ZENworks Mobile Workspace

Migration guide

Version 3.18.4 - March 2019

Table of Contents

Overview

Usually, an update of the ZENworks Mobile Workspace application server to a newer version only requires to execute the installer tool.

However, some manual operations may be necessary to ensure the proper functioning of the product.

This guide describes the required steps to finalize the migration to the desired supported version. All instructions for versions between the previous version and the updated version need to be followed.

From ZENworks Mobile Workspace 3.X to ZENworks Mobile Workspace 3.18

Introduction

This version introduces the push configuration per application.

Required

Server applications

Push configuration

Since ZENworks Mobile Workspace 3.18.0, push is no longer configured globally on the server, but on a per-application basis directly from the administration console.

The private keys and configuration have changed and need to be gathered from Apple's and Google's Firebase developer consoles, respectively.

Read the documentation for more information:

- **System Administration/security_admin**
  - Business and Security configuration
    - APPLICATIONS
      - Push configuration

Optional

Server applications

Push configuration

For NPNS configuration

The files (that are no longer needed on the file system) must be kept aside since they must be uploaded to the server through the administration console (format hasn't changed with ZENworks Mobile Workspace 3.18).

Unix

- Delete the `$ZENworksMobileWorkspace_HOME/lib/npnsCertificate.crt` file
- Delete the `$ZENworksMobileWorkspace_HOME/lib/npnsKey.pem` file
- Update the `$ZENworksMobileWorkspace_HOME/bin/setenv.sh` file by removing the `JAVA_OPTS` for GCM (and his comment)

Windows

- Delete the `$ZENworksMobileWorkspace_HOME\lib\npnsCertificate.crt` file
- Delete the `$ZENworksMobileWorkspace_HOME\lib\npnsKey.pem` file
- Run the `$ZENworksMobileWorkspace_HOME\services\SENSE-SERVER_service_manager.bat` script
  - Under *Java* Tab, remove the Java Options for GCM:
    - `-Dgoogle.gcm.apikey=⋯`

Log4j configuration

The logging service has been upgraded to use the version 2 of Log4J (Log4j2). The configuration file use a slightly different syntax and must be modified in accordance.

For all default configuration, the ZENworks Mobile Workspace installer tool takes care of the migration. But if custom modifications had been done on the default configuration, they must be manually added again on the new configuration.

Example for a custom logger:

from conf/log4j.xml

```
<logger name="org.apache.http">
    <level value="DEBUG"/>
</logger>
```

to lib/log4j2.xml

```
<Logger name="org.apache.http" level="DEBUG" />
```

For more complex statements, please refer to the official documentation: Migrating from Log4j 1.x

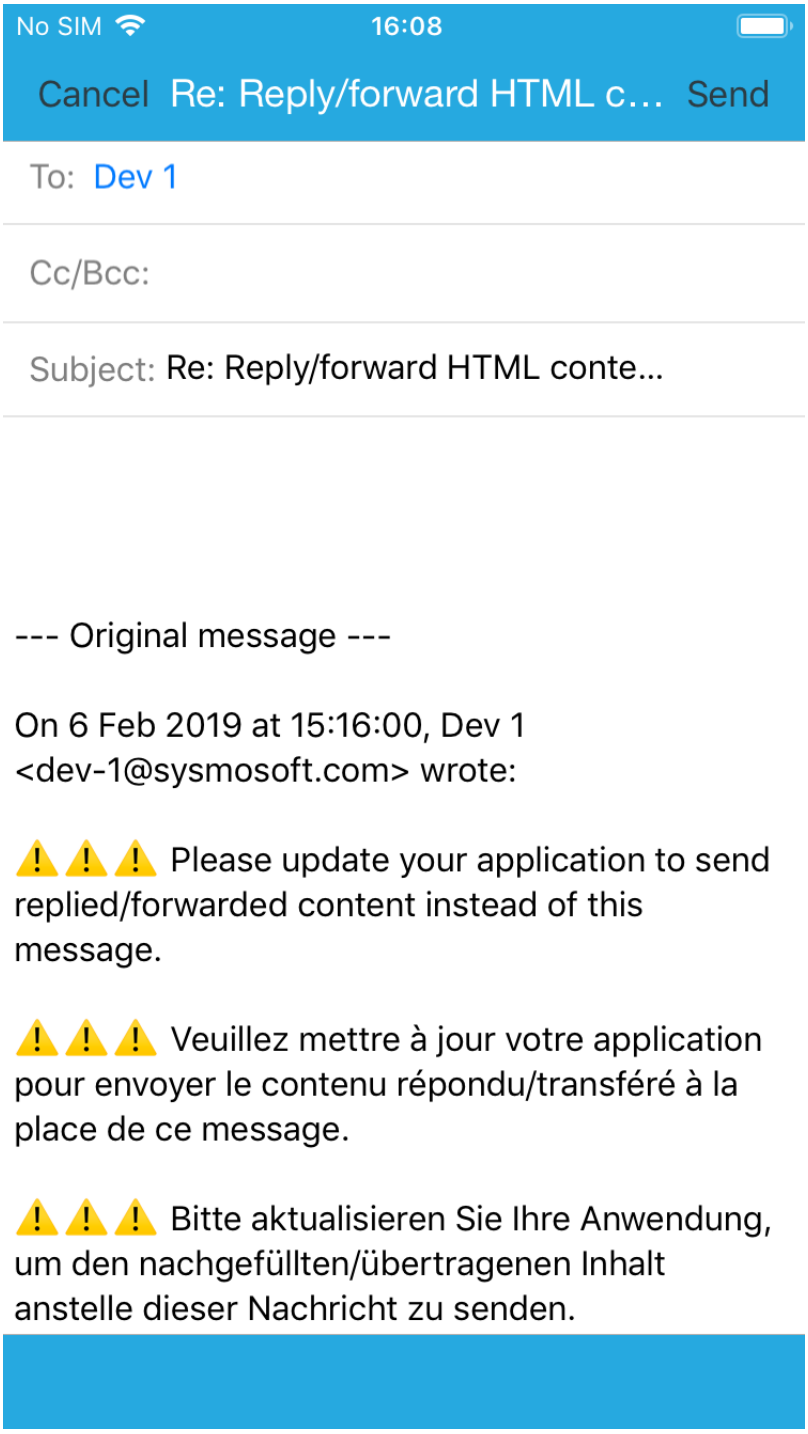
For information

Reply/forward HTML content

Support of HTML content when reply or forward an email is now effective with ZENworks Mobile Workspace application.

Clients still running an applications older than 3.18.4 version will be invited to update their application through a dedicated message taking the place of the regular replied/forwarded content.

See how it is submitted:



From ZENworks Mobile Workspace 3.X to ZENworks Mobile Workspace 3.17

Introduction

This version offers LDAP password changing features (including notifications when the password is about to expire), caller identification based on Workspace contacts, new settings for the browser (admin.configured homepage and web apps), and contains several hidden features for the Smart Contract project.

Required

Server applications

LDAP configuration

In order to be able to enable the password changing features, LDAP authentication must be configured, and the URL must be set using `ldaps://` since TLS is required to be able to change passwords.

Log4j configuration

The new *Windows network share* implementation for the *Document* application that supports SMB2 uses a library that is extremely verbose at `INFO` level and should log only from the `WARN` level.

The following logger configuration should be added to the `conf/log4j.xml` file:

conf/log4j.xml

```
<logger name="com.hierynomus.smbj">
    <level value="WARN" />
</logger>
```

Optional

Customer infrastructure

For most customers, no change is required.

The Tomcat server provided by the Workspace installer has been updated from branch 8.0 to branch 8.5, which now supports virtual hosts.

If a TLS HTTP connector has been manually configured in the `server.xml` with a keystore that contains more than one certificate entry, the `keyAlias` is required as documented in the *Troubleshooting* section of the Tomcat SSL/TLS Configuration HOW-TO.

From ZENworks Mobile Workspace 3.X to ZENworks Mobile Workspace 3.16

Introduction

This version contains a new workspace camera component, newly supported mail attachments file extensions, and simplified server configuration. While most steps are handled automatically by the installer, some post-install configuration may be required.

Required

Server applications

SSL/TLS certificates

While using a custom SSL/TLS trust store (set by the `-Djavax.net.ssl.trustStore=⋯` property in the server startup script) should still work, it is recommended to rely on the default installed trust store (by removing the `javax.net.ssl` system properties) and add trusted certificates directly in the administration console for easier management.

LDAP configuration

Since the LDAP configuration has been simplified, the migration to version 3.16 removes the duplicated authentication and synchronization configuration, and the configuration after the migration needs to be manually checked and eventually fixed. See the main ZENworks Mobile Workspace documentation for more information:

- **System Administration/security_admin**
  - Technical configuration
    - DOMAINS
      - Create a new domain
        - Identities

The LDAP URL must contain the server, the root DN and nothing more. If the relative context was set in the base URL, it must be moved to the new dedicated field.

If the any of the domain was using special synchronization parameters that are encoded in the LDAP URL and separated with semicolons, these must manually be set in the dedicated fields (original synchronization URL is preserved during update):

- Second parameter contains the *relative LDAP context* (context relative to the root DN), it must be moved to the dedicated field if configured.
- Third parameter contains the *LDAP attribute to use as username*, it must be moved to the dedicated field if configured (this parameter is normally only set when custom authentication is configured).

- Fourth parameter is not supported anymore (it was used to use a part of the username attribute's value). Please use a dedicated LDAP attribute to use as username instead.
- Fifth parameter contains the *search filter*, it must be moved to the dedicated field if configured.

Workspace camera feature

The new *camera* component is now part of the workspace application, but is disabled by default. It must be manually enabled for groups that require it.

New supported media extensions attachment

In the *workspace* configuration, all file extensions that are supported since version 3.16 are automatically added when the server is updated. If these new attachment extensions should not be allowed to be opened on the mobile application, they may be removed.

Customer infrastructure

For most customers, no change is required.

If there's a reverse-proxy (or equivalent network appliance) that filters *internal* request between server modules (eg. from the proxy to the security server), integrators must ensure that all the the `/sense/secserver/ServletServiceAccess/*` URLs can be accessed instead of just only the plain `/sense/secserver/ServletServiceAccess` URL. The reason is that each service is now exposed on its own URL. There should be only level and no URL parameter (services are accessed through the HTTP POST method).

If there's a reverse-proxy and that reverse-proxy does HTTP header and/or content analysis/filtering, integrators must be aware that since ZENworks Mobile Workspace 3.16.0, the requests are still authenticated with a HMAC, but the implementation has been improved in terms of security and efficiency:

- The data messages are transferred in binary instead of XML messages containing base-64 encoded text.
- The HMAC value is transferred in a `x-sense-authentication-hmac` HTTP header.

From ZENworks Mobile Workspace 3.X to ZENworks Mobile Workspace 3.15

Introduction

This version introduces an important change in the way the client applications are accessing the ZENworks Mobile Workspace server, the security server can now be deployed behind the proxy server, adding the possibility to deploy it in a separate DMZ, leaving only the proxy server exposed.

Optional

Server applications

A cleaning can be done in the *sense-server-config.properties*: the `applicationDownloadExternalUrl` key-value entry containing the *external* URL of the ZENworks Mobile Workspace server can be removed since it is not used anymore.

Customer infrastructure

If there's a reverse-proxy (or equivalent network appliance) that filters request, integrators must ensure that the `/sense/appserver/Server` can be accessed through the HTTP GET method (it should already be the case), and that HTTP GET parameters are forwarded to the ZENworks Mobile Workspace server since application delivery and updates will be downloaded through this URL with a download parameter (eg. *https://example.org/sense/appserver/Server?download=e45288e5-6731-459f-afea-3796e7d6ba99.plist*).

Reverse-proxy URL rewriting with ZENworks Mobile Workspace 3.15.0 and 3.15.1

If the proxy context path is rewritten on the reverse-proxy, for example `/mobile/Server` instead of `/sense/appserver/Server`, the proxy WAR must be deployed under the same name as the *external* context path. In this example, the *sense#appserver.xml* file must be renamed to *mobile.xml* in order to change the *internal* context path. The renamed file will normally be kept in future updates.

If the file is not renamed, application download on iOS won't work properly.

Check that the HTTP connector in the *server.xml* file is configured according to our integration guidelines.

ZENworks Mobile Workspace 3.15.2, 3.16.0 and later versions are relying on the proxy URL and don't require these infrastructure changes

The `/sense/secserver/download/` path won't be used anymore and can be removed from reverse-proxy rules immediately after update

The `/sense/secserver/ServletAuthentication` path can be removed from reverse-proxy rules once *all* client application are up-to-date (otherwise, they will need to be updated manually by downloading them through the distribution server).