Oostzeedijk 314
3063 CC Rotterdam, NL
T +31 (0)10 8910902
E mjong@magnafacta.nl

EPD Screen Integration for GemsTracker

Since version 1.8.7 GemsTracker (GT) has a generic method to show a screen of a patient within an EPD (Electronoc Patient Dossier) system. Before this version there were multiple application specific solution that often had security issues. The new solution is generic and uses and uses temporary keys that remain valid for only an hour (by default).

This manual describes first how the EPD can create the link. Then it describes how to set up the connection in GemsTracker.

The EPD link

The complete URL

The EPD link contains of both fixed and variable parts. The general format is:

> **{siteurl}**/embed/login?epd=**{systemUser}**&usr=**{epdUser}**
> &pid=**{patientId}**&org=**{organizationId}**&key=**{key}**

Variable	**Description**	**Example**
{siteurl}	The url of the GemsTracker site.	https://zorgmonitor.umcutrecht.nl/schisis
{systemUser}	An “Embedded (EPD) Login user” System User in GT.	HiX
{epdUser}	The username of the person logged into the EPD. A setup variable determines what should happen when this user is not known to GT.	m.de.jong
{patientId}	The patient id of the patient to show. In the setup you can choose to either create a non-existing patient or to show an error message,	12345678
{organizationId}	The organisation this patient belong to. This is primarily of importance on a multi-organisation installation.	72 Or e.g. a code like “utrecht” or a healtcare provider id as long as these are set for the organisation in GT.
{key}	By default a time sensitive key created using a fixed secret part and a time senstive part. This code must be hashed using e.g. sha256 (default) and then converted to base64.	KCMjF4tDVUI%2Fh%2BUz2LJkTD2sZ8bPd6raCN83p0ltOyk%3D This example uses, **test** as the fixed part: Base64(Sha256(**test**{YYYYMMDDHH})) (entered into GT as: test%s)
{YYYYMMDDHH}	Year-month-day-hour notatipn	2019101217

The order of the variables is neglected. Als a POST statement can be used instead of the above GET example.

The timecode ensures that a code is valid for at most an hour. In reality though this is about three hours as GT also accepts the codes used an hour earlier and later. This in case the time isn’t synchronized across the systems used.

Shortened URLs

To keep the link shorter and to hide the **{systemUser}** and **{organizationId}** fields, we often use a project specific link. E.g.:

{siteurl}/embed/hix?usr=**{epdUser}**&pid=**{patientId}**&key=**{key}**

This requires some extra work at the project level in GemsTracker, but that takes just a couple of minutes.

In the same manner we can change the key type to have a link that is e.g. valid for 5 hours or 15 minutes and to use a different hashing or encryption algorithm than sha256,

A HiX implementation example

HiX is the most used EPD system in the Netherland. This next example shows how to generate the (shortened) url in HiX:

```
setvar('Medewerker’, ’?usr=' +
  display('CODE', HuidigeMutatieGebruiker));

setvar('Patnum', ‘&pid=' +
  ValueAsString('PATIENT_PATIENT.Patientnummer'));


setvar('Secret’, ’&key=' + URLEncode(ComputeHashAsBase64(
  "sha256", 'test' + FormatDateTime('YYYYMMDDHH', Now)));

setvar('Url',
  'https://zorgmonitor.umcutrecht.nl/embed/hix' +
  Medewerker + Patnum + Secret);
```

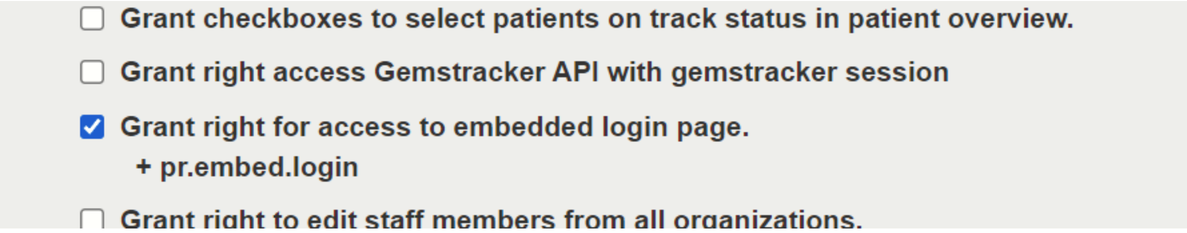
(The writer of this document doesn’t have any access to HiX, so sorry but I do not know where to set these and I do not have a screenshot.)

Set up in GemsTracker

Set the correct rights for roles

By default the embed/login page is not usable. To enable this, edit the “nologin” role in Setup => Access => Roles. Usually only super administrators have the right to edit roles..

The right below for access to the embedded login page must be checked for all users not logged in.



□ Grant checkboxes to select patients on track status in patient overview.

□ Grant right access Gemstracker API with gemstracker session

☑ Grant right for access to embedded login page.
+ pr.embed.login

□ Grant right to edit staff members from all organizations.

When this right has not been checked the user will be redirected to the general login page. When the embedded login page is enabled and another setting is at fault, you will always get just the message” “**Unable to authenticate**”.

On a sidenote: the embedded login page is never visible as a menu option.

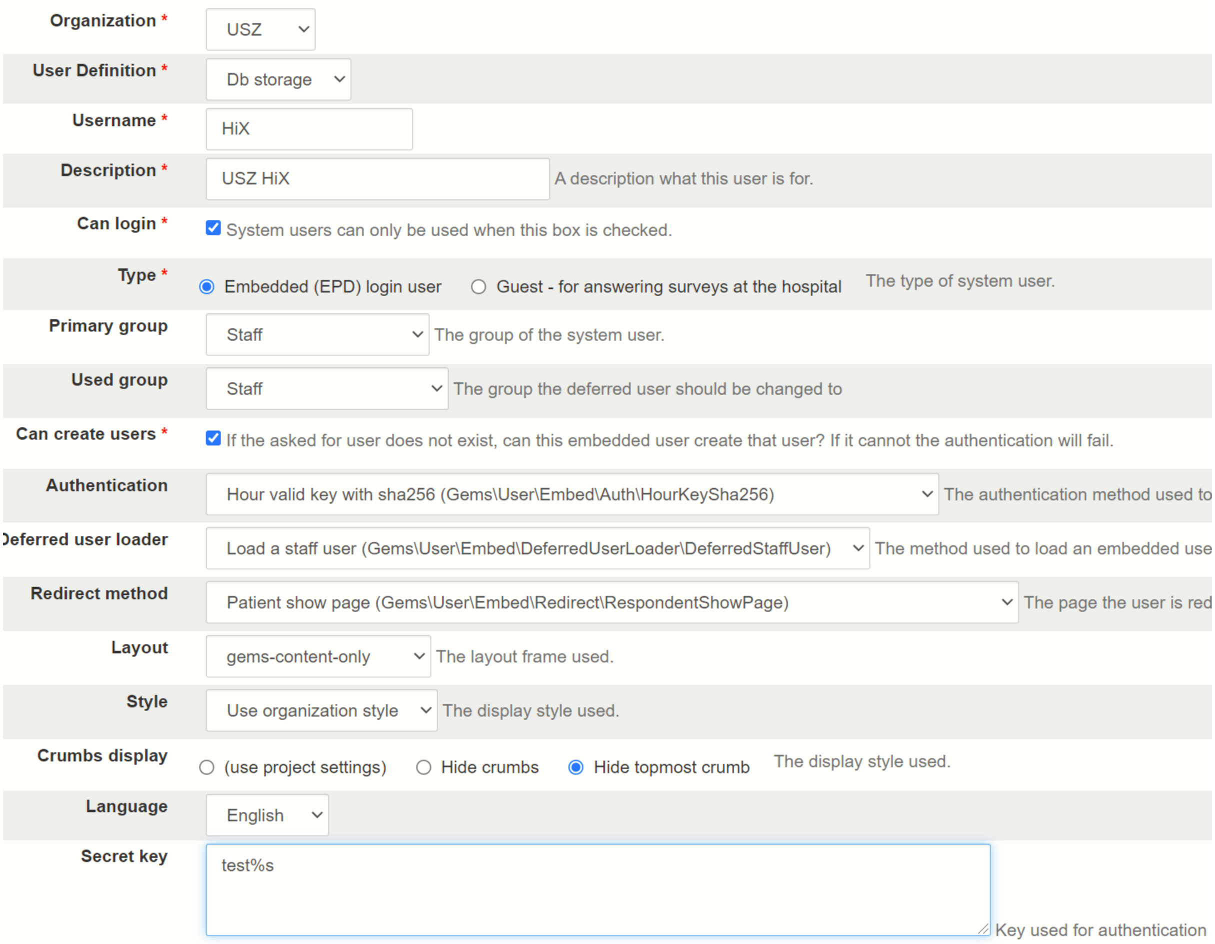
N.B.: It is best practice to also grant all other roles the this right. Otherwise the user can get an error message when trying to view a second patient using the same integration method.

Creating the {systemUser}

Also located in Setup => Access since 1.8.7 is the option for super administrators to create System user.

At the moment of writing, two types of system user exist: a “guest” account that is used to lookup a patient and then have that patient answer surveys, while disabling access to the system after survey completion. The other type is the Embedded (EPD) login user, used here.

The next screen below shows an example system user.



Organization *	USZ	
User Definition *	Db storage	
Username *	HiX	
Description *	USZ HiX	A description what this user is for.
Can login *	☑ System users can only be used when this box is checked.	
Type *	● Embedded (EPD) login user ○ Guest - for answering surveys at the hospital	The type of system user.
Primary group	Staff	The group of the system user.
Used group	Staff	The group the deferred user should be changed to
Can create users *	☑ If the asked for user does not exist, can this embedded user create that user? If it cannot the authentication will fail.	
Authentication	Hour valid key with sha256 (Gems\User\Embed\Auth\HourKeySha256)	The authentication method used to
Deferred user loader	Load a staff user (Gems\User\Embed\DeferredUserLoader\DeferredStaffUser)	The method used to load an embedded use
Redirect method	Patient show page (Gems\User\Embed\Redirect\RespondentShowPage)	The page the user is red
Layout	gems-content-only	The layout frame used.
Style	Use organization style	The display style used.
Crumbs display	○ (use project settings) ○ Hide crumbs ● Hide topmost crumb	The display style used.
Language	English	
Secret key	test%s	Key used for authentication

The **Organization** is the organization that is used to add an unknown **{epdUser}** to, when the user does not exist. After creation these users can be managed using Setup => Access => Staff.

Usually “Db storage” is the only option for the **User Definition** field. However, when a hospital uses LDAP or Radius for centralized password management, these choices are added here. When set to one of these values, any EPD user added to GemsTracker can access the system through the web interface using his or her normal password. Otherwise users are created without a password and must be enabled for login by an administrator.

The **Username** is the **{systemUser}** code used in the URL.

The **Primary group** is the group in which a new **{epdUser}** is created.

In contrast the **Used group** is the group used to log the user for an embedded session. This is usually a different group with more limited rights that shows less buttons for simplicity and less data because that data is already available in the EPD.

Can create users determines whether or not a new GemsTracker user is created when the EPD user is not known. If access to a patient in the EPD, does not grant access to the data in GemsTracker, this option should remain unchecked.

Authentication is the method used to generate the **{key}**. The default option is a sha256 key valid for an hour. Other options include the use of md5 or a key that is valid for a day. Some other options exist as well and the number of options can easily be extended with other encryption methods.

At the moment there exists only one **Deferred user loader**, i.e. to load a staff member. In the near future we expect to extend this for e.g. patient portal intergration.

The **Redirect method** determines the kind of screen a staff member sees after login. Default is to show the patient, but show or create patient is another often used option.

The **Layout** determines the makeup of the screen. “gems-content-only” is the default and hides the menu’s, logo’s, header and footer parts of a normal GT screen. This option displays only the patient data and doesn’t allow access to other parts of GT. “Do not change layout” and “gems-responsive” both allow full access to all parts of GT, like overviews, etc…

Style determines the fonts and colors of the display. By default we use the same style as set for the Organization, but it is possible to create a style that makes the interface look more like part of the EPD.

Crumbs display is (again) an option to prevent the staff member to browse to the data of another patient. The crumbs are shown at the top of the screen and allow navigation without the menu being shown. By hiding the topmost crumb the patient search screen is unreachable.

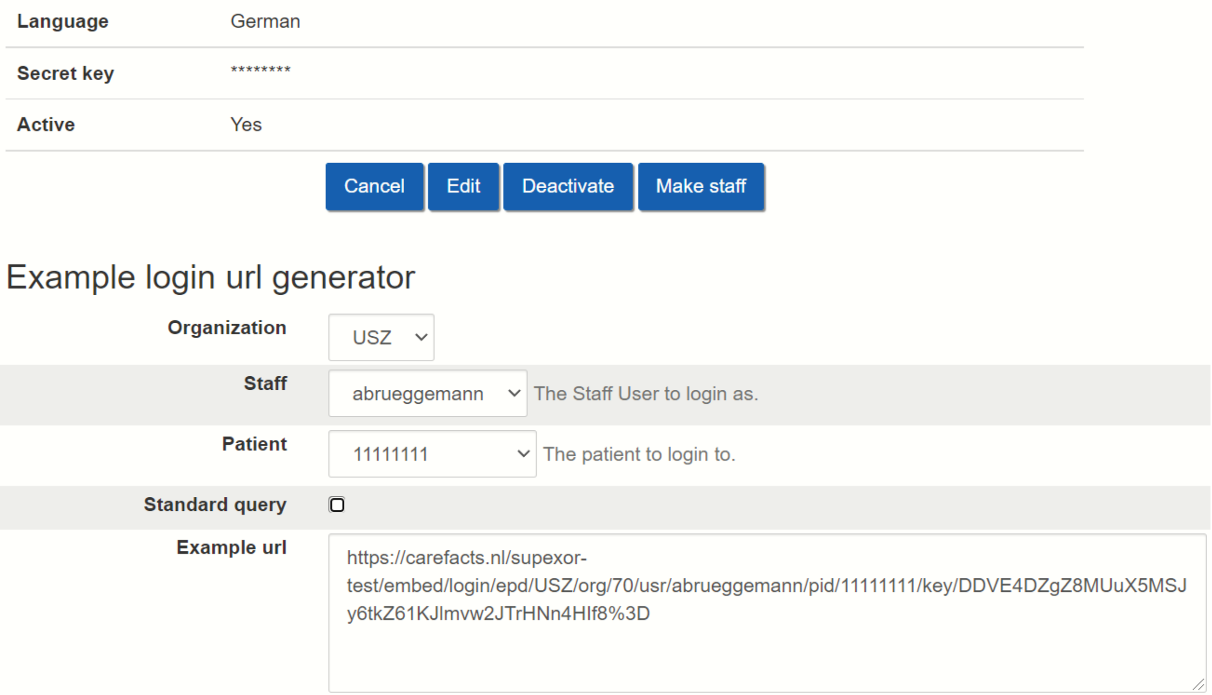
The **Language** is the language set for new users created. After login the language used will be the language set for that user, independent of this setting.

Last but not least the **Secret key** is used to generate the **{key}** part of the url. If this key contains the string “%s”, then that is the place where the **{YYYYMMDDHH}** time-code is put (or **{YYYYMMDD}** when using a day key). If the “%s” is missing the time-code is put at the end of the key.

(This key is stored encrypted in the database, but is shown decrypted here, because otherwise we tended to lose a lot of keys.)

Testing EPD accounts

To simplify the correct setup we created a login URL generator under the System user => Show screen. If you select a Staff member and a patient the system generates an URL that can be used at that moment to fake the EPD login in an (other or private mode) browser.



Language	German
Secret key	********
Active	Yes

Example login url generator

Organization	USZ
Staff	abrueggemann The Staff User to login as.
Patient	11111111 The patient to login to.
Standard query	□
Example url	https://carefacts.nl/supexor-test/embed/login/epd/USZ/org/70/usr/abrueggemann/pid/11111111/key/DDVE4DZgZ8MUuX5MSJy6tkZ61KJlmvw2JTrHNn4HIf8%3D

The **Standard query** option generates the url in a manner that works in all browser / server combinations – and that we prescribed at the beginning of this document. Without that check the URL is (somewhat) easier to read, but then it doesn't work on some Windows servers.