

# Security Documentation

## ITM Platform



**ITM Platform**  
PROJECTS ▪ PROGRAMS ▪ PORTFOLIO



[www.itmplatform.com](http://www.itmplatform.com)



@itmplatform

## Contents

---

Contents .....	0
1. SaaS and On-Demand Environments.....	1
1.1. ITM Platform configuration modes.....	1
1.2. Server .....	1
1.3. Application and Database .....	2
1.4. Domain.....	3
1.5. Access .....	4
1.6. User Identification .....	4
2. Access to ITM Platform .....	5
2.1. Passwords.....	5
2.2. Licenses .....	6
2.3. Roles.....	7
2.4. Role Configuration .....	8
2.5. Assignment as Project, Service or Program Manager .....	10
2.6. Company Admin .....	12
3. Backup .....	13
3.1. Database .....	13
3.2. Web Files .....	13
3.3. Location of the Backup Server .....	13
3.4. Encryption and Safekeeping .....	13
3.5. Backup to the Client and Data Deletion .....	14
3.6. Space for Backups.....	14
4. Backup Environment.....	15
5. Software Control and Updates .....	16
5.1. Application.....	16
5.2. System .....	16
6. Online Security .....	17
6.1. Firewall and Port Blocking.....	17
6.2. Access Network and Administration Network .....	17
6.3. Suspicious Network Blocking .....	17
7. Security and Vulnerability Control.....	18
7.1. Weekly Control .....	18
7.2. Monthly Control .....	18
7.3. Quarterly Control .....	18
8. Availability and Performance.....	19

## 1. SaaS and On-Demand Environments

ITM Platform can be configured in a variety of ways to ensure it adapts to the needs of different organizations in terms of security, policies and the preferences of each client. These various configurations range from shared environments (**SaaS**) that require no adaptation whatsoever to environments that are customized (**On-Demand**) to suit each individual organization.

Generally-speaking, we recommend the SaaS environment implementation model as it is more economical than On-Demand environments, where all infrastructure costs are passed on to the client.

### 1.1. ITM Platform configuration modes

ITM Platform provides by default the SaaS (Software as service) system in a shared infrastructure and with all the necessary guarantees to ensure the privacy of customer information security.

As an extension of the SaaS system, ITM Platform provides other custom modes from the SaaS OnDemand dedicated to different configurations to meet the needs of each client.

	Server			Database and APP		Domain		Access			Identification	
	shared	Physical server	Cloud	shared	dedicated	app.itmplatform.com	Costumized	Access http	Access https (ssl)	Access via VPN	ITM's User / Password	synchronized User / Password
SaaS	✓			✓		✓		✓	✓		✓	
Dedicated SaaS	✓				✓		✓	✓	✓		✓	
Physical OnDemand		✓			✓		✓	✓	✓		✓	
OnDemand Cloud			✓		✓		✓	✓	✓		✓	
OnDemand VPN			✓		✓		✓			✓	✓	
OnDemand VPN - Sync			✓		✓		✓			✓		(studies Required)

### 1.2. Server

#### Shared Server

In this default ITM Platform configuration, the execution environment is shared by the various clients to guarantee secure access to the information at all times via user identification protocols. Access to the data of an organization can only be accessed by users from that same organization. Furthermore, each user can only access the content allowed by the permissions configured in their profile (role).

In Shared Server mode, machine resources are shared by all clients and performance by those resources is therefore the same for all clients. ITM Platform guarantees correct server design and application performance.

Shared servers are used for both SaaS and dedicated SaaS system types, in which an instance of the application and database is created on the shared server.

### Physical Server

If the client so requires, ITM Platform enables the configuration of one or more dedicated servers for the execution of its environment. The design criteria for these physical servers and their configuration are established by the client but administered by ITM Platform as an integral part of its servers.

The expansion of or configuration changes to these dedicated servers require scheduled intervention of a more or less complex nature depending on the task, which may require temporary service downtime. They are therefore not recommended when absolute flexibility is required for expansion or modification.

### Cloud-based Server

This service is based on highly-available Cloud-based systems and enables a dedicated server to be configured in a flexible manner. Unlike physical servers, virtual servers can be expanded and configured with great ease and therefore adapted to the needs of the client at any given moment.

In addition, a dedicated Cloud-based server can be complemented with VPN services and/or integration of the server into the client identification system via trust relationships created through the VPN.

### Included in all formats

The following services are included in all the above formats (adapted to suit each environment):

- System administration
- Backup
- Software control and updates
- Security and vulnerability checks
- Performance control and system optimization

## 1.3. Application and Database

### Shared Environment

In the **SaaS** environment, all clients share the ITM Platform application and database to optimize the use of resources. ITM Platform guarantees secure access to the information at all times via user identification protocols. Access to the data of an organization can only be accessed by users from that same organization. Furthermore, each user can only access the content allowed by the permissions configured in their profile.

### Dedicated Environment

In both the shared environment (dedicated SaaS) and On-Demand environments, an entirely dedicated instance of ITM Platform can be configured for a client to allow independent management of its data and users.

In the dedicated SaaS environment, the machine is shared with other clients but a customized copy of the application is made available and an entirely independent database instance is used. In this case, the hardware resources and operating system are shared while the data and application are isolated from other clients.

In the On-Demand environments, both the machine and the system as well as the application and the database are entirely independent and used by a single client to provide complete independence.

## 1.4. Domain

### app.itmplaform.com

This is the default ITM Platform domain that is used as standard for all clients. Each environment and its data are differentiated by the access codes. This domain is only valid for the SaaS service.

### Subdomain

In the case of using a customized configuration, either from the dedicated SaaS service or the On-Demand service, a subdomain of itmplatform.com can be registered in the following manner:

*<company\_name>.itmplatform.com*

These subdomains incur no additional cost for the client and are managed directly by the ITM Platform DNS servers.

### Own Domain

ITM Platform offers clients the chance to register a domain or subdomain of their own corporate domain when using a customized configuration, either from the dedicated SaaS service or the On-Demand service.

These customized domains or subdomains can be registered at will by clients, such as itmplatform.<company\_name>.com.

These own domains are managed by the client and their DNS servers must point to the ITM Platform server IP addresses.

## 1.5. Access

### HTTP and HTTPS Protocols

A client can access the server hosting its environment from anywhere with an Internet connection by using HTTP and HTTPS (secure) protocols. When using a customized domain, the client will need to obtain a server certificate for that domain name if wishing to access via the HTTPS (secure) protocol.

### VPN

Those clients only wishing to access ITM Platform from their corporate networks can request a VPN connection to the server.

This VPN connection service is currently only provided with Cloud-based servers, although this solution can be studied for physical servers.

## 1.6. User Identification

### ITM Platform Passwords

Standard access to ITM Platform is granted via user passwords to thus guarantee the correct use and security of data.

### Identification Synchronization

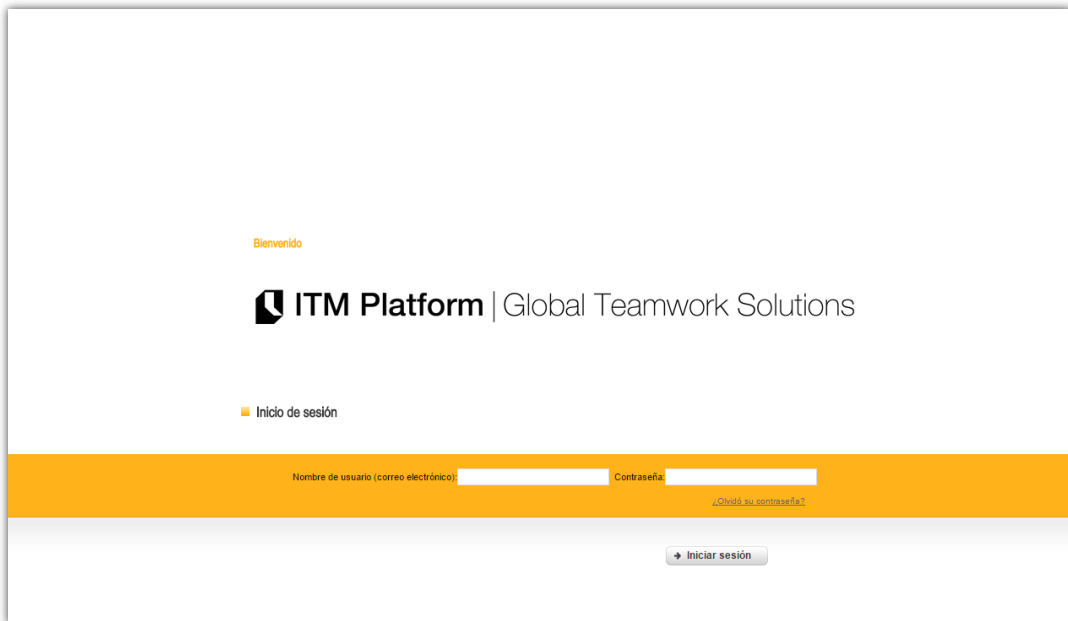
When requested by a client, corporate identification systems can be connected to the ITM Platform servers for access to be granted via the passwords normally used by users of the organization.

This user identification synchronization process must be studied on a case-by-case basis, requiring a VPN connection between the corporate network and the ITM Platform servers so as to guarantee maximum security.

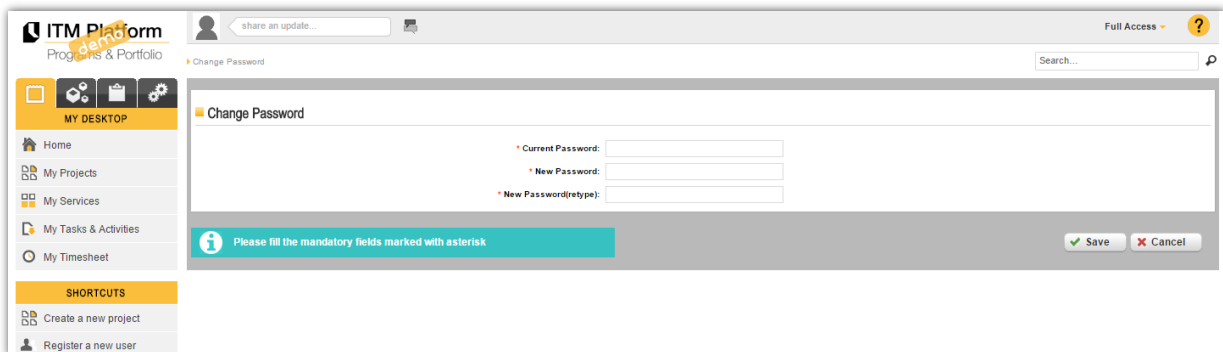
## 2. Access to ITM Platform

### 2.1. Passwords

ITM Platform grants access to the environment via the use of user passwords.

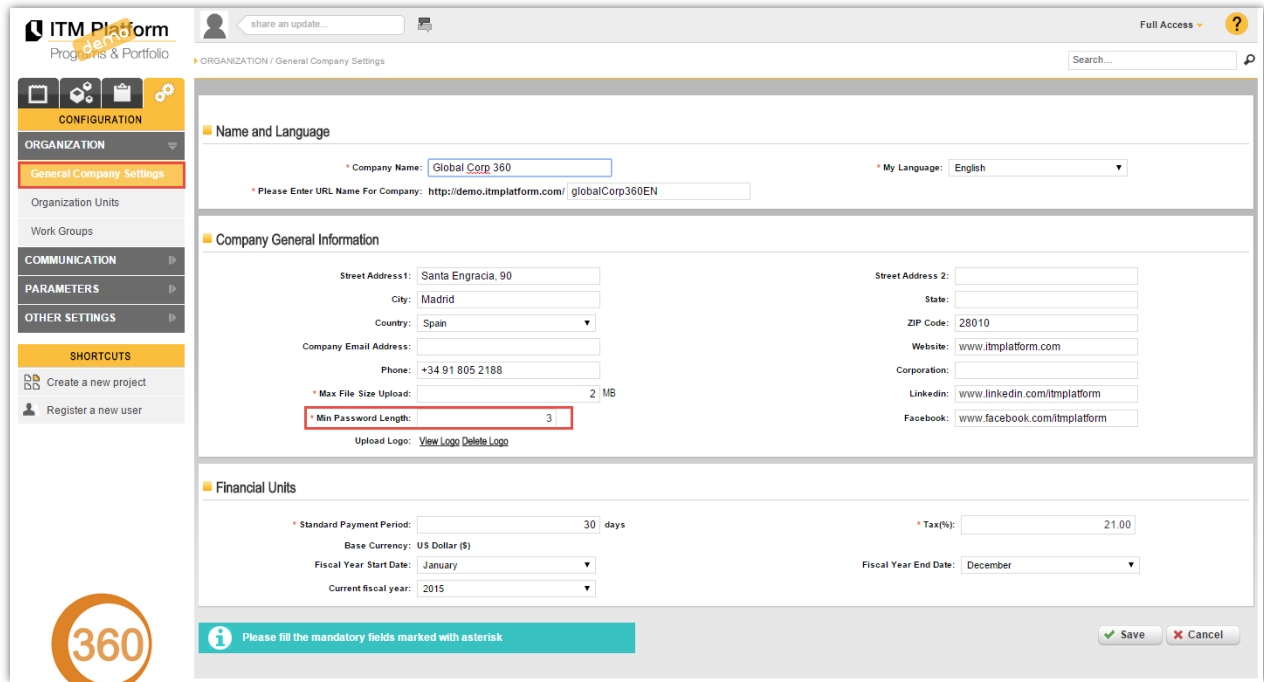


The email address is used for usernames and will also be used for sending notifications from the system. Users can change their passwords at any time:



## Password Length Configuration

Each organization can configure a standard length for the passwords used to access its environment. These changes can only be made by users whose role grants them access to the “General Data” window.



## Password Recovery

If a user forgets or loses their password, a new one can be requested via the “Forgotten your password?” option. An email containing the passwords will be sent to the email address used as the username.

## 2.2. Licenses

When a client acquires an ITM Platform solution, it receives the right to use a number of licenses that will grant access to the various ITM Platform functionalities.

These licenses configure the functions acquired by a client within a customized environment. One client can have licenses for every ITM Platform solution in such a way that each license will determine access to certain functionalities or others.

In turn, the licenses - the cost and conditions of which vary - define two key factors in terms of access to functionalities:

### Access to Functions

These functions allow users to be assigned as:

- Project Manager
- Service Manager
- Program Manager

If this type of function is not included in the license, it will not be possible to assign these roles.

See the chapter entitled Assignment as Project, Service or Program Manager for further information.



## Access to Functionalities

Licenses configure the access by each user to certain functionalities of the environment. In turn, the roles of each user that grant access to a larger or smaller set of functions can be configured in each license. See Chapter 2.3 *Roles* for further information.

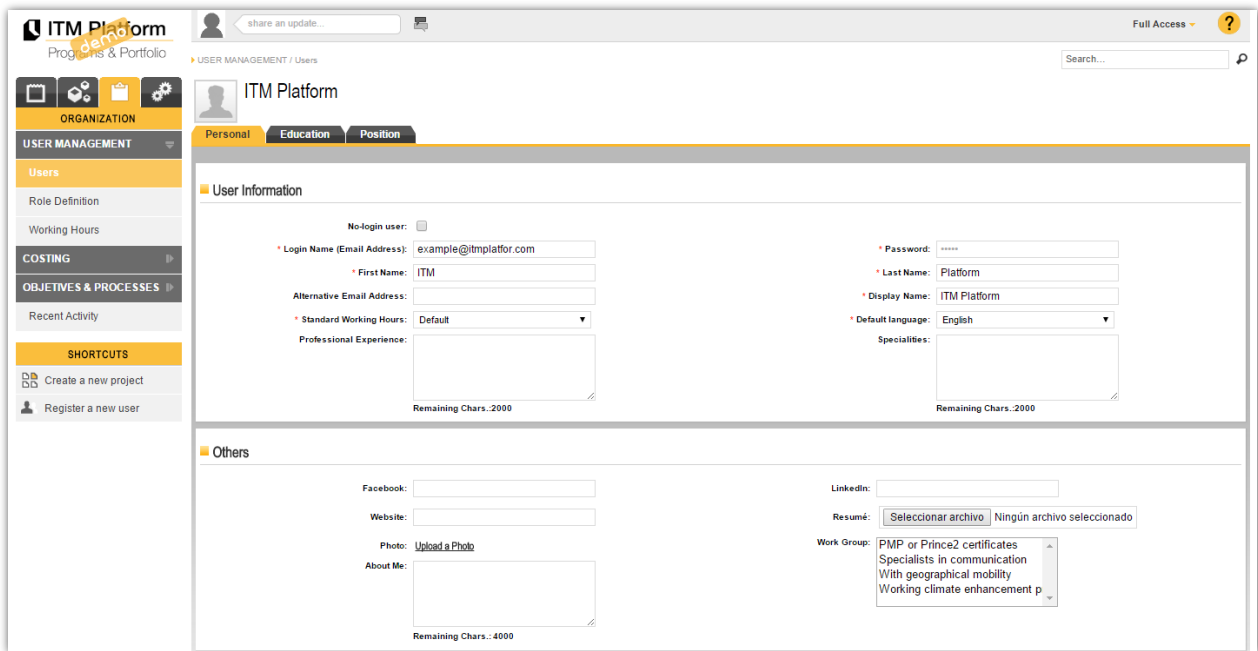
## Update Procedure

The license system is updated from the Product Development Department.

## 2.3. Roles

### Assigning Users

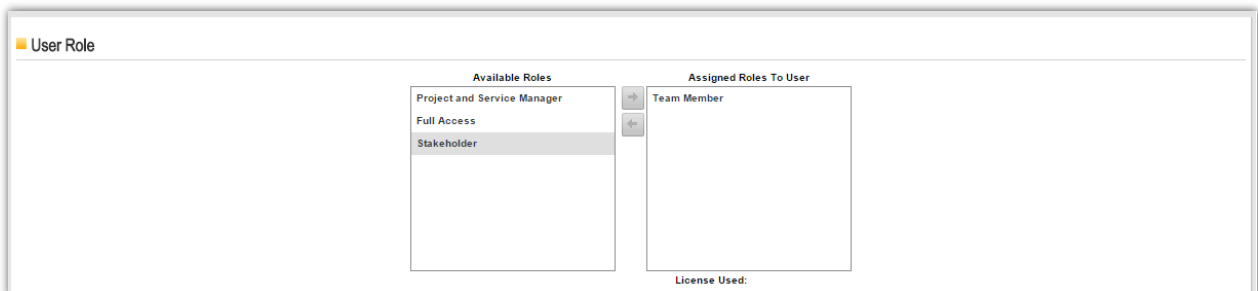
A role should be assigned whenever a new user is created. ITM Platform assigns a role to each newly created user by default.



The screenshot shows the ITM Platform user management interface. The user profile for 'ITM Platform' is displayed with the following details:

- User Information:**
  - No-login user:
  - Login Name (Email Address): example@tmplatfor.com
  - First Name: ITM
  - Alternative Email Address:
  - Standard Working Hours: Default
  - Professional Experience:
  - Password: \*\*\*\*\*
  - Last Name: Platform
  - Display Name: ITM Platform
  - Default language: English
  - Specialities:
- Others:**
  - Facebook:
  - Website:
  - Photo:
  - About Me:
  - LinkedIn:
  - Resumé:  Ningún archivo seleccionado
  - Work Group: PMP or Prince2 certificates, Specialists in communication, With geographical mobility, Working climate enhancement p

One user can have more than one assigned role, in which case the permissions associated with each role are combined. In other words, all the functions of each role will be available.



The screenshot shows the 'User Role' assignment interface. It features two columns:

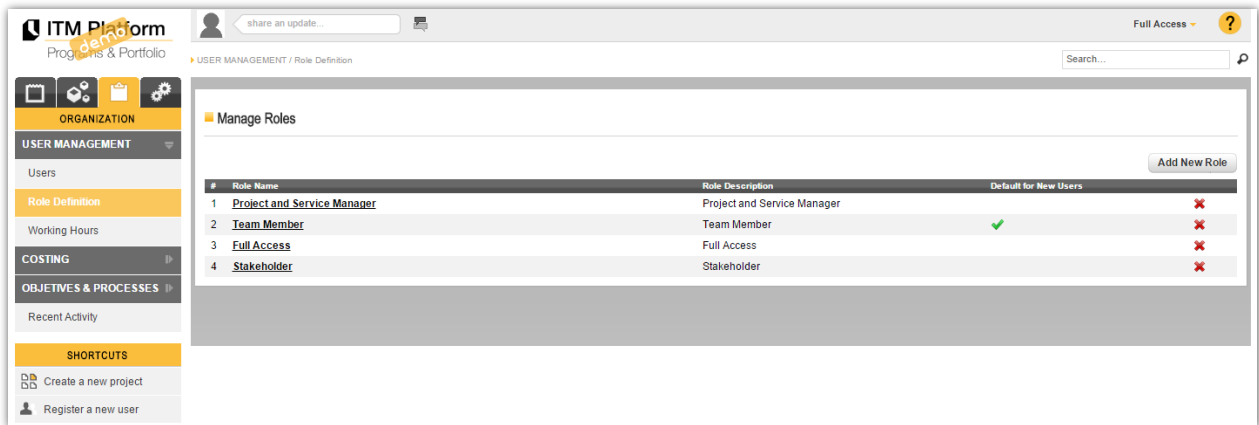
- Available Roles:** Project and Service Manager, Full Access, Stakeholder.
- Assigned Roles To User:** Team Member.

Arrows between the columns indicate the ability to move roles between them. Below the columns, it says 'License Used:'.

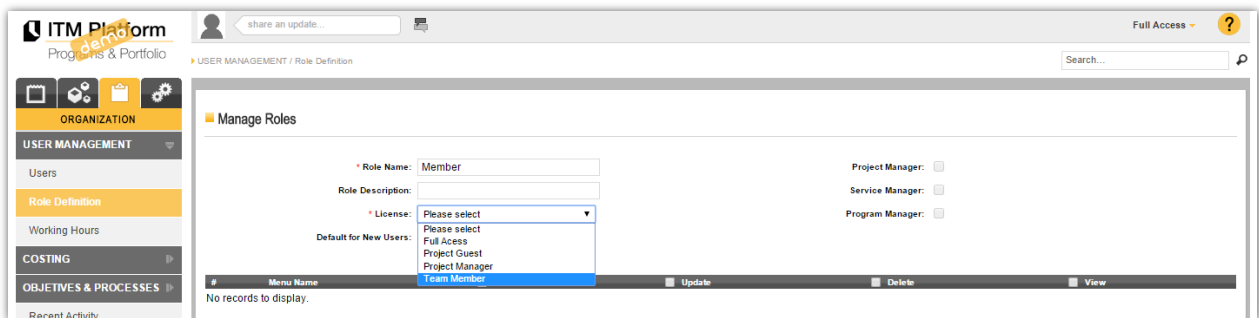
The functionality for creating users and assigning roles is only available for users whose role allows access to the “Users” option.

## 2.4. Role Configuration

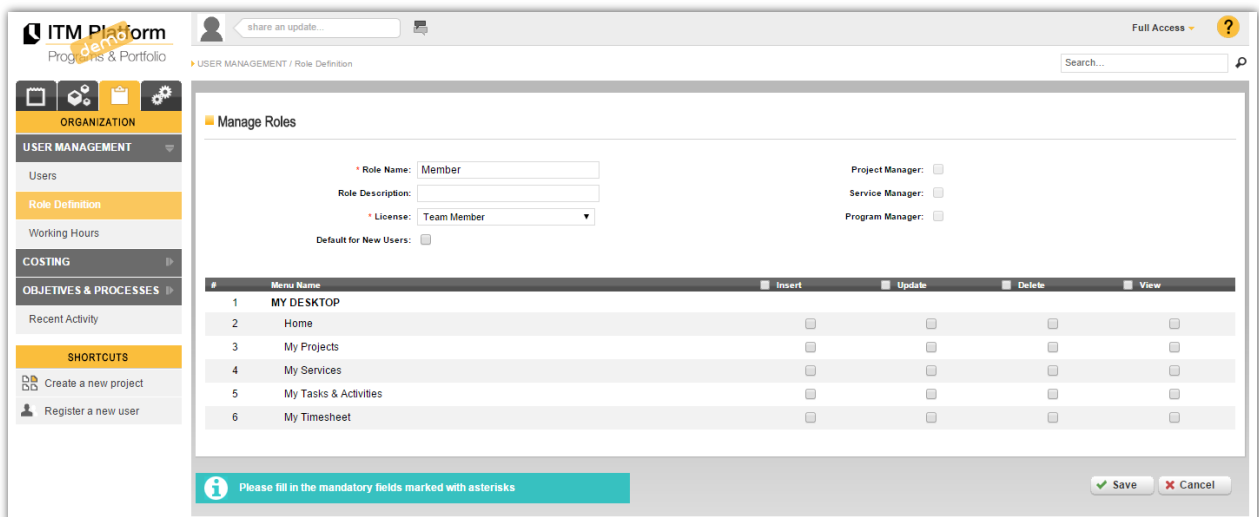
ITM Platform offers various pre-configured roles. However as many roles as are deemed necessary can be modified, added or deleted:



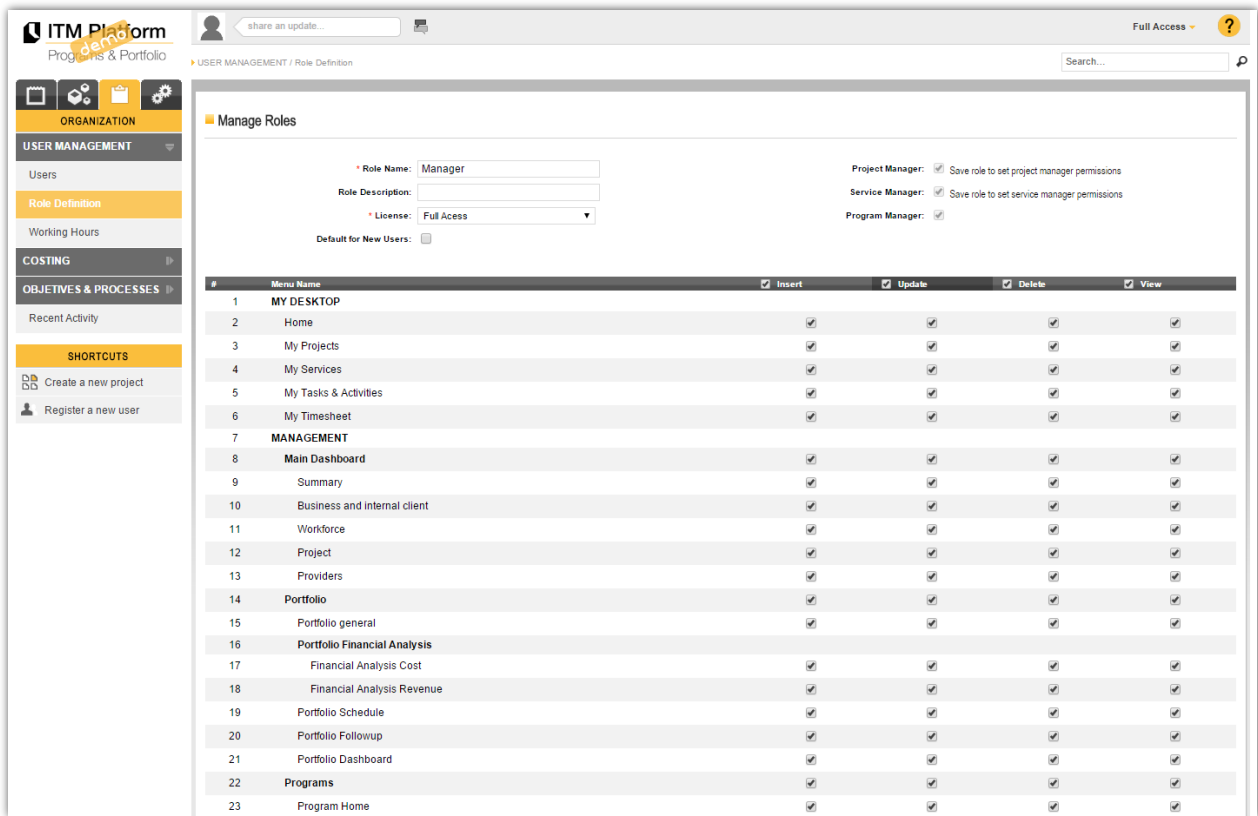
A fundamental step in creating a new role is assigning the license it will be used by. Hence, the basic configuration of *Access to Functions* and *Access to Functionalities*:



Certain options under the **Team Member** role can be configured but they cannot be assigned as Project, Service or Program Manager:



The **Full Access** role enables all options of this role to be configured and the user to be assigned as Project, Service or Program Manager:



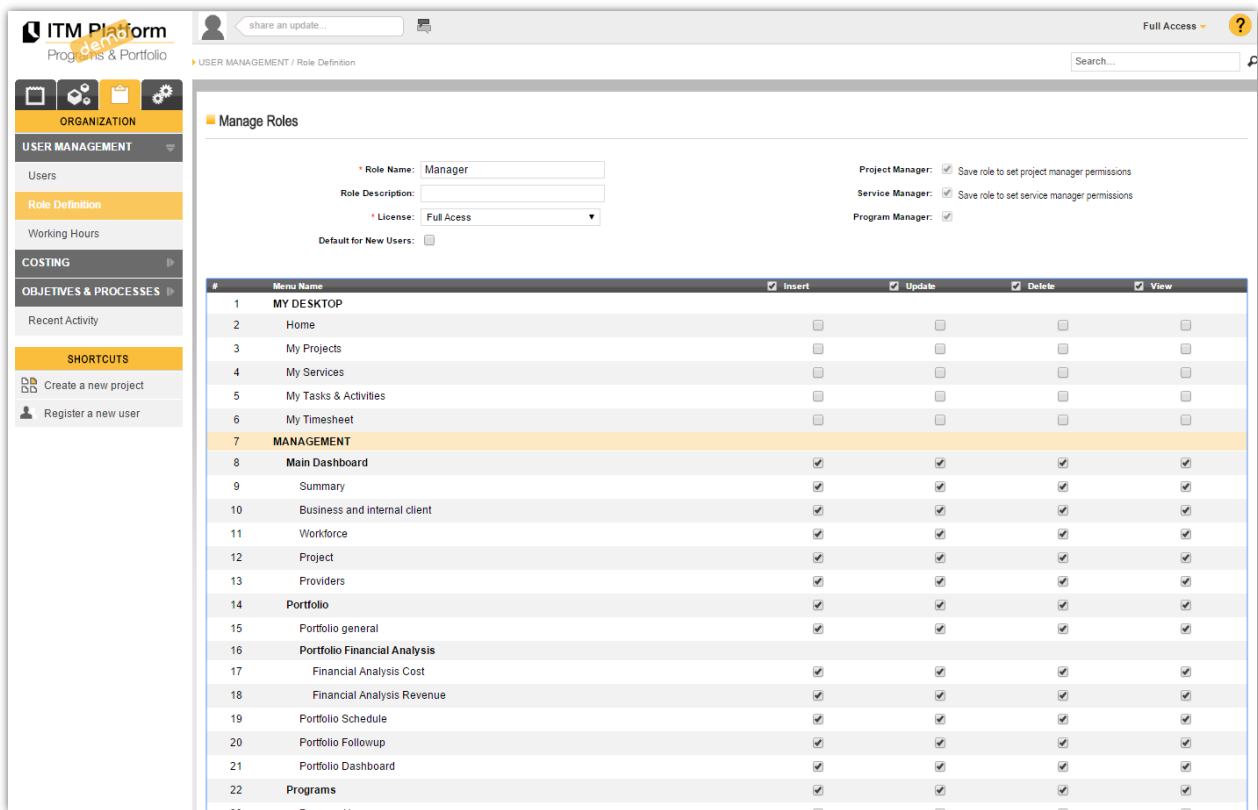
**Manage Roles**

Role Name:  License:  Default for New Users:

Project Manager:  Save role to set project manager permissions  
 Service Manager:  Save role to set service manager permissions  
 Program Manager:

#	Menu Name	Insert	Update	Delete	View
1	MY DESKTOP				
2	Home	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	My Projects	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	My Services	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	My Tasks & Activities	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6	My Timesheet	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7	MANAGEMENT				
8	Main Dashboard	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
9	Summary	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10	Business and internal client	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
11	Workforce	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
12	Project	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
13	Providers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
14	Portfolio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
15	Portfolio general	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
16	Portfolio Financial Analysis				
17	Financial Analysis Cost	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
18	Financial Analysis Revenue	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
19	Portfolio Schedule	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
20	Portfolio Followup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
21	Portfolio Dashboard	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
22	Programs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
23	Program Home	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

In this example, a role is being configured with access to all options under the **MANAGEMENT** function:



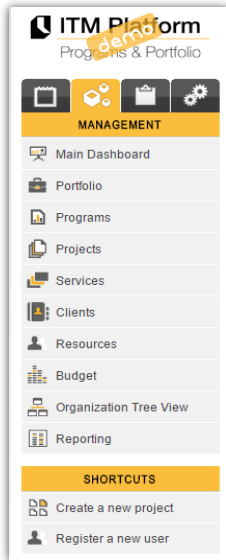
**Manage Roles**

Role Name:  License:  Default for New Users:

Project Manager:  Save role to set project manager permissions  
 Service Manager:  Save role to set service manager permissions  
 Program Manager:

#	Menu Name	Insert	Update	Delete	View
1	MY DESKTOP				
2	Home	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	My Projects	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	My Services	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	My Tasks & Activities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	My Timesheet	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	MANAGEMENT				
8	Main Dashboard	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
9	Summary	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10	Business and internal client	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
11	Workforce	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
12	Project	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
13	Providers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
14	Portfolio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
15	Portfolio general	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
16	Portfolio Financial Analysis				
17	Financial Analysis Cost	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
18	Financial Analysis Revenue	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
19	Portfolio Schedule	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
20	Portfolio Followup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
21	Portfolio Dashboard	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
22	Programs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
23	Program Home	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

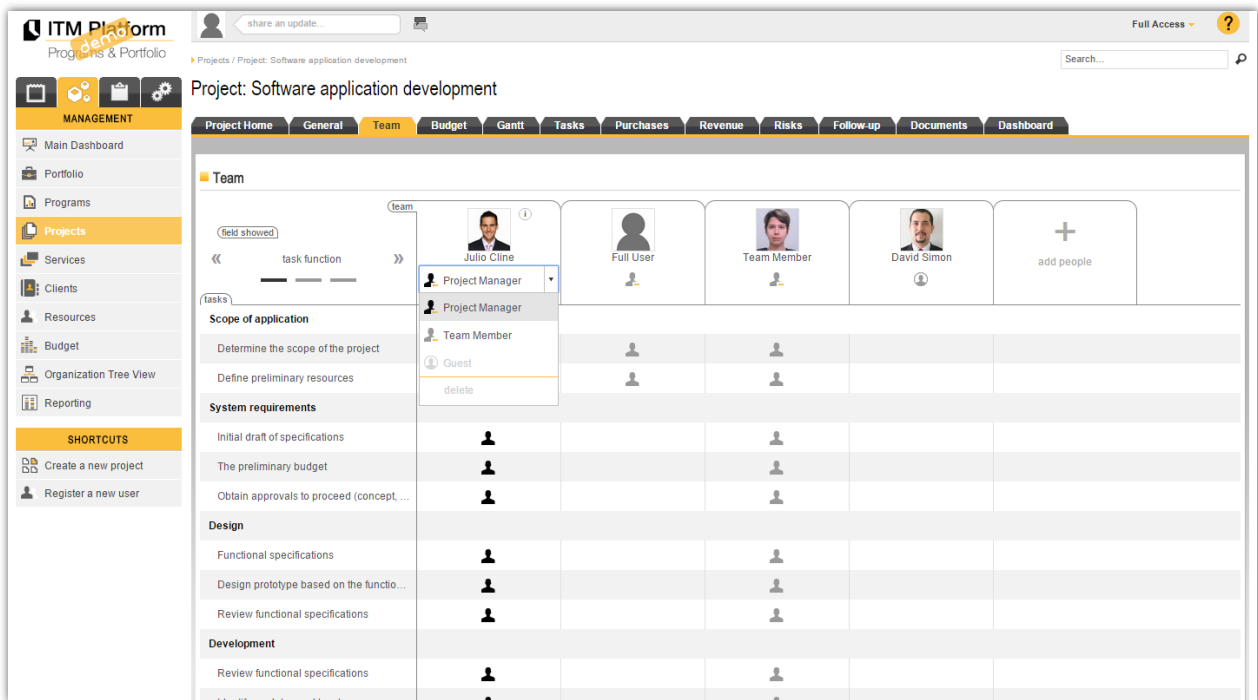
As a result, the user will see this menu configuration:



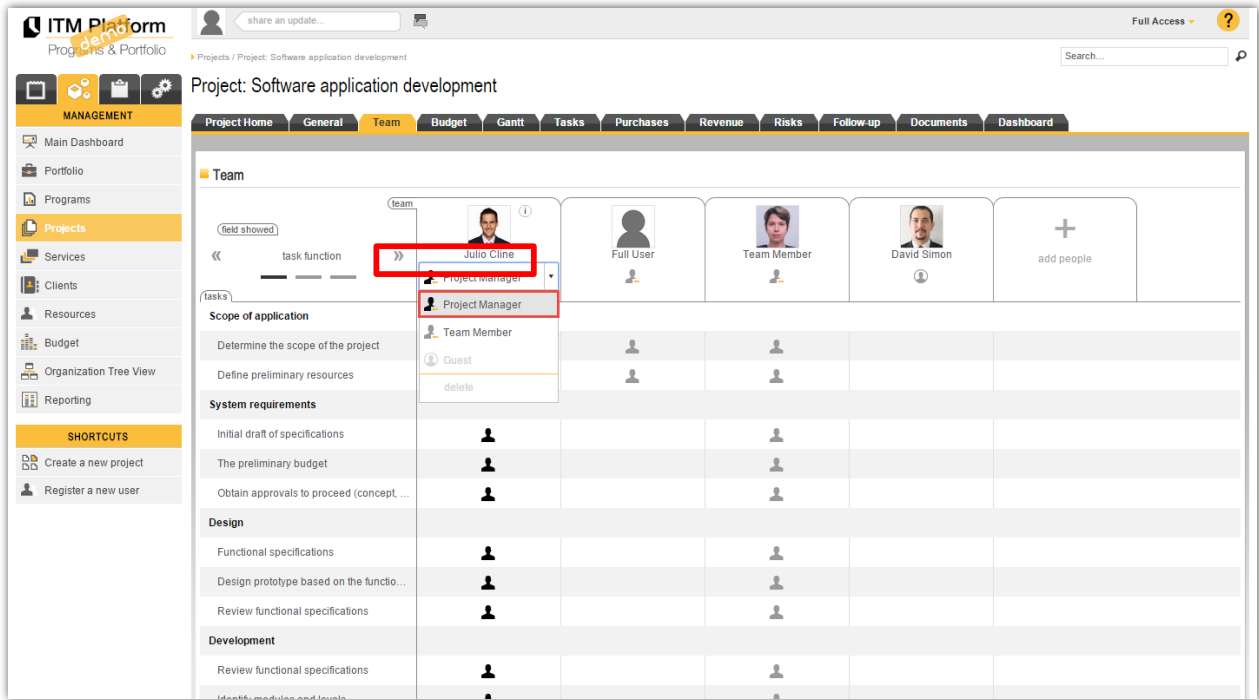
The functionality for creating users and assigning roles is only available for users whose role allows access to the “Role Definition” option.

## 2.5. Assignment as Project, Service or Program Manager

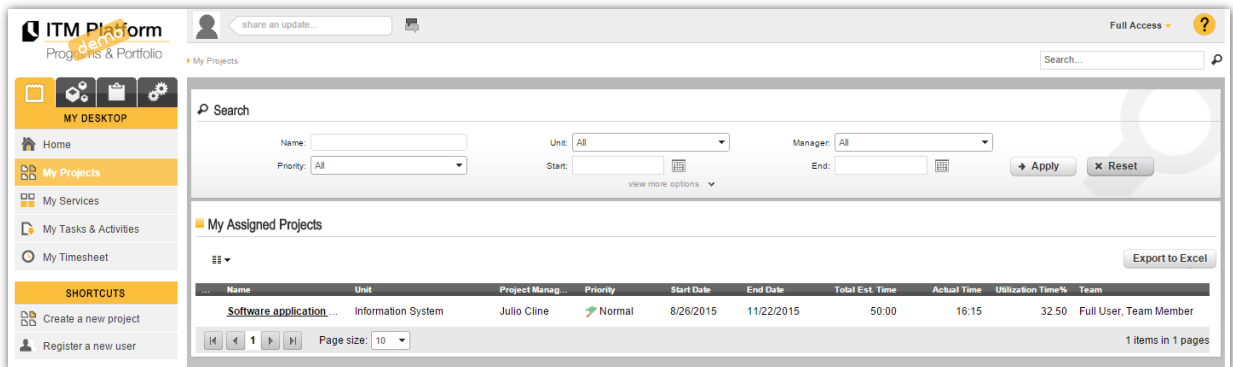
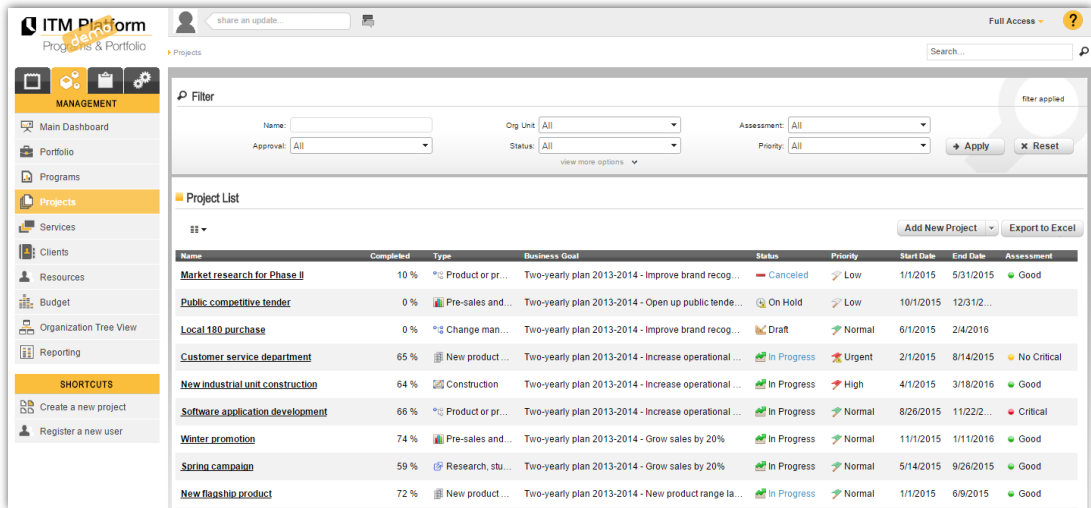
When assigning an ITM Platform user to the team of a project, service or program, they can be configured as a Project Guest, Team Member or Manager.



When assigning a user as Project, Service or Program Manager, ITM Platform checks that the user has a role that allows this to be done.

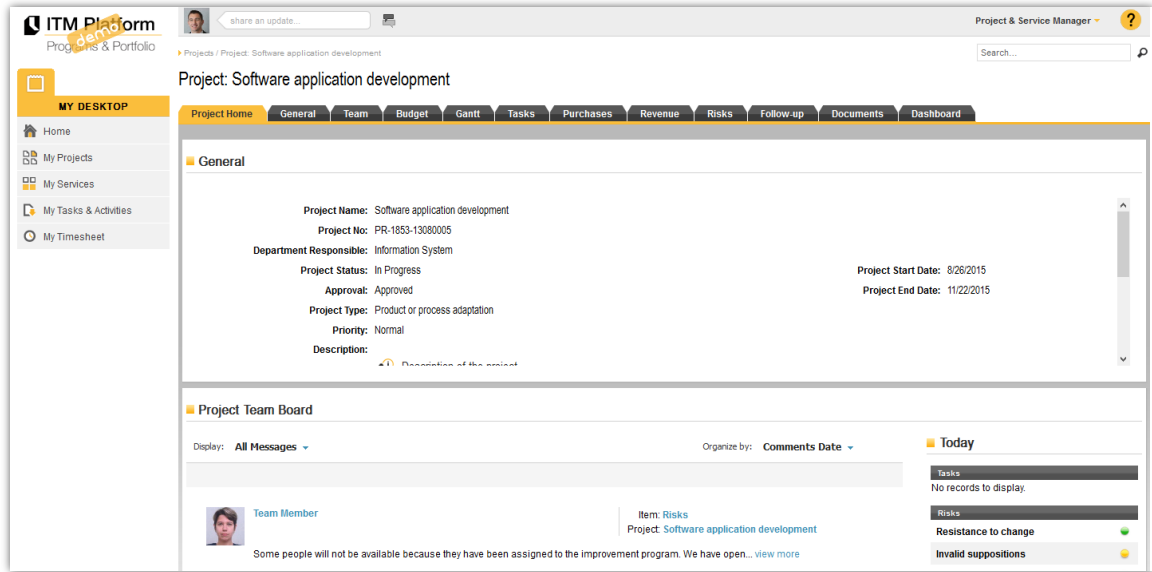


Whenever a user is assigned as a Project Guest, Team Member or Manager within a project or service, they can then access the “My Projects” or “My Services” options. The same does not happen with programs, which are only available through the MANAGEMENT tab.

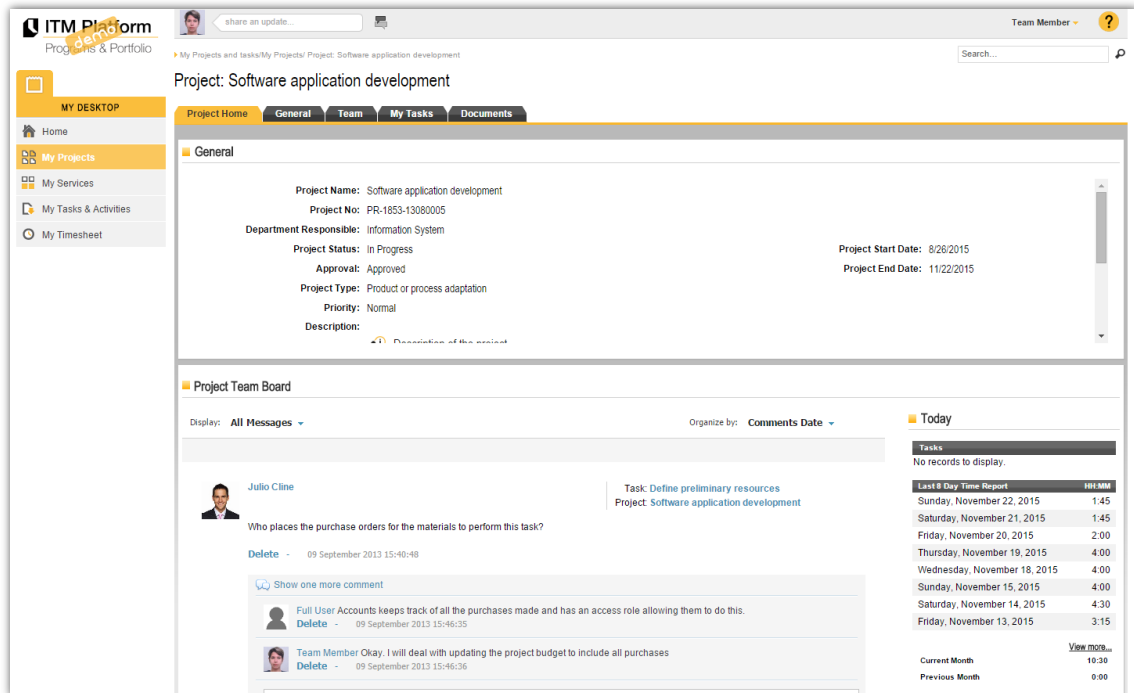


Whenever a project or service is accessed from the “My Projects” or “My Services” menu, respectively, two options will be available depending on whether the user is a Manager or a Team Member.

If the user has been assigned as a Manager, they will have both read and write permissions.



If the user has been assigned as a Team Member, they will only have read permissions.



## 2.6. Company Admin

As well as the above-mentioned users, ITM Platform also has a “Company Admin” user. This is the user who creates the environment and has complete access to all functionalities without license- or role-based restrictions.

## 3. Backup

---

### 3.1. Database

ITM Platform automatically creates a copy of the database every two hours. The copy is compressed and encrypted once it has been made. The open version is then deleted and the encrypted version is sent to the backup server. Subsequently, it is stored on the production server where it was made and finally an email is sent to the operators for copy control.

The copy stored on the production server is deleted after seven days but the copy on the backup server is kept.

The only reason for keeping backup copies on the production server is to ensure maximum data recovery speed in the event of a mid-level incident.

### 3.2. Web Files

Web files, including documents uploaded by users, are copied once a day, compressed and encrypted on the production server and the backup server.

They are deleted from the production server after one month but a weekly backup is kept on the backup server for one year.

### 3.3. Location of the Backup Server

The backup server is located on the premises of an external provider and therefore not subject to the availability of and access to our own production servers.

### 3.4. Encryption and Safekeeping

All backup copies are encrypted with strong algorithms and 64-bit keys to protect them from undue operations.

Backups are only stored on the production servers and the backup server. Backup servers have no data until they are converted to production servers in order to avoid possible security oversight.

All backup procedures are recorded in the operations book and only the operations team can handle backup copies.

### 3.5. Backup to the Client and Data Deletion

In the event that a client requests a backup copy of its data, the customer service team will first check that the person making this request is authorized to receive the data for recovery.

The operations team will only respond to those backup copy requests that are authorized by the Customer Service Department and will not respond to direct requests coming from the Support Department.

If a client asks for any or all information to be deleted from the database, the information will be deleted from the database and an additional backup copy will be made of the deleted data.

This additional backup copy will be marked as a special snapshot because it will not be possible to perform data recovery operations using backups dated prior to this snapshot. There is no way to delete client data from previously made backup copies.

### 3.6. Space for Backups

Here are some approximate backup copy file size figures:

## Backup Plan

### Data Base

Backups should be performed several times to ensure that we can retrieve customer data with a minimum data loss.

Date	Copy	nº	Location
Between now and 7 days	Backup every 2 hours	84	Main server and backup server
Between 7 days and 1 month	Backup every first hour of the day	25	Main server and backup server
Between 1 and 12 months	Backup every first hour of every monday	48	Backup server
		<b>nº</b>	<b>occupied space</b>
	12 month backup	241	24.100MB
	Main server	84	8.400MB
	Backup server	157	15.700MB
	average compressed size		100MB

### Web

Can be made less backups. It is convenient to have several versions to revert to a previous version if detecting a disastrous update, but do not need to manage multiple copies.

Date	Copy	nº	Location
Between now and 1 month	Backup every day at 01:00 UTC	31	Main server and backup server
Between 1 and 12 months	Backup every first hour of every monday	48	Backup server
		<b>nº</b>	<b>occupied space</b>
	12 month backup	110	5.500MB
	Main server	31	1.550MB
	Backup server	79	3.950MB
	average compressed size		50 MB



## 4. Backup Environment

---

A backup environment exists for recovering the system in the event of a major incident that prevents the production servers from providing a service.

This backup environment is located with an external service provider and therefore not subject to the availability of and access to our own production servers.

In the event of a major incident on the production servers, a contingency plan will be activated that, generally-speaking, establishes the following protocols:

- Complete block on access to the production servers while providing an incident warning to ensure that no clients continue accessing the servers while they are down
- Software version check on the alternative servers and update if necessary from the backup copy on the backup server
- Collection of database backup from the backup server and restoration thereof on the backup servers
- General system check
- Redirection of client access to the backup server

Once the incident has been resolved, the production environment recovery procedure is executed by using the backup environment backups and always as part of an operation planned in advance and notified to users.

An incident simulation will be performed once a year to check that all procedures are up-to-date and correct, and that the backup servers can be activated in less than two hours following a system collapse.

## 5. Software Control and Updates

---

### 5.1. Application

#### Environments

ITM Platform has two environments for use before any update is put into production:

- **Test:** a first level of software confirmation at which checks are performed to ensure that all updates are:
  - o Complete: checks to ensure that files, components and other elements are all present.
  - o Correct: checks to ensure that the changes or new functionalities are correct and perform their operations in accordance with the functional specifications.
  - o Compatible: checks to ensure that other functionalities that are theoretically unaffected maintain their functional specifications.
  - o Secure: a series of security tests are performed, which include code injection, access control and denial of service attacks.
  - o Efficient: the system is monitored to check that it maintains the same level of performance and there are no freezes or other execution incidents that could affect the platform.
- **Demo:** the environment tests are repeated in this environment and a second stage of testing is carried out, especially data-related tests because this environment includes data on organizations that are updated regularly. In addition, it is also checked that each update is:
  - o Whole: the data existing before the update is revised and checks are performed to ensure that the values remain the same or equivalent if changes were performed that affect the data.
  - o Consistent: checks are performed to ensure that the existing data and the new data behave as expected and do not cause inconsistencies between the various entities.
- **App:** production environment where, once all the tests have been completed successfully, ITM Platform is updated.

#### Authorization and Communication

Approval from the functional, systems and security teams is necessary before the production environment can be updated. If any of these teams disagrees with the update, it will be returned to the development team. Once the update has been approved, the operations team and support team are notified of the production launch date.

### 5.2. System

Server software is only updated by the operations team. Weekend maintenance includes a review of updates, patches and solutions from the manufacturers of the operating systems and basic software on all ITM Platform servers.

In the event that a manufacturer issues an emergency update alert, the ITM Platform systems team will assess the advantages or risks of completing this update outside of scheduled maintenance periods.

## 6. Online Security

---

### 6.1. Firewall and Port Blocking

ITM Platform has a first level of access through an external firewall that filters all port and server address access attempts.

This firewall includes a scan that warns of denial of service attacks and suspicious access attempts that might pose a security risk.

All servers have additional security filters that block all ports and addresses that are not strictly necessary. A security warning is issued if an attempt is made to access a blocked port or address.

### 6.2. Access Network and Administration Network

All servers have two network cards: one connected to the administration network; and another connected to the general access network.

Administration network access is only available to operations personnel accessing the administration consoles on the various servers. This network provides highly restricted traffic and enables access to the servers in the event of denial of service attacks produced by large-scale calls to the servers.

The general access network is used for access via HTTP and HTTPS protocols to the public web servers. This network only allows access to the appropriate ports and domains, but any vulnerabilities that may exist are especially controlled.

### 6.3. Suspicious Network Blocking

If access attempts are made from suspicious networks during a review process, an additional security protocol is created that blocks these networks in order to avoid attacks from zombie servers or other types of large-scale attack from uncontrolled locations.

## 7. Security and Vulnerability Control

---

### 7.1. Weekly Control

The following is performed during the standard weekly operating procedures:

- Operating systems and basic software update checks
- Complete antivirus scan of the servers
- General scan of the servers to detect any firewall configuration changes, unauthorized access to ports or addresses, or any other network security breach
- Reading of denied access logs to identify unauthorized access attempts

### 7.2. Monthly Control

The following is performed during standard procedures on the first weekend of each month:

- A general review of the server software, checking the system configuration and the version of all key files
- Execution of an extensive series of security controls

### 7.3. Quarterly Control

Every quarter, an external company performs a security assessment and simulates a range of attacks against the installations to ensure that no security vulnerability exists.

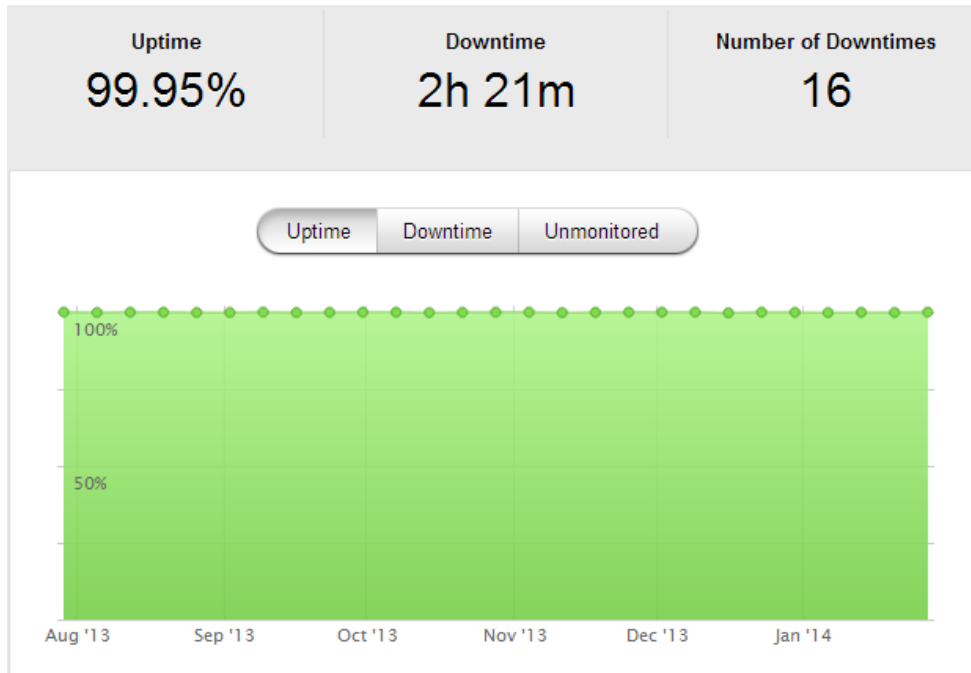
## 8. Availability and Performance

The servers have alert services that warn of any problems in the system.

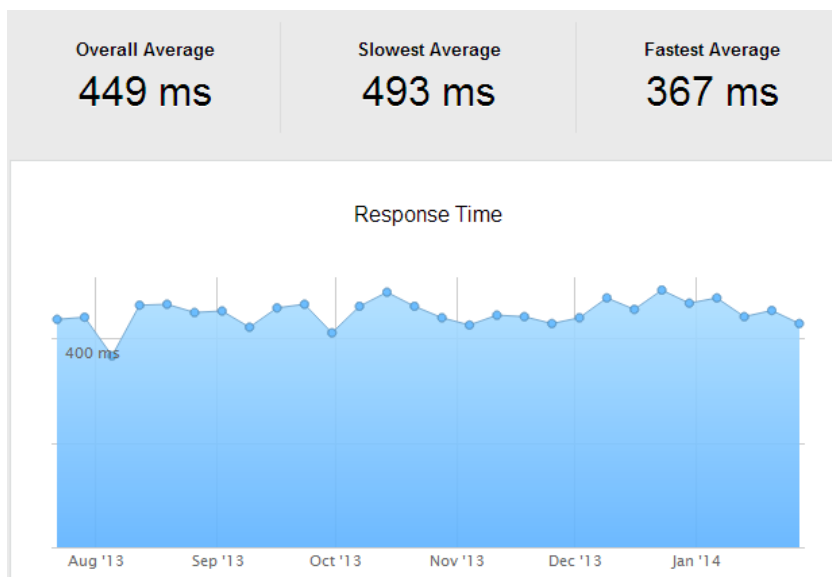
In addition, an external service monitors the servers and checks that the platform is offering a correct service every five minutes - not only from a systems point of view but also at a functional level of the application.

These services - both internal and external - constantly monitor the availability and performance of the system, warning of any problems that may arise.

The figures from ITM Platform last quarter were:



All downtime was scheduled and there were no client incidents





[info@itmplatform.com](mailto:info@itmplatform.com)



[www.itmplatform.com](http://www.itmplatform.com)