AppBox Configuration

DME 4.6 • G/On 5.7

How to install and set up AppBox for DME

Document version 2.3

Published 09-05-2017

Soliton®

Contents

Introduction

This is the manual for setting up AppBox for DME. The manual describes how to install the G/On server needed for AppBox, and also describes how to set up both G/On and DME.

The manual does not cover the installation of DME itself. Please refer to the DME documentation at

`resources.solitonsystems.com`

Copyright information

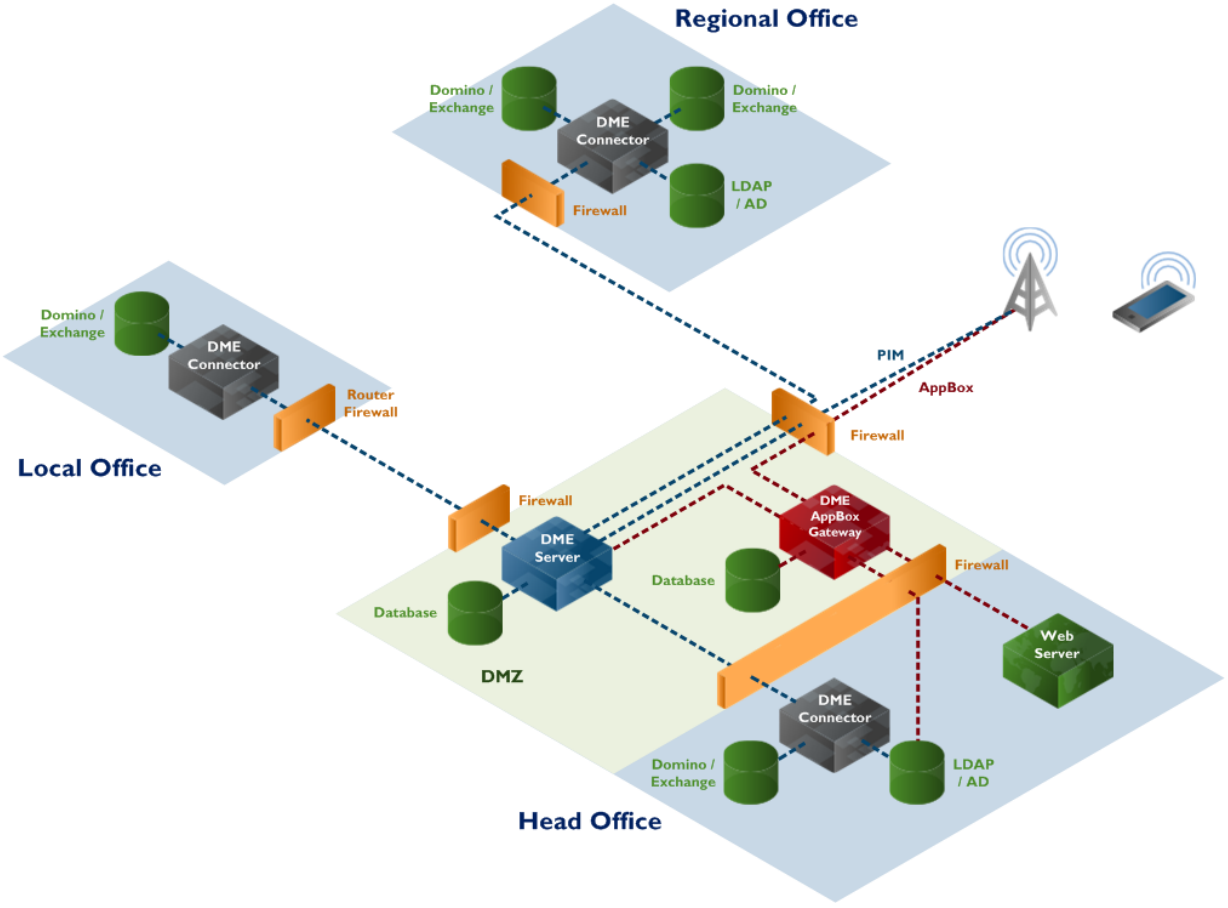
Company Information

Soliton Systems
Spotorno Allé 12
2630 Taastrup
Denmark
Phone +45 70 216 800
mail@solitonsystems.com
www.solitonsystems.com

Overview

The G/On server (also known as the DME AppBox Gateway) controls the access to DME AppBox applications. It communicates with the DME server, and with the user directory, checking credentials and devices. Then it can give access to websites and to Web servers running the AppBox applications.

For a more detailed description of the DME server architecture, please refer to the *DME Server Administration Reference* that can be found at `resources.solitonsystems.com`



Installation

This chapter shows you how to install G/On for AppBox use with DME.

If you are planning to install G/On for G/On use only, please consult the G/On manuals instead. These can be found at Giritech's website `www.giritech.com/Support-Download/Product-Download/G-On-5.7-Product-Download`

It is also possible to install the two parts of the G/On Server system (the G/On Gateway Server and the G/On Management Server) on different machines, and it is possible to install several G/On Gateway Servers. For more information, see the G/On Server Manual, in the section on how to create Gateway Server installer. This manual can also be found at Giritech's website.

It is assumed that DME is already installed and running. If you do not already have a DME installation, please contact Soliton Systems or a DME partner. Visit `www.solitonsystems.com` for more information.

Note that AppBox requires **DME 4.0 or later**.

Before installation

Supported Platforms

G/On supports the following platforms:

- **Windows Server 2003R2**
- **Windows Server 2008**
- **Windows Server 2008R2**
- **Windows Server 2012**
- **Windows Server 2012R2**

Database:

- **SQLite (build-in)**
- **MS SQL Server 2005**
- **MS SQL Server 2008**
- **MS SQL Server 2008R2**
- **MS SQL Server 2012**

Firewall openings

For the G/On server to be working, the following firewall openings must be ready:

- From the internet to the external connect address for the G/On server, on the desired port, usually 443 or 3945.
  - Please note that both the address and the port are fixed values, that have been determined at the time of ordering G/On. The connection address and port are part of the license. If using the demo license, any address can be specified.

    The address and port can be found in one of these license files in the Giritech folder:

    `Giritech/gon_5.7.x-x/config/deployed/gon_license.lic`

    `Giritech/gon_5.7.x-x/config/deployed/dme_license.txt`

    ```
    Maintenance Expiration Date: 2012-12-31
    Client Connect Address: 48.246.27.213
    Feature: Multiple Client Connect Ports
    Client Connect Port: 3945
    Feature: HTTP Encapsulation
    ```
- From the G/On server to the DME server on the DME server port.
- From the G/On server to any web servers to be used through AppBox.

Java Runtime Environment

The G/On 5 Server Configuration and G/On 5 Management requires that Java Runtime Environment (JRE) is installed. It should already have been installed with the DME installation, but otherwise it can found here:

`http://www.java.com`

Note: On 64 bit systems, a 64 bit version of JRE is expected to be installed, and the 64 bit version of G/On Server Configuration and G/On Management should be used (both the 32 and 64 bit versions are present in the installation).

Known limitations

- HTML 5 applications that rely on one of the following features are currently not supported in AppBox:
  - Web Sockets.
  - HTML5 offline manifest. Use AppBox offline manifest instead.
  - Web SQL.

- HTML Video and audio elements. For more information on audio and video, please see
  http://resources.solitonsystems.com/content/appbox-development

Installation

The G/On installer comes automatically with the DME installer, but the latest installer can be downloaded from Giritech's website:

http://www.giritech.com/Support-Download/Product-Download/G-On-5.7-Product-Download

Store it on the server where you wish to install G/On.

1. Open the installer.
2. Wait while the installer is loading.
3. Click **Next**:

4. Read the License Agreement and click **I Agree**.
5. Click **Install** and wait while G/On is installed.

6. When done click **Finish**:

7. G/On is now installed and you are ready to configure the G/On server.

Configuration

The complete configuration consists of the following steps:

1. Copy the license to the G/On Server.
2. G/On Server Configuration: entering the network information that G/On needs to know.
3. Starting the G/On Services.
4. DME Configuration: letting DME know how the clients should connect to the G/On server.
5. G/On Management: setting up authorization for AppBox use.

Copy license file to G/On Server

Copy your license file `dme_license.txt` to the server in the folder

`Giritech/gon_5.7.x-x/config/deployed`

Start G/On Configuration

If the G/On Server Configuration wizard is not started automatically after installation, it can either:

- be started from the Windows Start menu, or
- be started from one of these locations in the Giritech folder.

  On 32 bit systems the version in the win folder should be used:

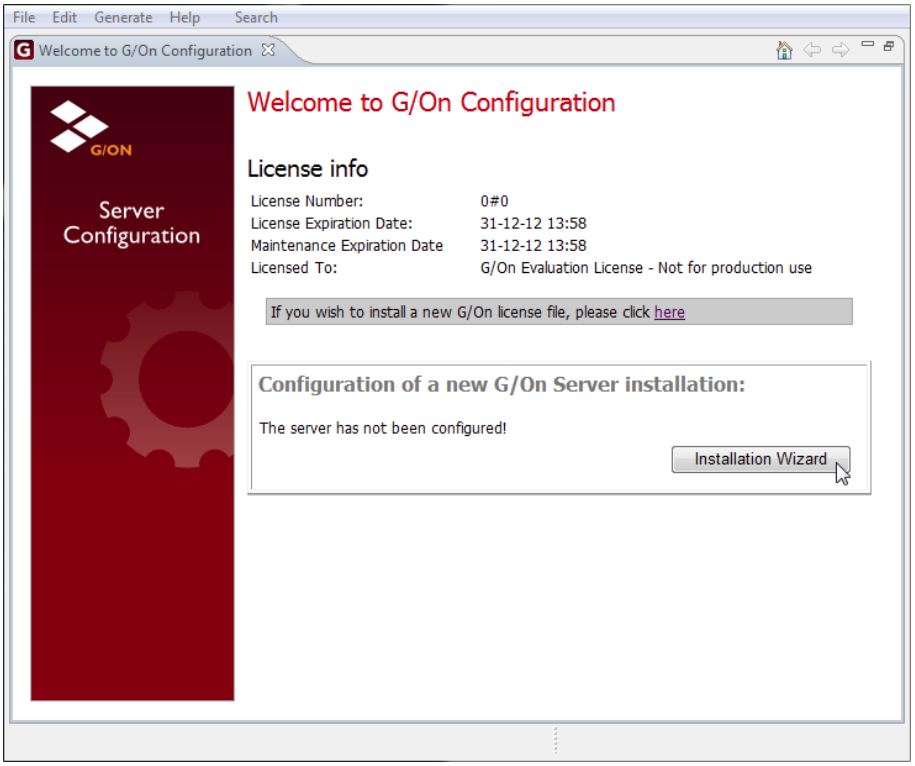
  `Giritech/gon_5.7.x-x/gon_config/win/gon_config.exe`

  On 64 bit systems the version in the win64 folder should be used:

  `Giritech/gon_5.7.x-x/gon_config/win64/gon_config.exe`

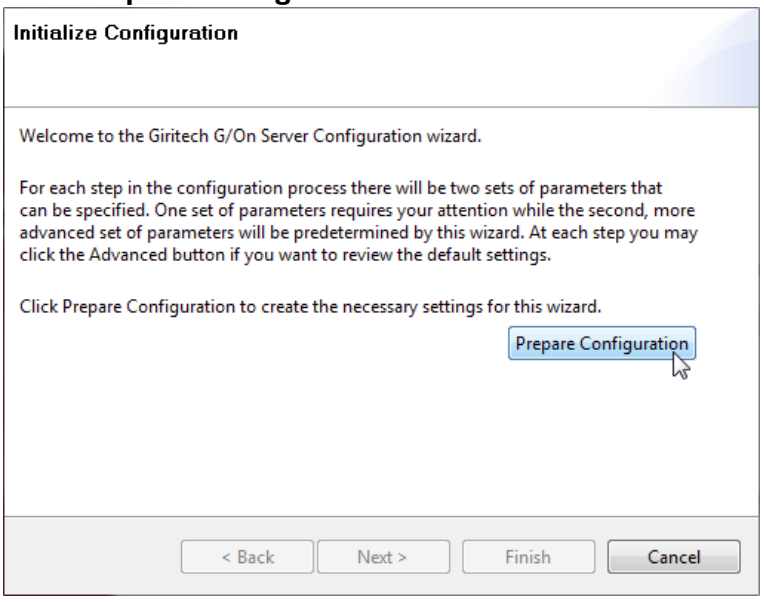
G/On Configuration

1. Click **Installation Wizard**:



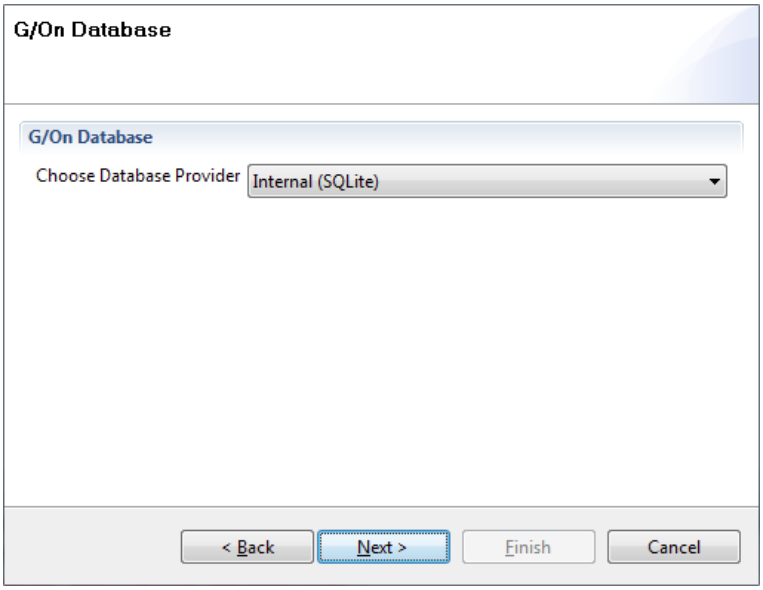
Note: If your license doesn't show up in this window, click the link to install a new G/On license file.

2. Click **Prepare Configuration**:



3. When done click **Next**.

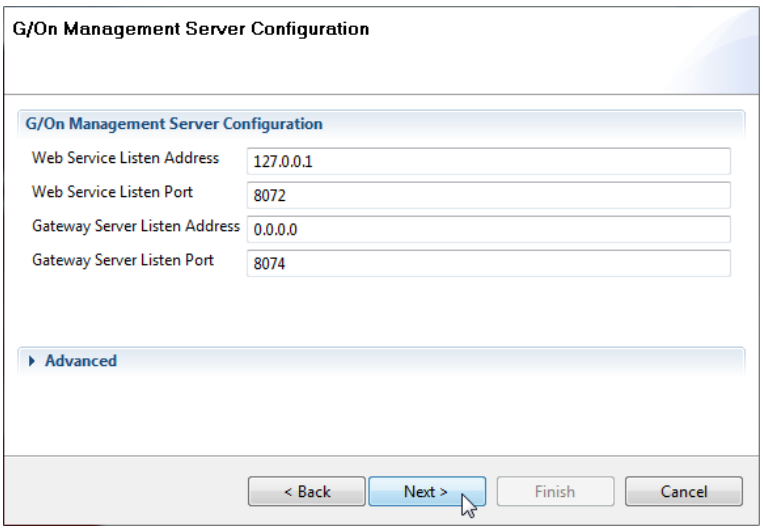
4. Choose database:



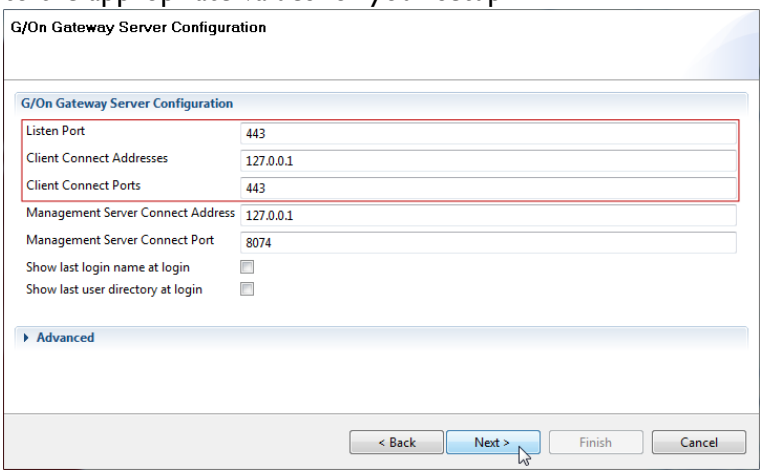
- If the installation only will have a single Gateway server, the **Internal (SQLite)** database can be chosen.
- If the installation will have multiple Gateway servers, select **Microsoft SQL Server**.

Then click **Next**.

5. No need to change the G/On Management Server configuration, so just click **Next**:



6. In the G/On Gateway Server Configuration, change the following fields to the appropriate values for your setup



- **Listen Port:** The port that the Gateway Server listens on in order to accept connections from G/On Clients.
- **Client Connect Addresses:** This is the IP address (DNS name or number), that the clients will use to connect to the G/On server.
  Please note that both the address and the port are fixed values that have been determined at the time of ordering G/On. The connection address and port are part of the license. If using the demo license, any address can be specified.

  The address and port can be found in one of these license files in the Giritech folder:

  `Giritech/gon_5.7.x-x/config/deployed/gon_license.lic`

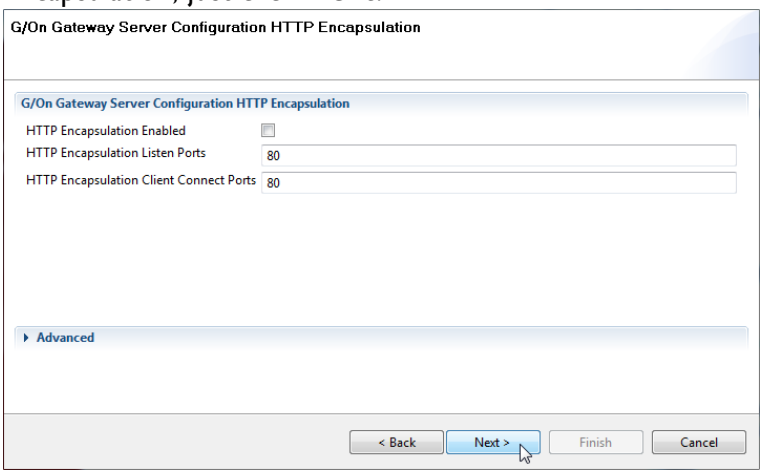
  `Giritech/gon_5.7.x-x/config/deployed/dme_license.txt`

```
Maintenance Expiration Date: 2012-12-31
Client Connect Address: 48.246.27.213
Feature: Multiple Client Connect Ports
Client Connect Port: 3945
Feature: HTTP Encapsulation
```

- **Client Connect Ports:** See the above for a description on how to find the port number.

Then click **Next**.

7. No need to change G/On Gateway Server Configuration HTTP Encapsulation, just click **Next**:



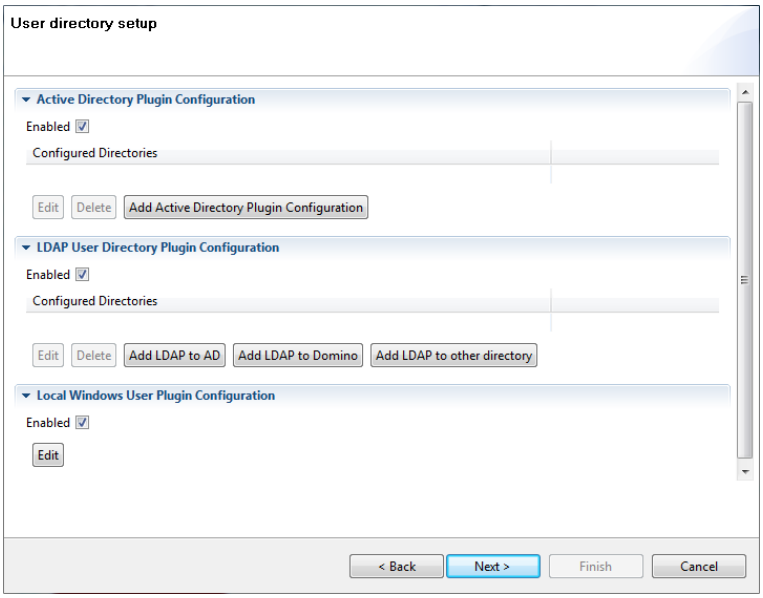
8. Identity management in G/On is through one or more of these directory services:

   - Active Directory (Microsoft Active Directory, AD).
   - LDAP (Lightweight Directory Access Protocol). Using the LDAP protocol from an LDAP enabled user directory.
   - Local users and groups on the G/On server machine.

   Note that Active Directory and LDAP are license features and therefore may not be available.

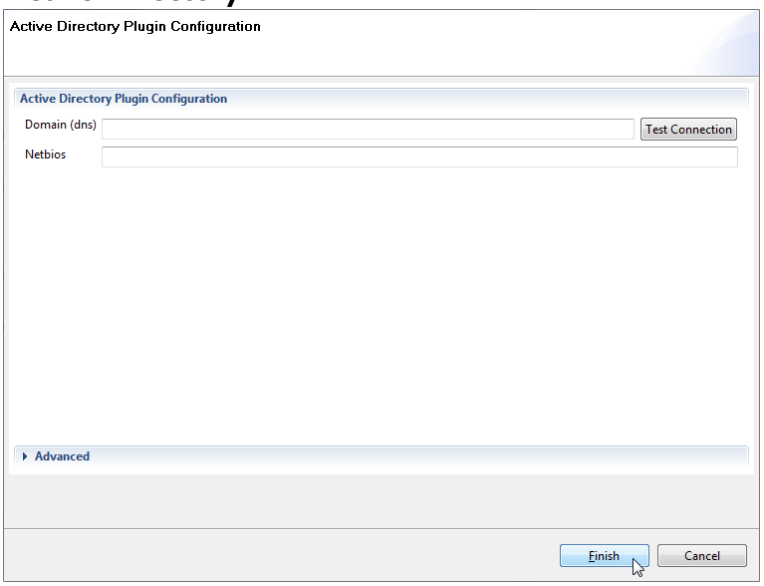
   Each user directory service can be enabled/disabled using the Enabled checkboxes.

   - For Active Directory and LDAP it is possible to add any number of different directory specifications.
   - For Local Windows User plugin, there can only be one instance.



Clicking **Add** or **Edit** will open new window with specification, as described below. For full description of the advanced fields and for more information, please consult the G/On Server Manual, that can be downloaded from Giritech's webpage: `www.giritech.com`

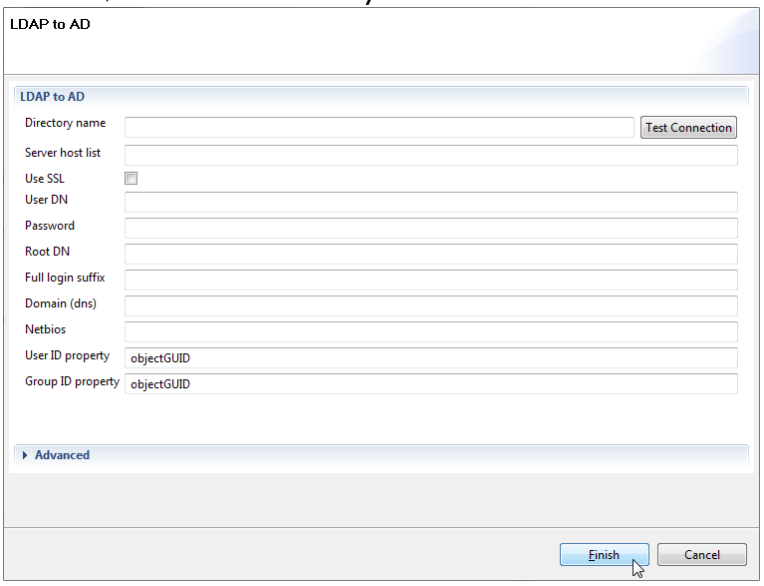
8.1. Active Directory



- **Domain (dns).** The domain (dns) name of the Active Directory domain, e.g. mycompany.com. Must be specified
- **Netbios.** Normally the Netbios name is automatically filled in. If this does not happen, please fill in the Netbios name manually

8.2. LDAP

LDAP can be specified to be used against Active Directory, Domino, or another directory.



- **Directory name.** This name will be used to identify users and groups from this LDAP directory. This name should

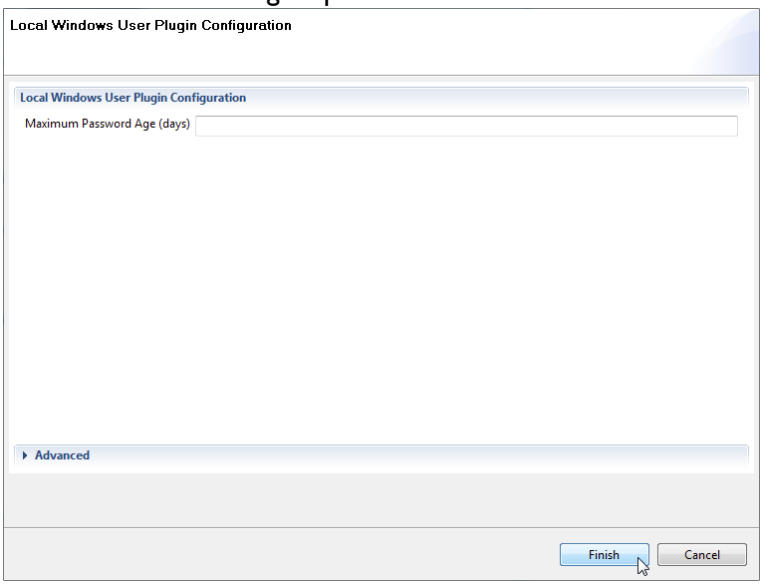
never be changed once users and groups have been entered in the system. Click **Test Connection** to verify that you entered the directory name correctly.

- **Server host list.** A comma-separated list of servers for the LDAP directory. Port number is assumed to be 389 unless specified. Example: `firstserver:636, secondserver, thirdserver`
- **Use SSL.** Set this if SSL communication is used.
- **User DN.** Name (dn) of user account used to connect to LDAP. Leave blank if anonymous access is enabled in the user directory.
  Note: Active Directory does not allow anonymous access.
  Example: `cn=myuser,ou=myorgunit,dc=mydomain,dc=com`
- **Password.** Password for the user account.
- **Full login suffix.** If more than one user directory is used, there may be clashes in the login names. In this case the users must enter a full login, which is the normal login succeded by an @ and the Full login suffix (e.g. `username@mydirectory`). So the login suffix is used to distinguish users from this directory from other users. If left blank the Directory name is used as suffix.
- **Domain (dns).** LDAP to AD only. The domain DNS name used when launching applications using the user.domain variable.
- **Netbios.** The domain Netbios name used when launching applications using the user.netbios variable.
- **User ID property.** To make sure that a user is always uniquely identified, the User ID property determines which property in the user directory to use as this unique identifier. Default value for LDAP to AD is `objectGUID`. Default value for LDAP to Domino is `uid`
- **Group ID property.** To make sure that a group is also always uniquely identified, the Group ID property determines which property in the user directory to use as this unique identifier. Default value for LDAP to AD is also `objectGUID`. Default value for LDAP to Domino is `dn`

8.3. Local Windows User

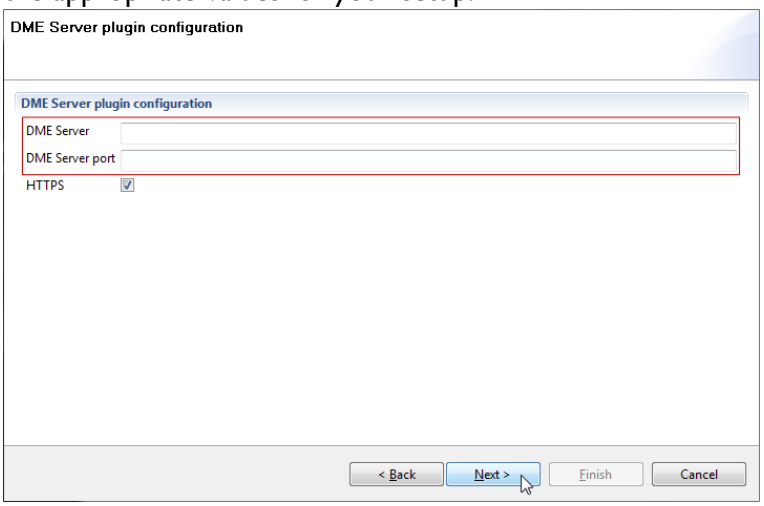
In order for this to work, the G/On Management and all Gateway servers should run on the same machine, so they will “see” the

same local users and groups.



- **Maximum Password Age (days).** When a user's password is older than this limit, G/On will ask the user to change the password.

9. In the DME Server plugin configuration, change the following fields to the appropriate values for your setup:



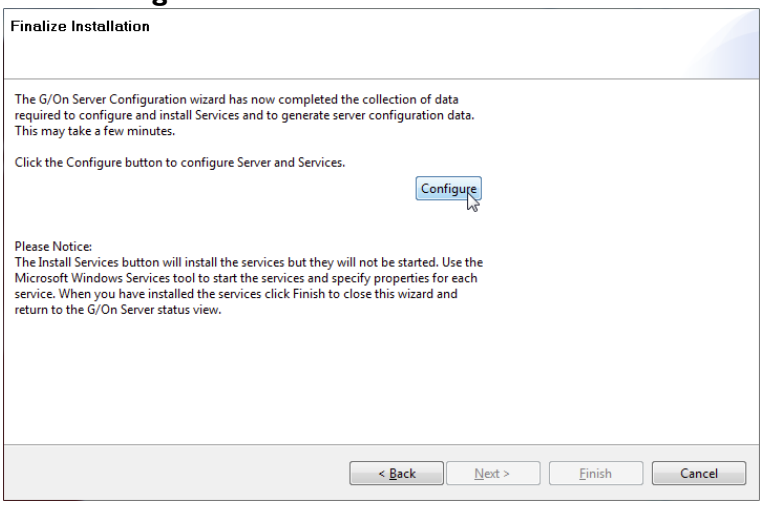
- **DME Server.** This is the fully qualified domain name (FQDN) that the G/On server must use for connecting to the DME server. See note below.
- **DME Server port.** The port number.

Note: The SSL certificate for the secure DME server is created using the DME server FQDN, for instance `dme.company.com`. Therefore you must specify the FQDN in the **DME Server** field. With both the DME and G/On servers in the DMZ segment, this might require you to make a new entry in the G/On Server's `hosts` file, in which you point the FQDN to the internal IP address of the DME Server.

It is also possible to use a split DNS setup instead of the `hosts` file.

Then click **Next**.

10. Click **Configure**:



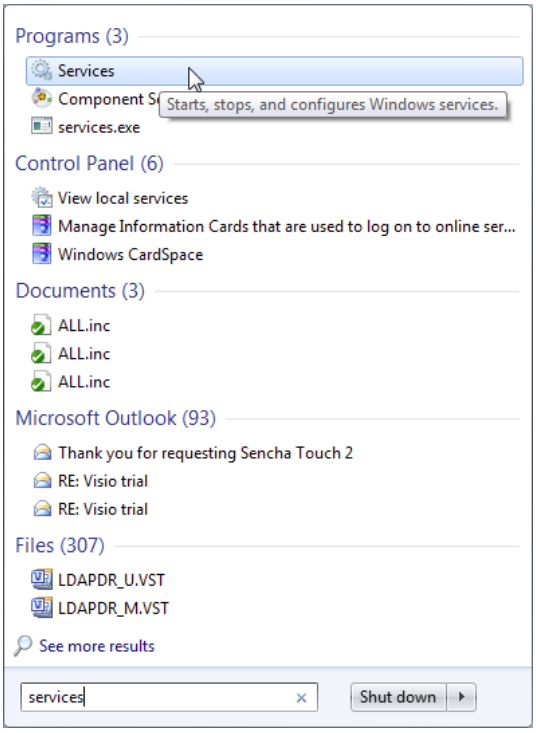
11. When done, click **Finish**.

Starting the G/On Services

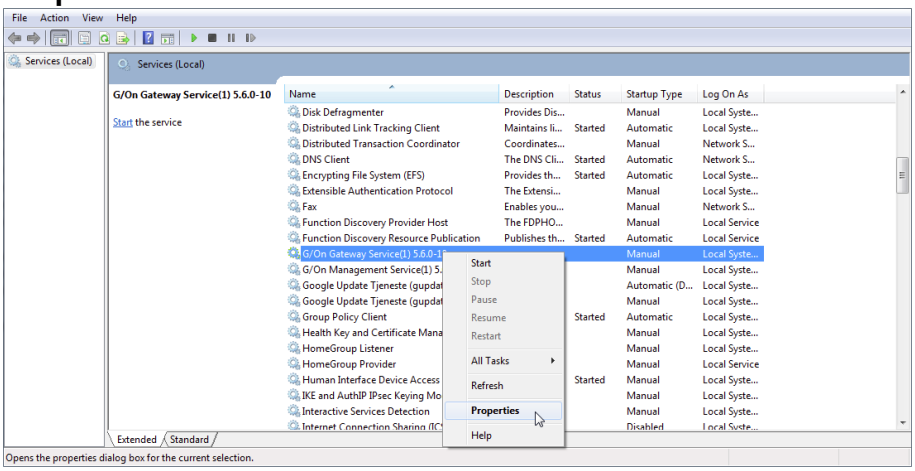
After configuring the G/On Server, you need to start the G/On Management Server and the G/On Gateway Server.

Starting the Services

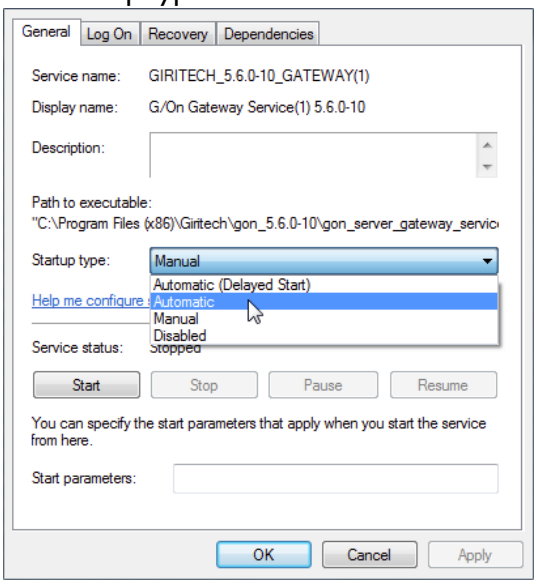
1. Start Windows Services. This can be done by opening the Windows Start menu and search for "services". Click **Services**:



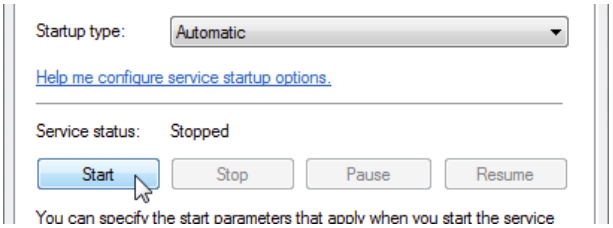
2. Find the **G/On Gateway Service**. Right-click it and select **Properties**:



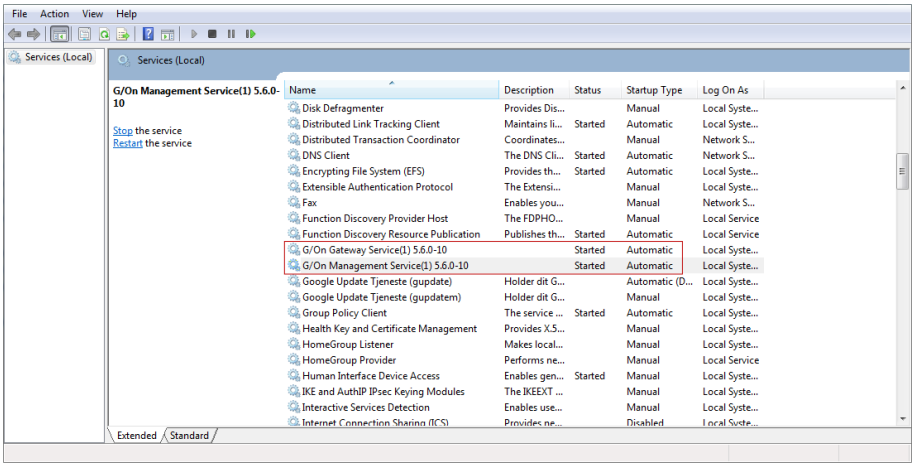
3. Set Startup type to **Automatic**:



4. Click **Start**. Then click **OK**:



5. Do the same for the G/On Management Service. The final result should look like this:



DME Configuration

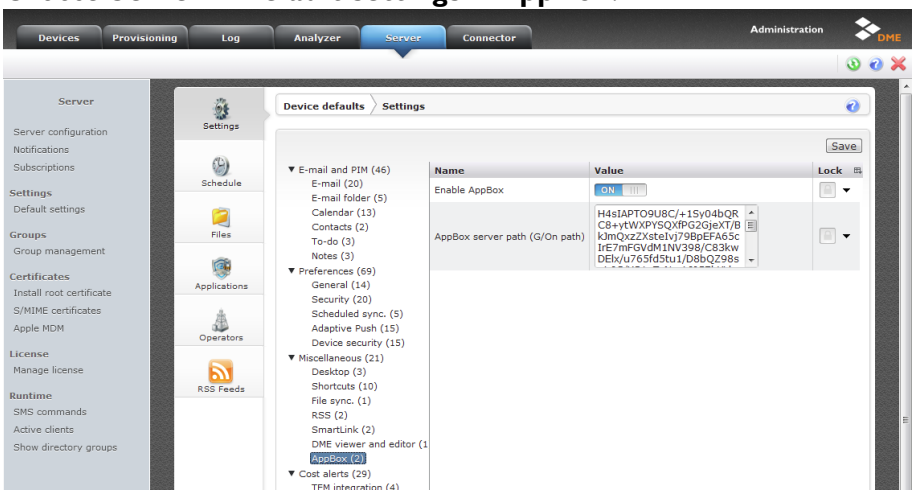
Now we need to make sure that DME has AppBox enabled and knows the G/On connection info.

1. Open the file

`Giritech/gon_5.7.x-x/config/deployed/gon_connect_info.dat`

in Notepad, and copy the contents.

2. Log into the DME Administration.
3. Choose **Server > Default settings > AppBox**:



4. Make sure **Enable AppBox** is **ON**.

   Insert the copied contents in the field **AppBox server path (G/On path)**.

G/On Management

The G/On Management handles the authentication and authorization for AppBox, and therefore access needs to be set up here.

Start G/On Management

Either:

- Find the program in the Windows Start menu, or
- Find the program in one of these locations within the Giritech folder.

  On 32 bit systems the version in the win folder should be used:

  `Giritech/gon_5.7.x-x/gon_config/win/gon_config.exe`

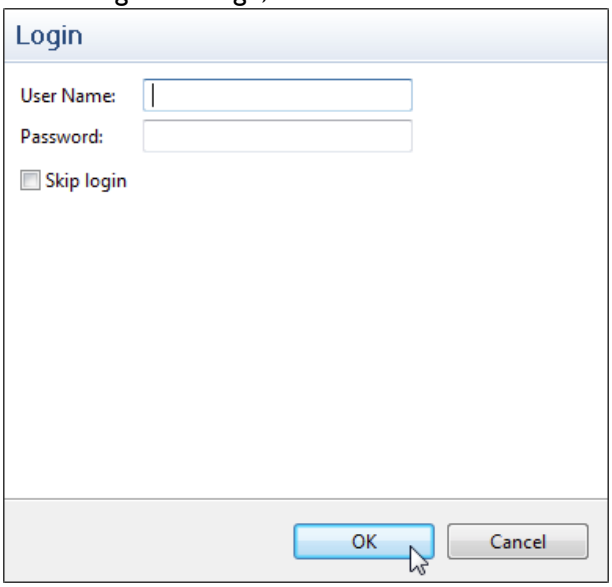
  On 64 bit systems the version in the win64 folder should be used:

  `Giritech/gon_5.7.x-x/gon_config/win64/gon_config.exe`

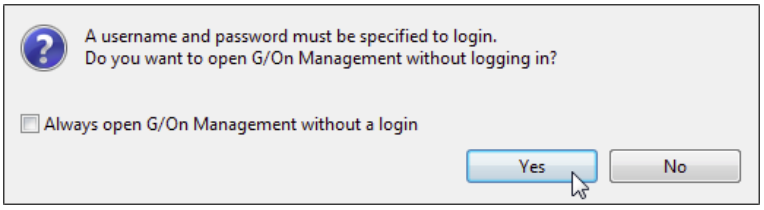
Note: On Windows Server 2008 and 2012, you must run the G/On Server Management program as Administrator. To do this right-click the program and choose **Run as Administrator**.

Management

5. In the Login message, click **OK**:

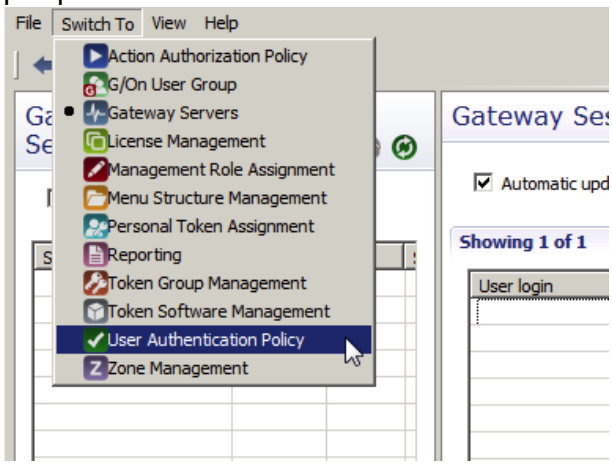


6. Click **Yes**:

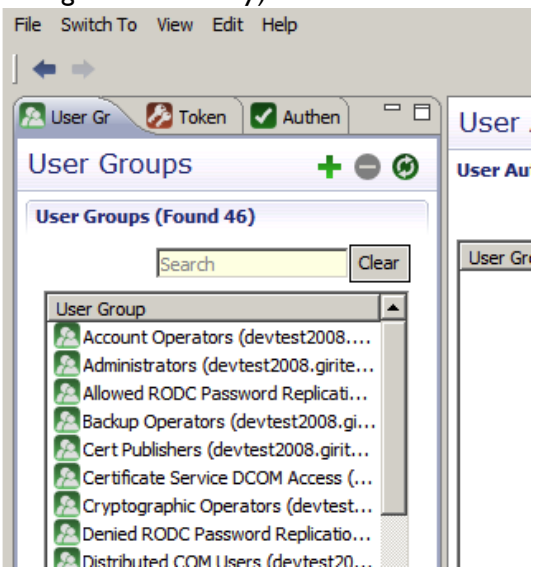


Initially G/On Management requires no login. This can be changed within the program itself. Please see the G/On Server Manual for more information.

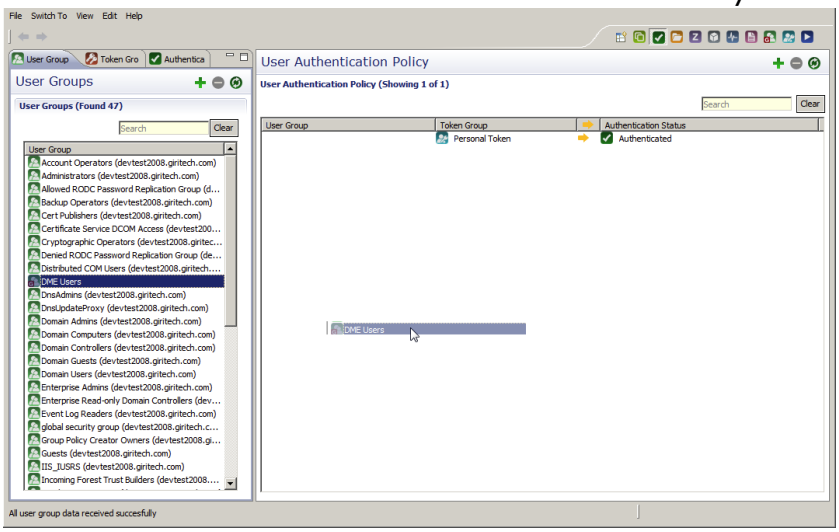
7. Use the **Switch To** menu to switch to the User Authentication Policy perspective:



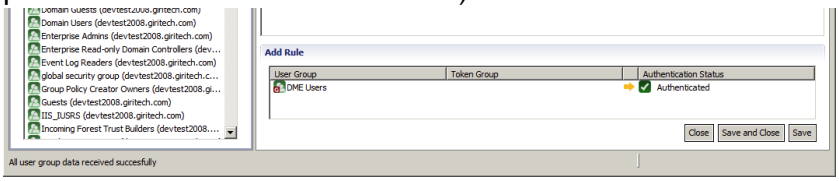
7.1. Check that the User Groups tab on the left actually contains User Groups from the user directory (indicating that the user directory configuration is okay):



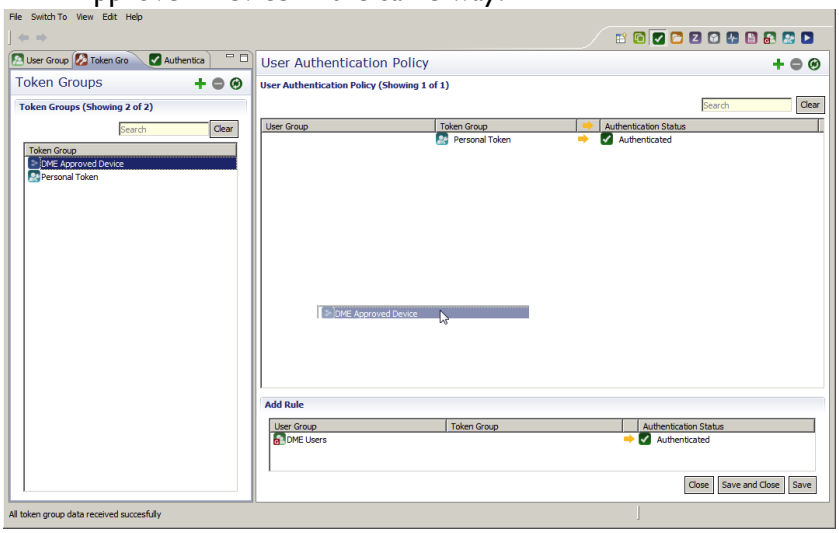
7.2. From the User Groups tab, drag a user group that contains the DME users to somewhere in the User Authentication Policy area:



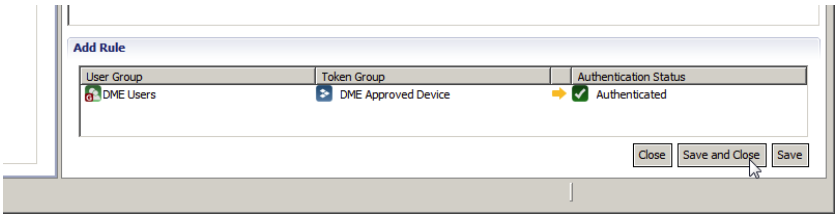
7.3. This will open a rule editor containing the user group (and with a preset value in Authentication Status):



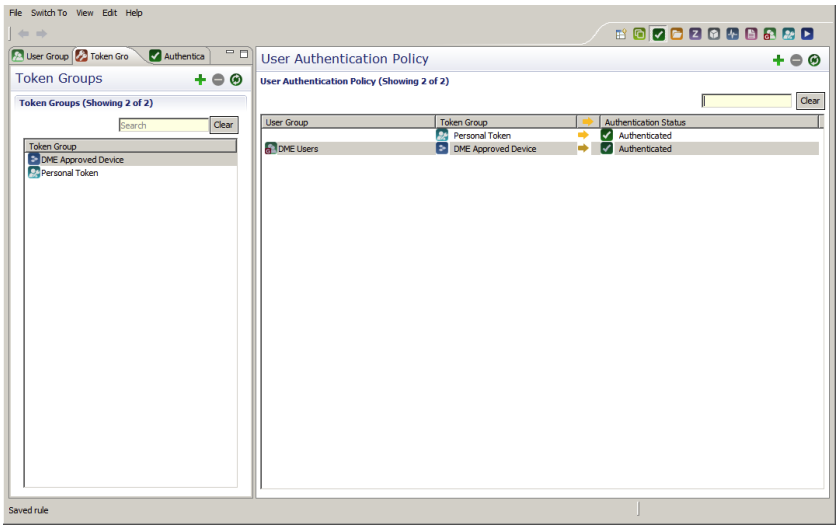
7.4. Select the Token Groups tab and drag the preset token group DME Approved Device in the same way:



7.5. Click **Save and Close**:

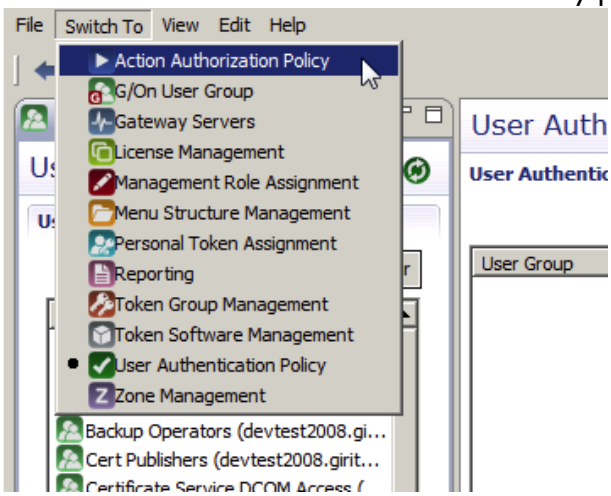


7.6. The rule is now added to the list of rules:

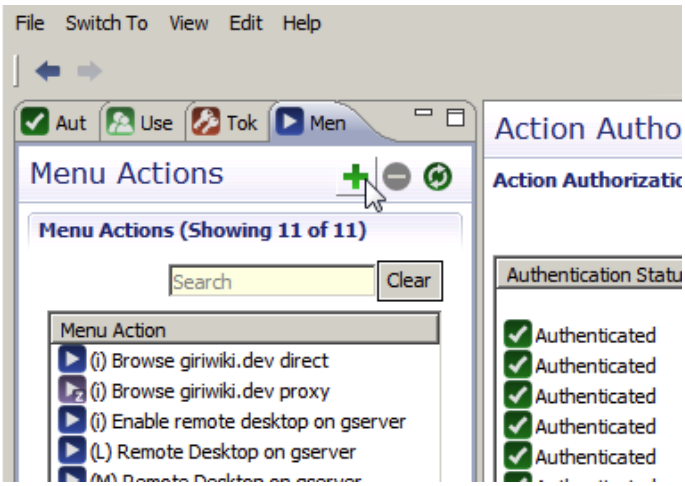


Note: The Personal Token > Authenticated rule above is a standard G/On rule, and makes no difference to the AppBox setup.

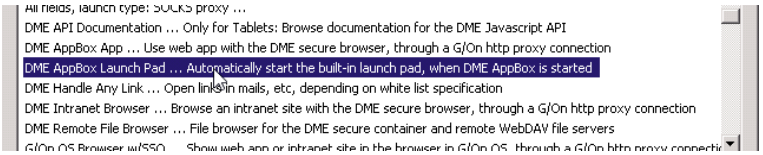
8. Now switch to the Action Authorization Policy perspective:



8.1. Select the Menu Actions tab, and click on the green plus sign (+) to make a new menu action:

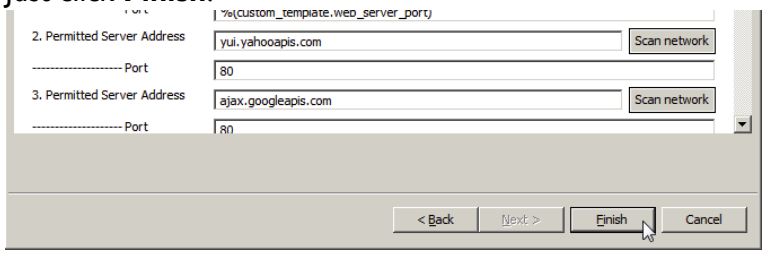


8.1.1. In the new window, select DME AppBox Launchpad… and click **Next**:



This is because we need to give the users access to the AppBox Launchpad itself in order for them to use AppBox at all.

8.1.2. Just click **Finish**:

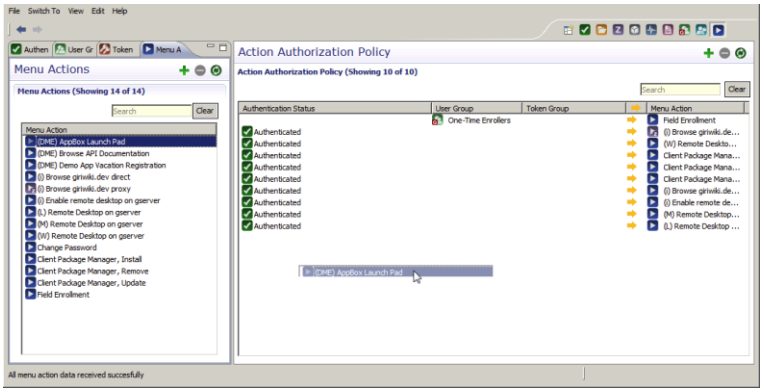


8.2. Return to 8.1 to add DME Api Documentation in the same way.

These are demonstrations of some of the AppBox functionality and can also be used to check that AppBox is correctly connected and working. See *Setting up other AppBox applications* on page 28 for more information on how to set up other applications.

8.3. For each of these two menu actions (DME AppBox Launchpad and DME Api Documentation) do the following:

8.3.1. Drag the menu action to the Action Authorization Policy to make a rule:



8.3.2. Click **Save**, and drag the next menu action over.

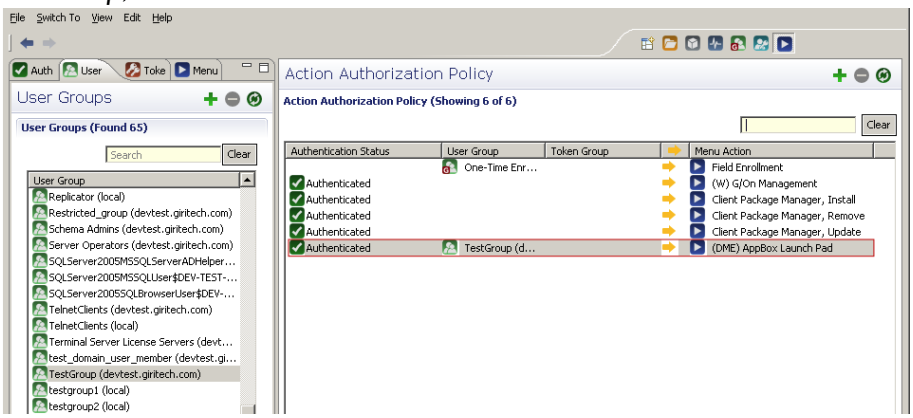
8.3.3. When all three rules are made, click **Close**.
These three rules gives the DME users access to the three menu actions (the first being AppBox itself).
It is possible to decide precisely which groups of users that have access to which AppBox applications. See *Giving access to certain user groups* on page 27 for more information.

Advanced

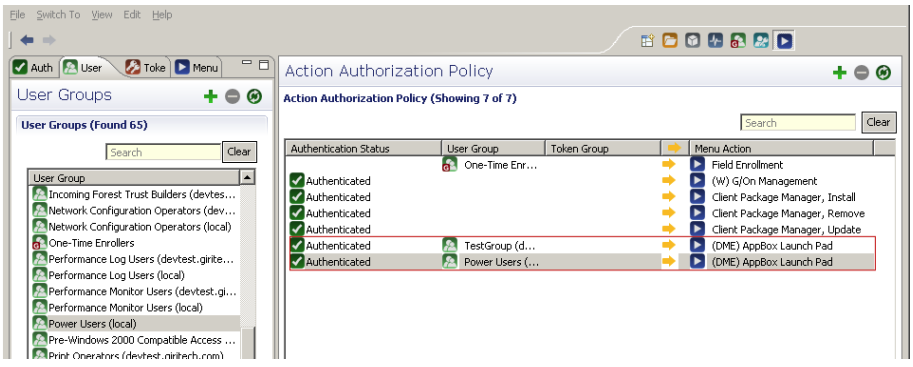
Giving access to certain user groups

It is possible to only give certain user groups access to certain AppBox applications. When setting up access to the menu actions (on page 25 in the *G/On* Management chapter), this can be done by adding a user group to the rule for the particular menu action.

In this example, the rule reads: if the user is *Authenticated* and part of the *TestGroup*, then the user has access to the menu action:



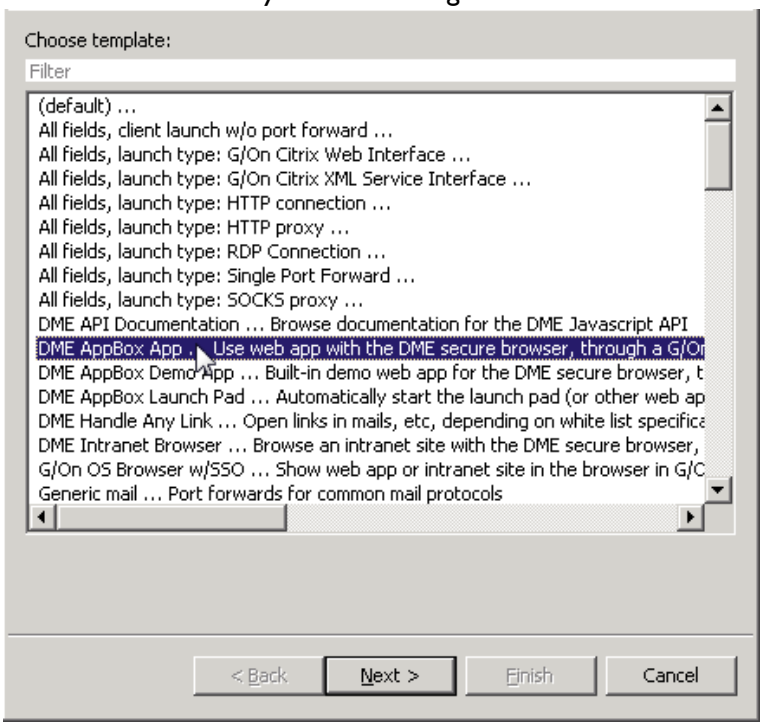
It is also possible to give access to more than one user group. This can be done by making more rules. If one of the rules is satisfied, then the user gets access:



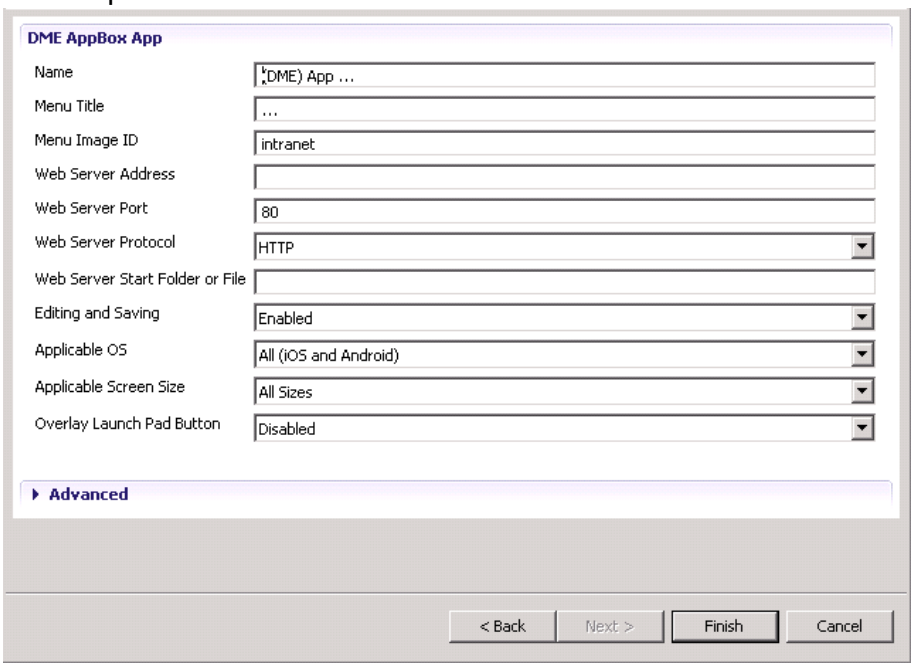
Setting up other AppBox applications

HTML 5 based application

To set up an HTML 5 based application, make a menu action based on the *DME AppBox App* template. This template will make the application run in fullscreen without any browser navigation buttons:



The template looks like this:



- **Name** is an internal and unique name identifying the application in the G/On management system.
- **Menu Title** is the name the end-users will see.
- **Menu Image ID** is an identifier for the icon that will be shown for the application in AppBox. The image itself must be placed within the Giritech folder: `Giritech/gon_5.7.x-x/config/images` in two sizes, named:

  `<Menu Image ID>_iphone_72x72.png`

  `<Menu Image ID>_iphone_144x144.png`

  in the example above: `intranet_iphone_144x144.png`
- **Web Server Address** is the address of the web server.

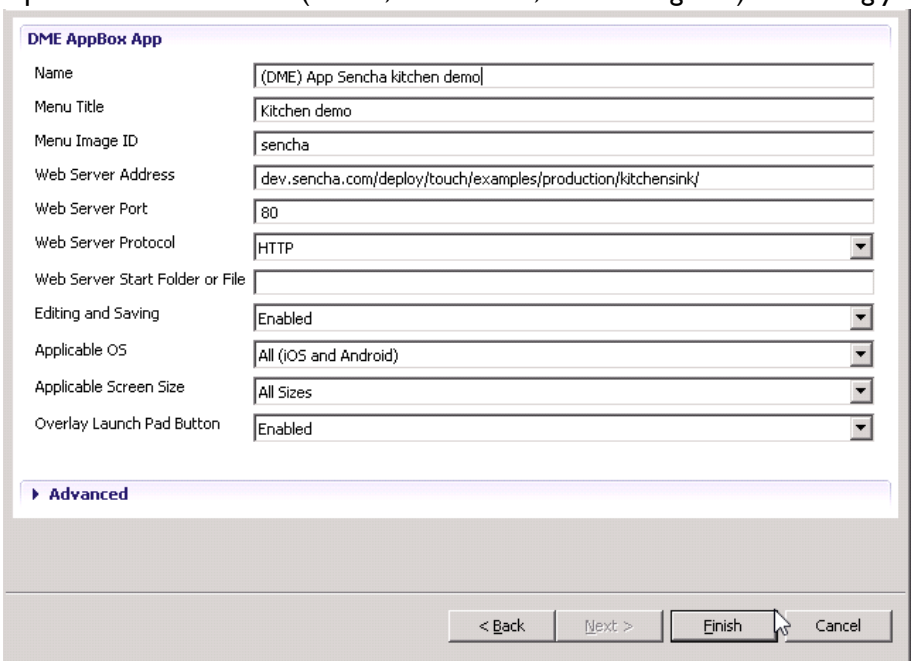
Example: Enabling Sencha demo app

This example shows how to set up a Sencha demo application. Using the DME AppBox app template, simply input the server address

`dev.sencha.com/deploy/touch/examples/production/kitchensink/`

Note: Do not enter `http://`

Update the other fields (Name, Menu Title, Menu Image ID) accordingly:



As this template provides fullscreen without any browser navigation buttons, there is no way to get back to the AppBox Launchpad, unless you set the field: *Overlay Launch Pad Button* to **Enabled**. This will provide a button to get back.

DME File Browser

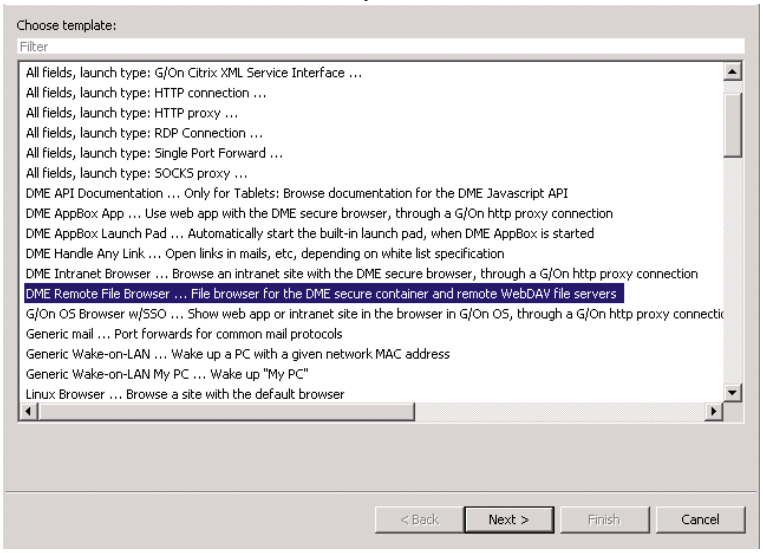
The DME File Browser lets you browse files in the secure container of the device, including files that were added by other AppBox apps (if permitted).

To set up the DME File Browser, create a menu action based on the *DME File Browser* template.

Please note that this template is included in G/On 5.6.1 and later versions, but ***not*** in G/On 5.6.0.

To create the menu action, complete the following steps:

1. In the G/On Management interface, create a menu action from the *DME Remote File Browser* template.



   See the description of setting up an HTML 5 based application above.

2. Authorize the relevant users to use the DME File Browser.

Note: It is important that you do not change the `#auth` instruction. The DME Server automatically detects whether Basic or NTLM authentication is required for the DME File Browser when accessing a WebDAV-enabled file share.

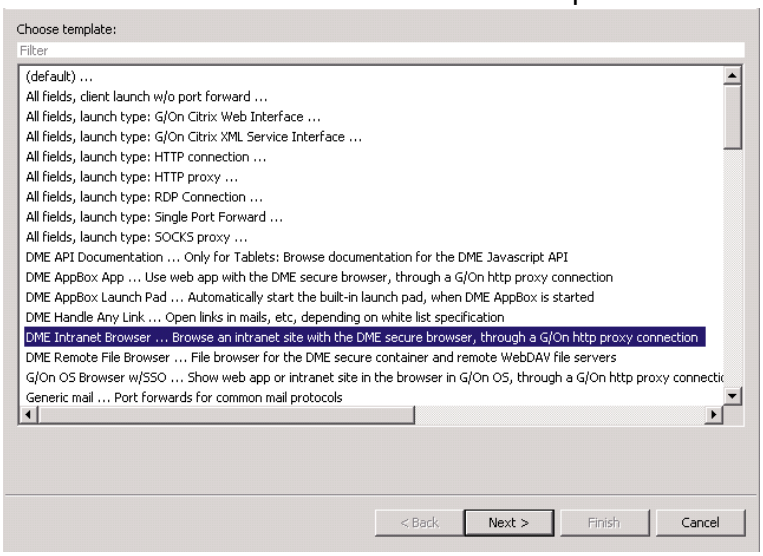
Single sign-on (SSO) information is sent from the AppBox Gateway to the File Browser (which resides on the DME Server). For domain, DME only supports the format `user@domain`. Hence, to specify a full domain username, use `%(user.login)@%(user.domain)` in the File Browser menu action.

Note also that DME always displays usernames in uppercase. This can prove to be an issue on web servers and shares where usernames are case-sensitive. To work around this, you can use alternate LDAP fields containing the user and domain names in lowercase.

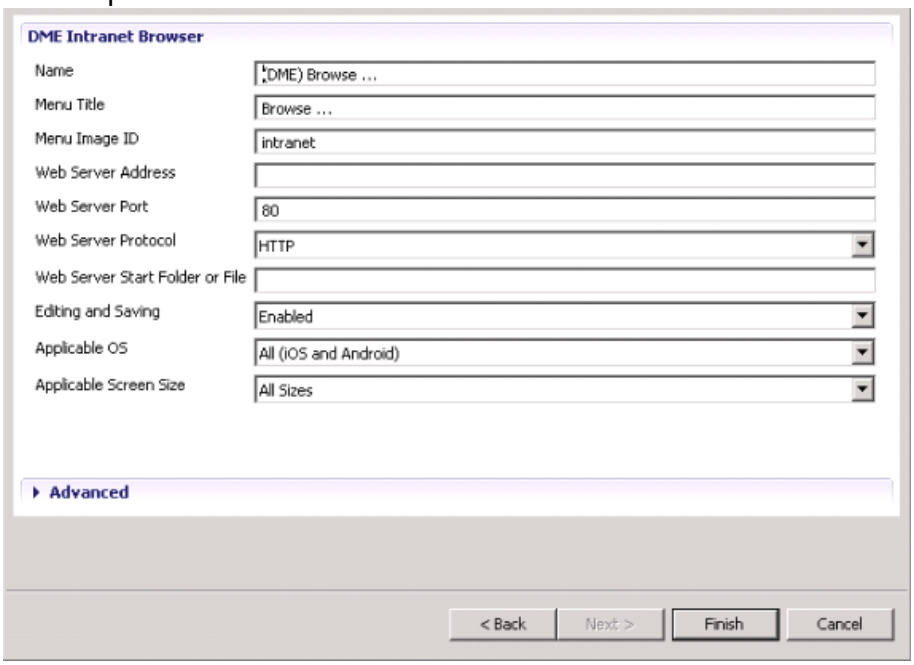
The DME File Browser is now available from the AppBox Launchpad for authorized users.

Intranet

To set up an AppBox application accessing an intranet site, make a menu action based on the *DME Intranet Browser* template:



The template looks like this:



- **Name** is an internal and unique name identifying the application in the G/On management system.
- **Menu Title** is the name the end-users will see.
- **Menu Image ID** is an identifier for the icon that will be shown for the application in AppBox. The image itself must be placed within the Giritech folder: `Giritech/gon_5.7.x-x/config/images` in two sizes, named:

  `<Menu Image ID>_iphone_72x72.png`

`<Menu Image ID>_iphone_144x144.png`

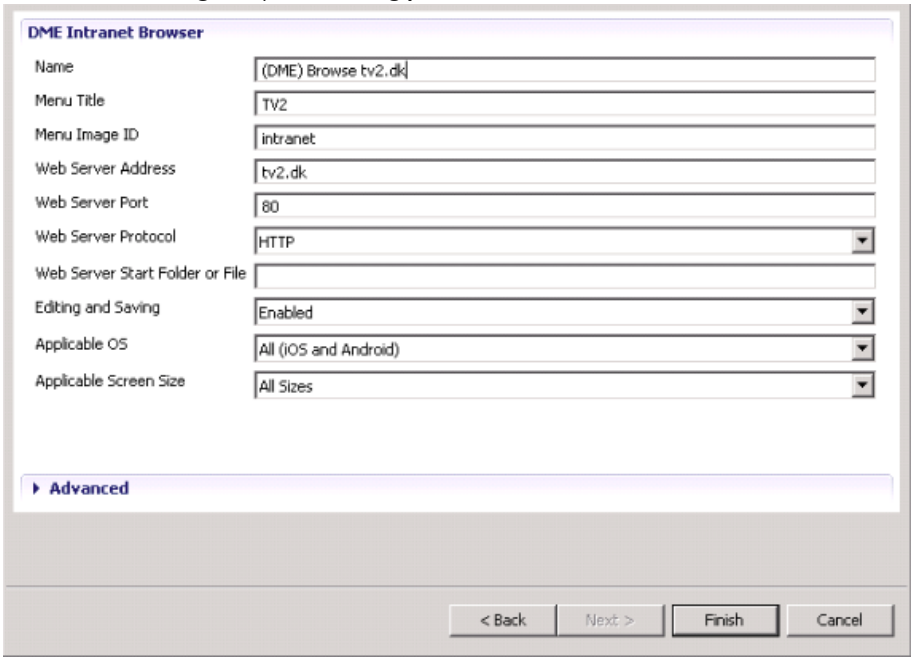
in the example above: `intranet_iphone_144x144.png`

- **Web Server Address** is the address of the web server.
- **Advanced**. For further information on the fields in the advanced section, please read the example below.

Example: Enabling intranet browsing

To show some of the challenges that can occur when giving access to an intranet site through AppBox, in this example we set up secure browsing of the Danish news site TV2.

Simply input the address tv2.dk and update the other fields (Name, Menu Title, Menu Image ID) accordingly:

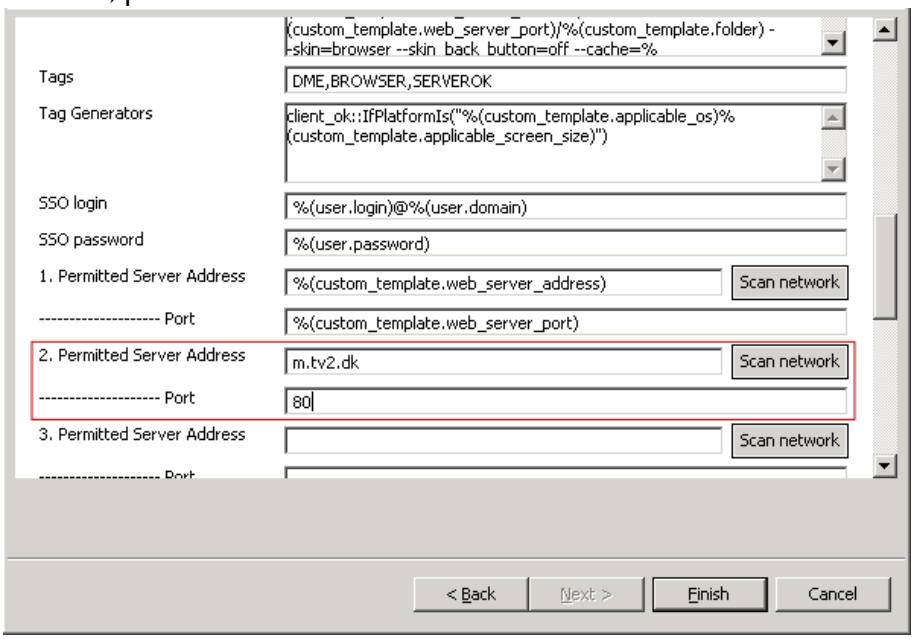


Challenge 1:

When browsing the site from an iPhone, tv2.dk is redirected to the mobile version m.tv2.dk, which is not in the default white list (only tv2.dk is in the white list). So the HTTP proxy in the G/On server will reject the attempt to access m.tv2.dk.

Solution:
Edit the menu action (double-click it) and in the advanced section add

m.tv2.dk, port 80 to the white list:

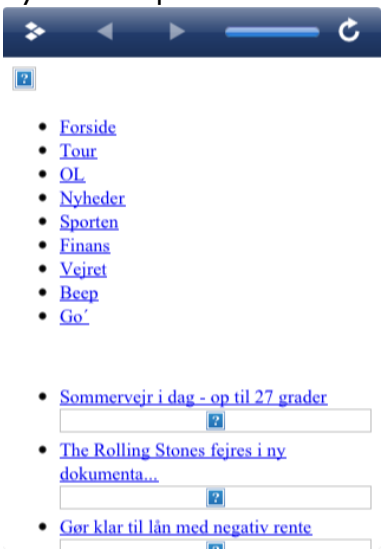


It is possible to use wild cards in the Permitted Server Address field (“.” Matches all addresses, and “.solitonsystems.com” matches all addresses that ends with solitonsystems.com).

Note that there are special rules for white lists that uses both wild cards and IP addresses. For more information on this, and on address formatting in general, please refer the Server Manual on Giritech’s website: `www.giritech.com/int/Support-Download/Product-Download/G-On-5.7-Product-Download`

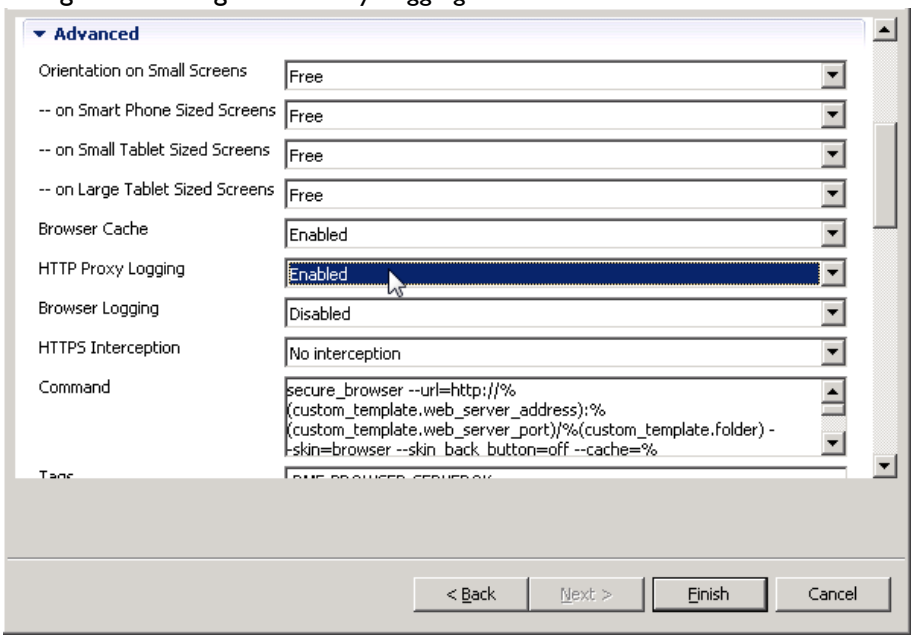
Challenge 2

Note now that the site does not look good: pictures are missing and the layout is simple text instead of having nice typography:

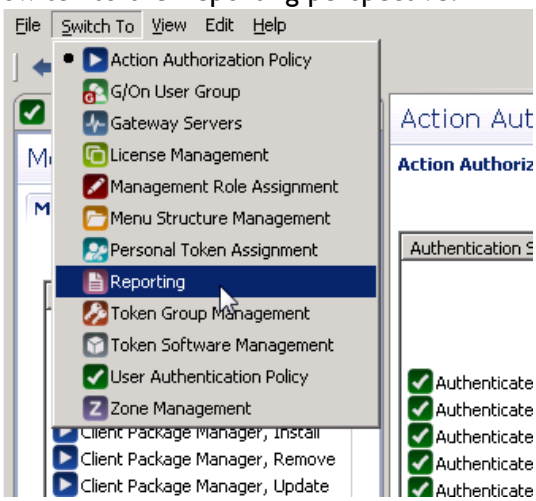


To find out what is wrong:

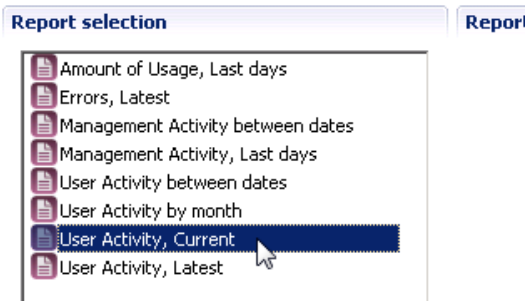
1. Edit the menu action (double-click it) and in the advanced section change the setting *HTTP Proxy Logging* to **Enabled**:



2. Access the page again from the device.
3. Switch to the Reporting perspective:



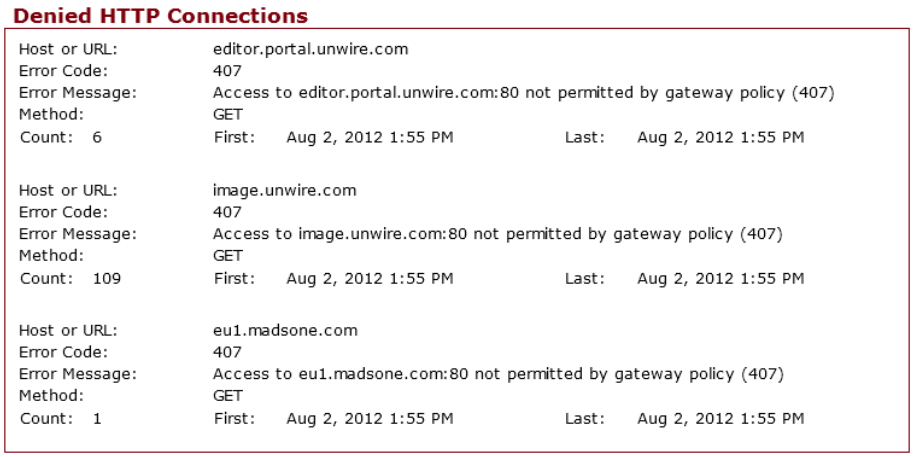
4. Double-click the report **User Activity, Current**:



5. For the user in question, click **Details**:

6. Then scroll down and find the menu action (DME) Browse tv2.dk and click **Details**:

7. In the section Denied HTTP Connections, every request that the HTTP proxy has rejected can be seen:



Solution:

Edit the menu action and add what is needed to the white list.

Note: If the company security policies allow it, a wild card can be added to the white list, allowing access to any server on any port that the G/On server can access. To do this, type 0/0 in the Permitted Server Address field and 0 in Port.

Alternatively, set up can be made so that:

- Certain internal sites are allowed.
- Certain other sites are blocked.
- Certain sites are forwarded (to already existing web proxy in the company infrastructure).
- In addition, it is possible to set up single sign-on for the internal sites, using so-called basic authentication or NTLM authentication.

The following example:

- Allows connection to `issues.solitonsystems.com` with single sign-on using basic authentication (1).
- Denies access to all other internal addresses (2,3,4).
- Forwards the remaining requests to an HTTP proxy that runs on the same machine as the G/On gateway server (5).

```
1. Permitted Server Address: issues.solitonsystems.com
#auth=basic
---------------------- Port: 80

2. Permitted Server Address: 192.168.0.0/16 #deny
---------------------- Port: 80

3. Permitted Server Address: 10.0.0.0/24 #deny
---------------------- Port: 80

4. Permitted Server Address: 172.16.0.0/16 #deny
---------------------- Port: 80

5. Permitted Server Address: 0/0 #httpproxy=127.0.0.1:8080
---------------------- Port: 80
```

Important!!

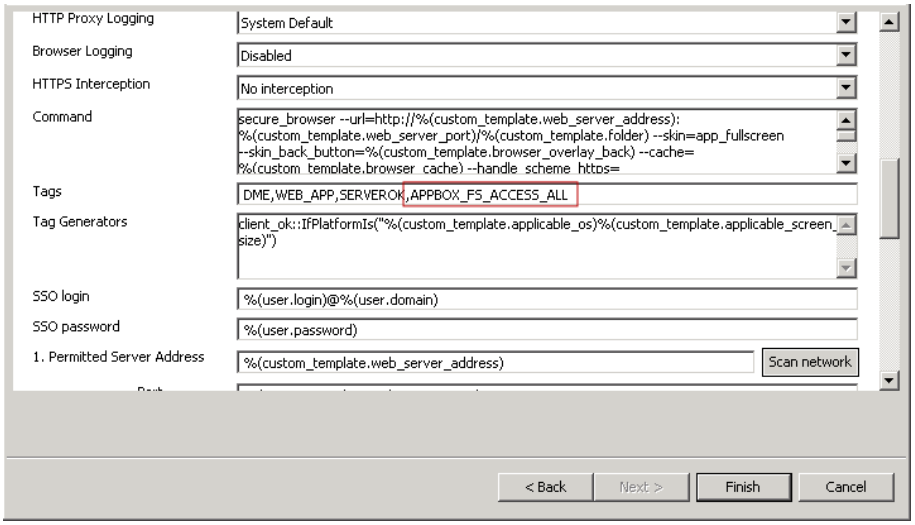
Never enter `0/0 #auth=basic` in the Permitted Server Address field! This will allow connections to all websites and send user credentials to all sites that are contacted (including external sites!).

Giving an application access to the file directory

If you have developed an HTML5 based application, which uses the Cordova file API, it will by default only have access to the files that it has itself created.

However, some applications, such as generic file tools, may need access to files that were added by other AppBox applications also.

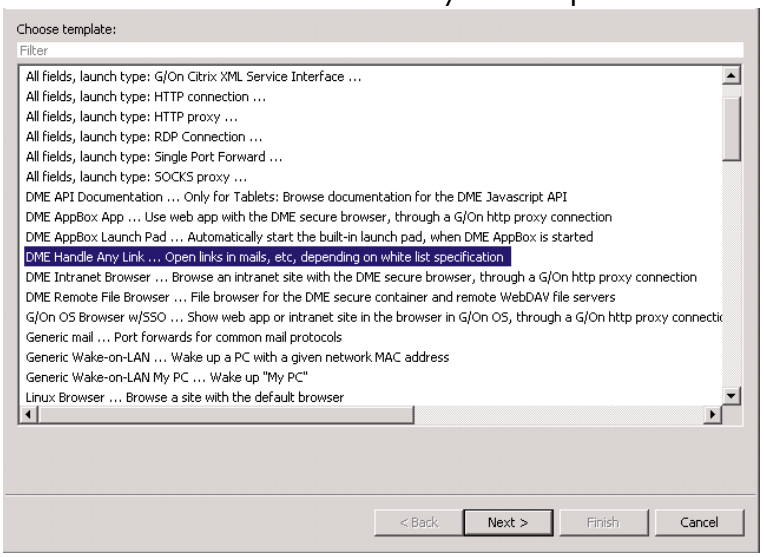
Such access can be granted by adding the tag `APPBOX_FS_ACCESS_ALL` to the **Tags** field in the menu action for your application. Use comma to separate tags.



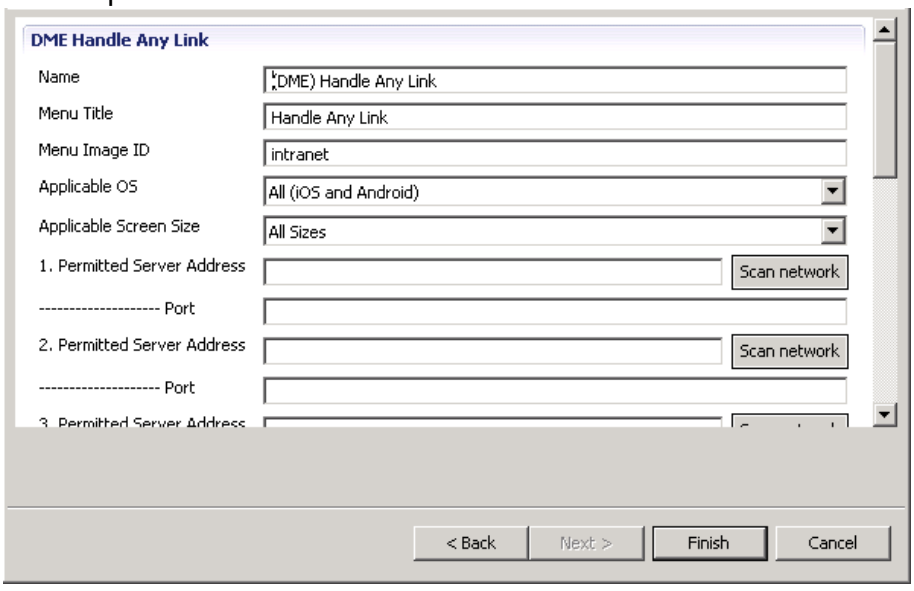
Open links from e-mails etc.

It is possible to enable DME users to open links from their DME applications (mail, calendar, etc.) in AppBox. This will make the users able to open e.g. a link to an intranet site received in an e-mail (or to any other white-listed website).

To set up an AppBox application accessing an intranet site, make a menu action based on the *DME Handle Any Link* template:



The template looks like this:

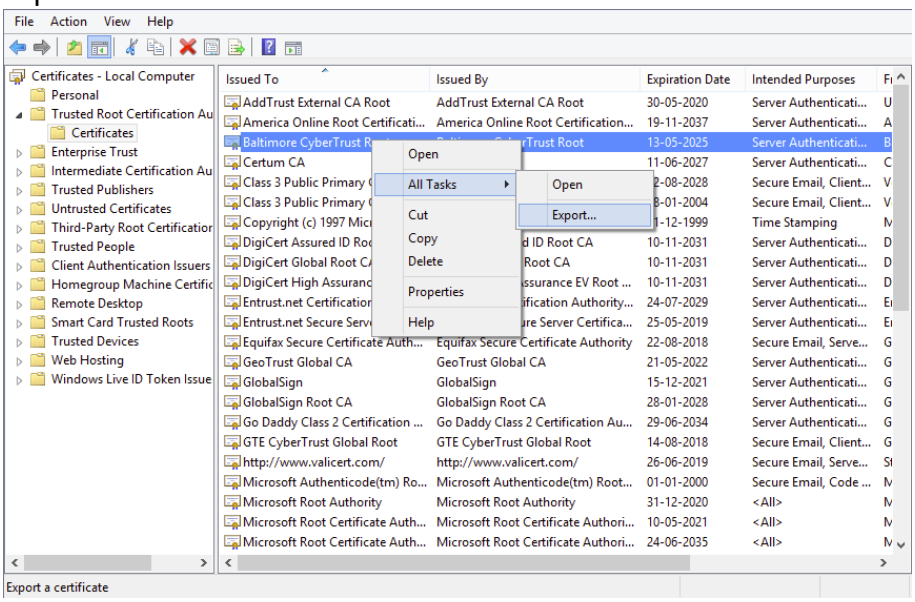


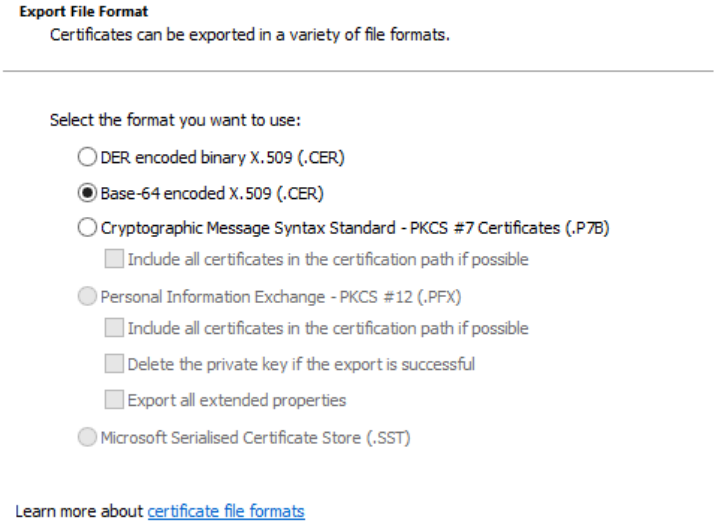
The template contains primarily a white list of permitted servers. This white list can be created as described in the section above, *Setting up other AppBox applications*.

Setting up SSL certificates

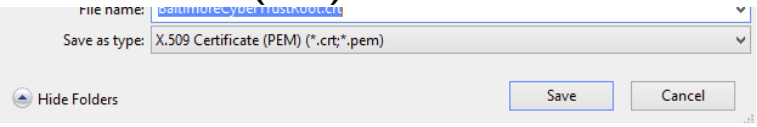
It is possible to add a Root or Intermediate Certificate, which is not already included in the pre-installed AppBox certificate collection.

1. Open your certificate manager
   - Windows 7 and XP: The *CertificateManagement.msc* program
   - Windows 8: The *Manage computer certificates* control panel
   - It is also possible to use the certificate manager in a web browser like Firefox.
2. Export the Certificate as **Base-64 encoded X.509**





- In Firefox, the certificate should be exported as **X.509 Certificate (PEM)**



3. Open the exported Certificate in an editor, and copy the text

export.cer

```
-----BEGIN CERTIFICATE-----
MIID+jCCAuKgAwIBAgIDAjbSMA0GCSqGSIb3DQEBBQUAMEIxCzAJBgNVBAYTAlVT
MRYwFAYDVQQKEw1HZW9UcnVzdCBJbmMuMRswGQYDVQQDExJHZW9UcnVzdCBHbG9i
YWwgQ0EwHhcNMTAwMjI2MjEzMjMxWhcNMjAwMjI1MjEzMjMxWjBhMQswCQYDVQQG
EwJVUzEWMBQGA1UEChMNR2VvVHJ1c3QgSW5jLjEdMBsGA1UECxMURG9tYWluIFZh
bGlkYXRlZCBTU0wxGzAZBgNVBAMTEkdlb1RydXN0IERWIFNTTCBDQTCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAKa7jnrNpJxiV9RRMEJ7ixqy0ogGrTs8
KRMMMbxp+Z9alNoGuqwkBJ7O1KrESGAA+DSuoZOv3gR+zfhcIlINV1PrqZTP+3RE
60OUpJd6QFc1tqRi2tVI+Hrx7JC1Xzn+Y3JwyBKF0KUuhhNAbOtsTdJU/V8+Jh9m
cajAuIWe9fV1j9qRTonjynh0MF8VCpmnyoM6djVI0NyLGiJOhaRO+kltK3C+jgwh
w2LMpNGtFmuae8tk/426QsMmqhV4aJzs9mvIDFcN5TgH02pXA50gDkvEe4GwKhz1
SupKmEn+Als9AxSQKH6a9HjQMYRX5Uw4ekIR4vUoUQNLIBW7Ihq28BUCAwEAAaOB
2TCB1jAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFIz02ZMKR7wAoErOS3VuoLaw
sn78MB8GA1UdIwQYMBaAFMB6mGiNifurBWQMEX2qfWW4ysxOMBIGA1UdEwEB/wQI
MAYBAf8CAQAwOgYDVR0fBDMwMTAvoC2gK4YpaHR0cDovL2NybC5nZW90cnVzdC5j
b20vY3Jscy9ndGdsb2JhbC5jcmwwNAYIKwYBBQUHAQEEKDAmMCQGCCsGAQUFBzAB
hhhodHRwOi8vb2NzcC5nZW90cnVzdC5jb20wDQYJKoZIhvcNAQEFBQADggEBADOR
NxHbQPnejLICiHevYyHBrbAN+qB4VqOC/btJXxRtyNxflNoRZnwekcW22G1PqvK/
ISh+UqKSeAhhaSH+LeyCGIT0043FiruKzF3mo7bMbq1vsw5h7onOEzRPSVX1ObuZ
lvD16lo8nBa9AlPwKg5Bbuvvnvdwns2AKnbIh+PrI7OWLOYdlF8cpOLNJDErBjgy
YWE5XIlMSB1CyWee0r9Y9/k3MbBn3Y0mNhp4GgkZPJMHcCrhfCn13mZXCxJeFu1e
vTezMGnGkqX2Gdgd+DYSuUuVlZzQzmwwpxb79k1ktl8qFJymyFWOIPllByTMOAVM
IIi0tWeUz12OYjf+xLQ=
-----END CERTIFICATE-----
```

4. In an editor, open the `cacert.pem` file from the folder `Giritech/gon_5.7.x-x/config/certificates/ssl_as_client`
5. Paste your Certificate in the file.

cacert.pem

```
##
## ca-bundle.crt -- Bundle of CA Root Certificates
##
## Certificate data from Mozilla as of: Sat Dec 29 20:03:40 2012
##
## This is a bundle of X.509 certificates of public Certificate Authorities
## (CA). These were automatically extracted from Mozilla's root certificates
## file (certdata.txt).  This file can be found in the mozilla source tree:
## http://mxr.mozilla.org/mozilla/source/security/nss/lib/ckfw/builtins/certdata.txt?raw=1
##
## It contains the certificates in PEM format and therefore
## can be directly used with curl / libcurl / php_curl, or with
## an Apache+mod_ssl webserver for SSL client authentication.
## Just configure this file as the SSLCACertificateFile.
##

# @(#) $RCSfile: certdata.txt,v $ $Revision: 1.87 $ $Date: 2012/12/29 16:32:45 $

GTE CyberTrust Global Root
==========================
-----BEGIN CERTIFICATE-----
MIICWjCCAcMCAgGlMA0GCSqGSIb3DQEBBAUAMHUxCzAJBgNVBAYTAlVTMRgwFgYDVQQKEw9HVEUg
Q29ycG9yYXRpb24xJzAlBgNVBAsTHkdURSBDeWJlclRydXNOIFNvbHV0aW9ucywgSW5jLjEjMCEG
A1UEAxMaR1RFIEN5YmVyVHJ1c3QgR2xvYmFsIFJvb3QwHhcNOTgwODEzMDAyOTAwWhcNMTgwODEz
MjM1OTAwWjB1MQswCQYDVQQGEwJVUzEYMBYGA1UEChMPR1RFIENvcnBvcmF0aW9uMScwJQYDVQQL
Ex5HVEUgQ3liZXJUcnVzdCBTb2x1dGlvbnMsIEluYy4xIzAhBgNVBAMTGkdURSBDeWJlclRydXNO
IEdsb2JhbCBSb290MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCVD6C28FCc6HrHiM3dFw4u
sJTQGz0O9pTAipTHBsiQl8i4ZBp6fmw8U+E3KHNgf7KXUwefU/ltWJTSr41tiGeA5u2ylc9yMcql
HHK6XALnZELn+aks1joNrI1CqiQBOeacPwGFVw1YhOX404Wqk2kmhXBIgD8SFcd5tB8FLztimQID
AQABMA0GCSqGSIb3DQEBBAUAA4GBAG3rGwnpXtlR22ciYaQqPEh346B8pt5zohQDhT37qw4wxYMW
M4ETCJ57NE7fQMh017l93PR2VX2bY1QY6fDq81yx2YtCHrnAlU66+tXifPVoYb+O7AWXX1uw16OF
NMQkpw0PlZPvy5TYnh+dXIVtx6quTx8itc2VrbqnzPmrC3p/
-----END CERTIFICATE-----

Thawte Server CA
================
-----BEGIN CERTIFICATE-----
MIIDEzCCAnygAwIBAgIBATANBgkqhkiG9w0BAQQFADCBxDELMAkGA1UEBhMCWkExFTATBgNVBAgT
DFdlc3RlcmG4gQ2FwZTESMBAGA1UEBxMJQ2FwZSBUb3duMR0wGwYDVQQKExRUaGF3dGUgQ29uc3Vs
```

6. Save and close the file.

7. If the Gateway server is already running, please restart it for the change to take effect.