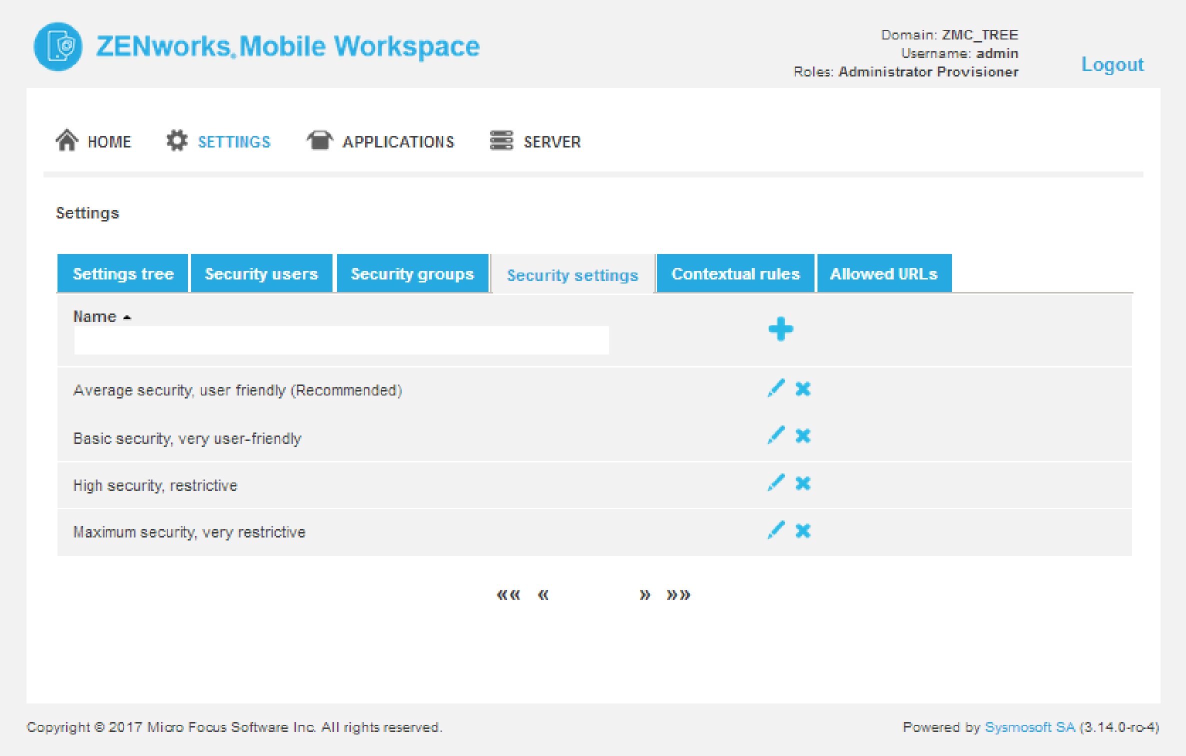
Security settings: Define security rules that are compatible with your company IT security policies.

Device integrity checks: Define security checks which can be used in *Security settings* to allow or deny access to devices according to their configuration.

Contextual rules: Upload business rules engine contextual rules file.

5.1 Manage Security settings

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



Name
Average security, user friendly (Recommended)
Basic security, very user-friendly
High security, restrictive
Maximum security, very restrictive

Tip: *You cannot remove security settings that are currently being used by a security group.*

Each *Security setting* is divided into **Defaults** settings and **Contextual** settings.

5.1.1 Defaults

Enter a unique ***Name*** for the set of rules you are defining.

The *Default* security settings are divided into several categories. You can click ? in front of each rule to view a short description.

Authentication and session: Define formal authentication policies such as maximum authentication tries, session timeout, background execution, and secret key encryption.

Maximum formal authentication tries (Required)	Set how many times a user can enter a wrong password before having his/her account blocked. The account can then be reactivated only by an administrator.
User inactivity timeout (Required)	Set the time the user can remain inactive on the workspace application before he/she is required to re-enter the login credentials. The session will be updated once the user re-enters the credentials.
Session inactivity timeout (Required)	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 (Required)	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: Define enrollment code policies such as length and validity duration.

Enrollment code length	Set length of enrollment codes that will be generated when activating enrollment for a user.
Enrollment code duration	Time after which the enrollment code will not be valid anymore.

Storage: Define cryptographic key renewing interval and whether or not the storage is enabled.

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	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: Determines whether security user has access to information when no longer connected.

Enable offline access	If checked, the user will be allowed to access sensitive data without a connection to the server.
Offline access authorization validity	Set how long a user can operate in offline mode after the last connection to the server.

Push: Enable or disable push functionality.

Enable push notification	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.

5.1.2 Contextual

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. See: Drools 5.5.0.Final

Different rules can be defined (time based, location based, etc.). One or more rules can be selected for each Security Setting.

5.2 Manage Security Groups

The Security group option was designed to prevent administrators from having to define security settings for every user.

Every group can be synchronized with an LDAP (by default) group. 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 (Required): The name of the group.

Security settings (Required): Select which security rules will be applied to this group.

Sync Group (Required): 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.

Each user has is symbol in front of their name indicating their status:

✚ The user will be imported in the group.

✓ The user has already been synchronized.

❗ 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.

✖ The user is no longer in the LDAP group, and will be removed from the ZENworks Mobile Workspace group.

5.3 Manage Security 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.**

Lock user: Although the access can be disabled through the authentication server, this provides a way for ZENworks Mobile Workspace administrators to disable a user's access as well.

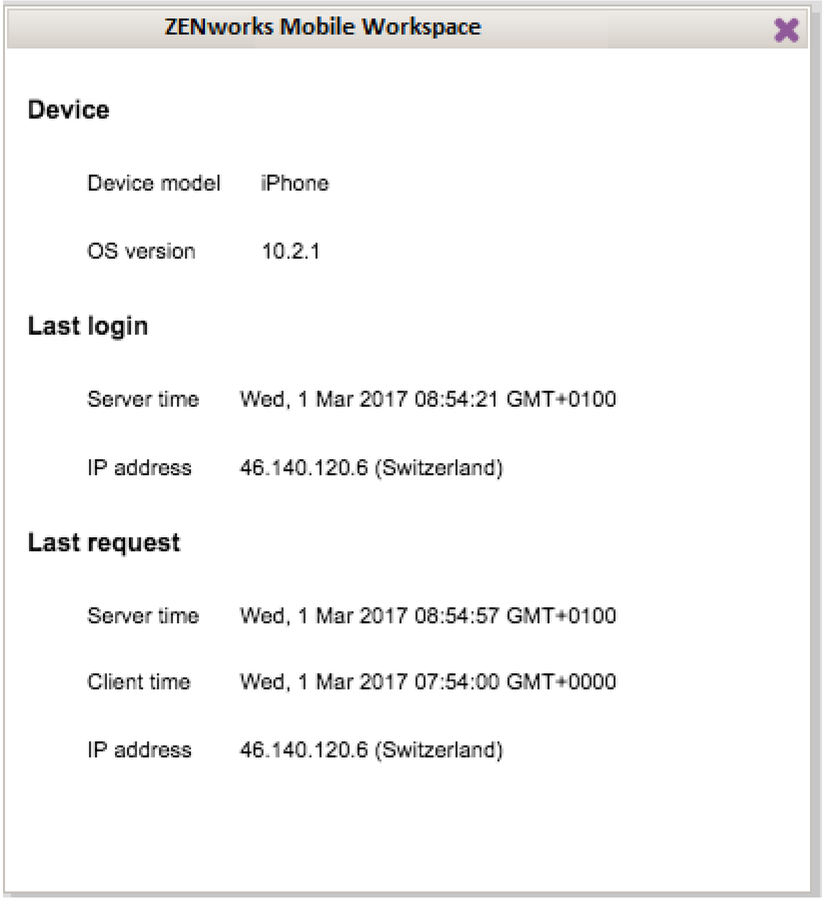
Active enrollment (optional): If your server has been configured to use the secure activation, this button allow an administrator to generate an enrollment code for the user. Therefore, this enrollment code is displayed in this screen and in the user's download portal as well.

If a user's status is *Disabled*, a reason is displayed:

- **No license available** - You have reached the maximum limit on users allowed by your license or your license has expired.
- **Never been enabled** - The user was disabled by default at the time of importation because he/she never enrolled.
- **Max formal tries reached** - The user has attempted to log in with the wrong password, multiple times.
- **Disabled by an administrator** - An administrator has locked the user.

Otherwise, the status will be *Enabled*.

Applications: This list displays all applications that have been enrolled.



ZENworks Mobile Workspace

Device

Device model iPhone

OS version 10.2.1

Last login

Server time Wed, 1 Mar 2017 08:54:21 GMT+0100

IP address 46.140.120.6 (Switzerland)

Last request

Server time Wed, 1 Mar 2017 08:54:57 GMT+0100

Client time Wed, 1 Mar 2017 07:54:00 GMT+0000

IP address 46.140.120.6 (Switzerland)

You can see information about an application by clicking on the question mark:

Device: Gives some information about the device that runs the application.

Last login/request: Gives some information about the last login and last business request:

- **Server time:** The server date/time at which the login was made
- **Client time:** The device date/time at which the login was made
- **IP address:** The IP address from which the server received the last login request. The country (or network) related to the IP address is shown in parentheses.
- **Geolocation:** The GPS location from which the server received the last login request based on GPS coordinates sent by the workspace application.

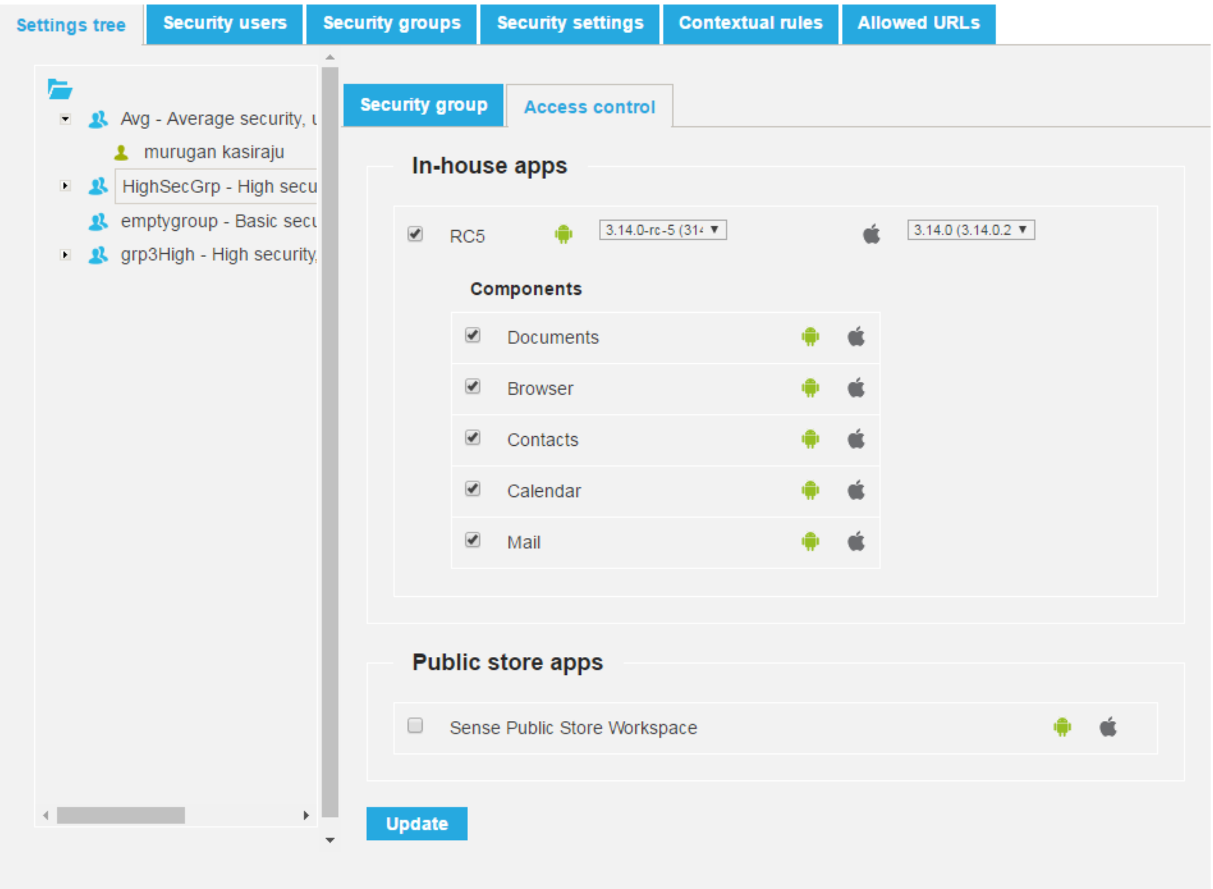
5.4 Settings Tree

The Settings Tree gives an overview of all security groups created, the security users in each group, and the mobile device(s) possessed by each security user. For more information on a specific element, select it and wait for the content panel to update.

The Settings Tree also provides an easy way to quickly edit and update the security groups, security users, and mobile devices. You can select an item, edit it, and click the *Update* button to apply the modification.

5.4.1 Access Control

When you select a group in the *Settings tree*, you will be able to define the applications and versions the users belonging to that group will be allowed to use.



In-house apps

☑ RC5 3.14.0-rc-5 (31‹ ▼ 3.14.0 (3.14.0.2 ▼

Components

☑ Documents

☑ Browser

☑ Contacts

☑ Calendar

☑ Mail

Public store apps

□ Sense Public Store Workspace

5.5 Allowed URLs

Simple HTTP requests sent via the ZENworks Mobile Workspace application are automatically wrapped and sent through ZENworks Mobile Workspace proxy. For these applications, ZENworks

Mobile Workspace acts as a VPN, allowing the ZENworks Mobile Workspace app to make HTTP requests as if it were within the internal network.

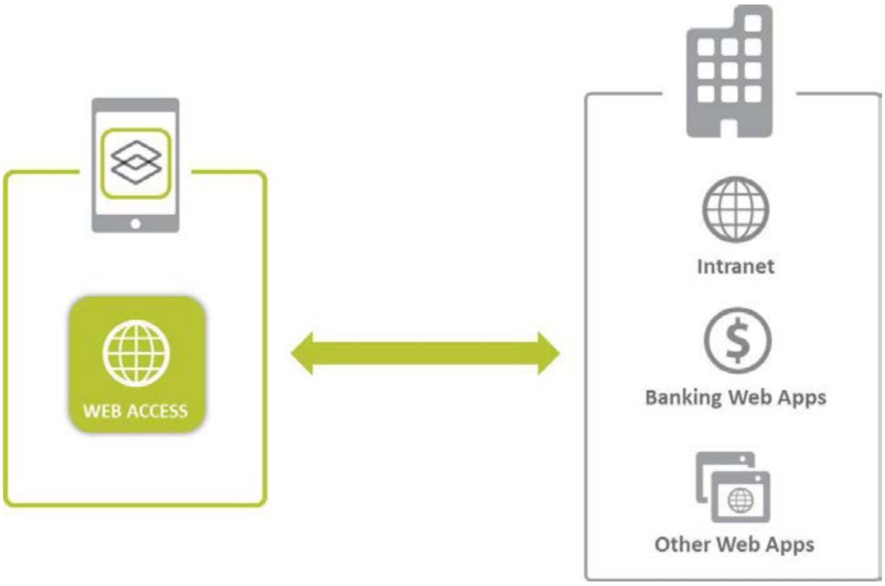
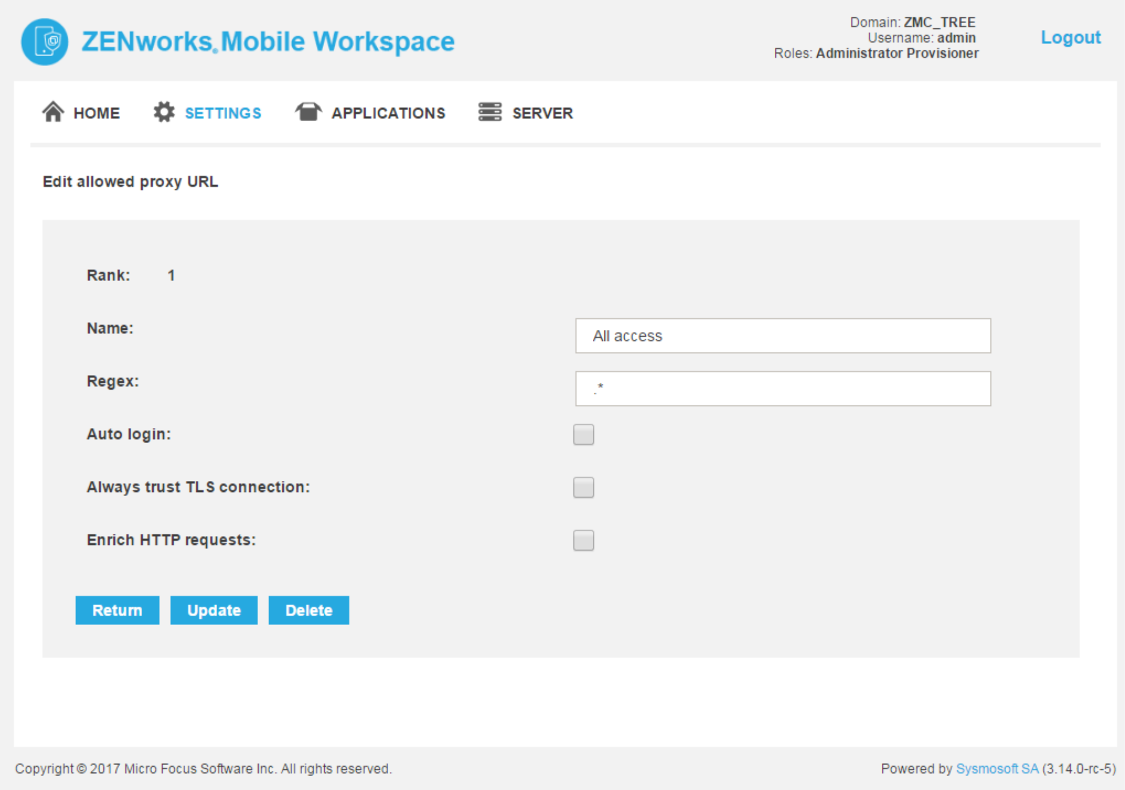


Figure 39: Proxy schema

To avoid unauthorized access from outside, ZENworks Mobile Workspace proxy allows access to back end resources based on a white list. Using the *First*, *Last*, *Up,* and *Down* buttons, the URLs can be ranked by priority.

Click on the plus sign icon to add a URL to the white list.



Edit allowed proxy URL

Rank: 1

Name: All access

Regex: .*

Auto login: □

Always trust TLS connection: □

Enrich HTTP requests: □

Powered by Sysmosoft SA (3.14.0-rc-5)

Name: Name of the rule.

Regex: 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 http://www.regular-expressions.info/ website and can be tested on this website: http://www.fileformat.info/tool/regex.htm.

Auto login: If the checkbox is selected, 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.**

Always trust TLS connection: If this option is selected, any certificate will be accepted (the validity of the certificate will not be checked).

Enrich HTTP requests: Allow the proxy to enrich client HTTP requests with the following headers:

- **x-sense-client-ip-country**: Country name based on the IP seen by ZENworks Mobile Workspace
- **x-sense-client-ip-address**: IP address of the client seen by ZENworks Mobile Workspace
- **x-sense-client-location**: GPS coordinates and precision of the device

- **x-sense-client-time**: Date/time of the device
- **x-sense-identity-domain**: User’s domain
- **x-sense-identity-name**: User’s username
- **x-sense-identity-group**: Name of the group to which the user belongs