"Linked Open Apps Ecosystem to open up innovation in smart cities"
Project Number: 297363

Deliverable:	**D4.1 System Management Adaptation**
Version:	**V01**
Delivery date:	**08/02/2013**
Dissemination level:	**PU**
Author:	**RETEVISION, CISCO**
Reviewer:	**PMO**

Statement of originality:

This deliverable contains original unpublished work except where clearly indicated otherwise.

Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

Summary

This deliverable contains all additions, updates, integrations and developments made in the System Management of the Platform.

Administrator need to have real time information concerning the network in order to control the service level agreement for the iCity Platform. Therefore, information adaptation concerning the network management of the infrastructure devices has to be done and be delivered to the application layer to provide the need information SDK and the end-users. Furthermore, System Management tool should provide authentication and profiles for access.

DOCUMENT HISTORY

Version	Date of issue	Status	Content and changes	Modified by
V01	05/10/2012	Draft	Creation	Retevision
V02	21/12/2012	Draft	Edited Positioning vs. Existing solution	Retevision
V03	06/02/2013	Draft peer review	Final draft version peer review.	Retevision

Document contributors

Partner	Contributor
Retevision	Carmen Vicente, Javier Marcos, Luis Moreno y Elena Villa
CISCO	Frank Van Steenwinkel

TABLE OF CONTENTS

TABLE OF FIGURES

Abbreviations and Acronyms

Acronym	Description
WPX	Work Package X
D4.x	Deliverable 4.x
SSO	Single Sign On

1. Introduction

This document reports the work achieve in WP4 regarding with system management adaptation.

1.1 Purpose

The aim of this deliverable is to set up the first version of system management prototype, which has the main goal of provide real time information concerning the cities infrastructure integrated in the iCity Platform. Also, the system management has to be able to work with different platforms and has to provide access to them identifying each one of the external authentication processes.

System management has to establish an access control in order to decide the different type of information.

This activity is alive until the end of the project and the system management prototype will be enriched following the inputs coming from WP3, WP5 and WP7.

Finally, it is important to mention that this document will be alive and modified during the whole life of the project in order to adapt its contents to the final iCity platform architecture. It will gather in the following deliverable:

- D4.6 (M24).
- D4.11 (M35).

1.2 Scope

The deliverable is mainly focused on the definition of different features of system management, in order to describe in a easy way the prototype.

As a result, the iCity platform first version prototype adapts a simple System management which will be improved with more functionalities and features in future versions of the iCity platform prototype.

1.3 Overview

First part of the deliverable is a description of the different features of system management, and second part of the deliverable is focused on the description of the system management adaptation to iCity prototype.

2. System Management Definition

2.1 Security Access

2.1.1 Overview

The mail goal of security access procedure is to provide iCity platform the right levels of authorization and access to iCity resources, confidentiality and privacy assurance.

Thus, iCity platform must implement a system management that provides cross functionality to register all the actions on the iCity platform components.

The system management has to provide components for treating key aspects of security, tracking and reporting not only iCity platform activities but also apps that use iCity platform moduls. Therefore system management is responsible for:

- Provide both authentication and authorization services; and ensure proper levels of privacy, confidentiality and integrity of data.
- Log all the activities performed on iCity platform components, identifying relevant information from these actions.
- Use information from the iCity services catalog to manage all activities related with them.
- Log all the activities performed on iCity platform components, identifying relevant information from these actions.

The system management will cover the main requirements as:

- Authentication
- Single Sign On (SSO)
- Authorization
- Confidentially of data
- User privacy

- User management: profiles, access, etc.
- Tracking management: settings, queries, views
- Tracking log registration
- Reporting

2.1.2 Functional description

2.1.2.1 *Authentication & Authorization*

This component will be responsible for ensuring right levels of protection, security and privacy assurance in the iCity platform, as well as services or apps that interact with iCity platform.

Main goal is manage authentication and authorization of “users” (apps and iCity services).

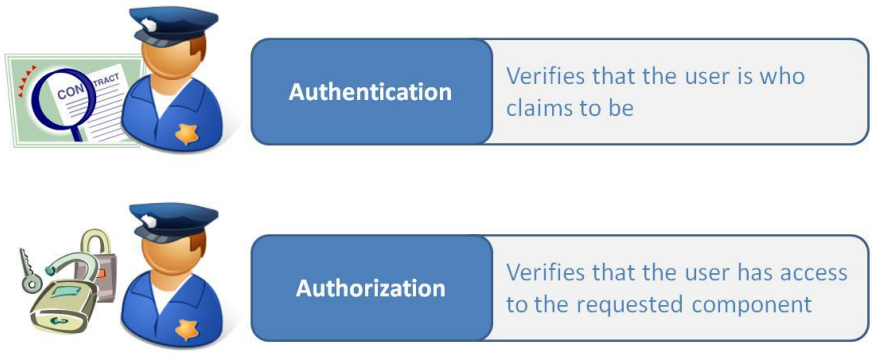

Figure 1: Authentication & Authorization

Furthermore, system management has to ensure secure interactions between users and iCity platform components, and covering following items:

- **Confidentiality:** Assure the privacy of the information, especially personal data.
- **Integrity**. Ensure that information is not manipulated by third parties.
- **Authentication**. Assure end-to-end identity of users and iCity platform components involved in a process.

- **No-rejection**. Ensure is not possible to refute the validity or ownership of information exchanged through the platform.

Authorization access module will enable settings to manage policies based on different user profiles and iCity components. It will use the information provided by the catalog of iCity services applying the right polices.

System management will include a setting module to manage security aspects related to users and services authentication and authorization requirements.

2.1.2.2 *Reporting y Tracking*

This module is in charge of activity tracking (logs) and transactions registry (reporting).

It will provide tracking registry of iCity platform components and services or apps, generating activity messages. Every track should include a time stamp, the security level of the track, the app and/or iCity service, and the description of the action.

3. iCity System Management Prototype

3.1.1 City Admin Portal

In this portal, the administration of the iCity Platform portals can be done.

Following roles are required:

- Administrator with full access rights
- API manager to manage the API settings
- Community manager to manage communities and users
- Content manager to manage the documentation and blogs
- Portal manager to manage the portal settings
- Program manager to manage the reports
- Reports user to access the reports

The API manager approves the API requests made by the developers.

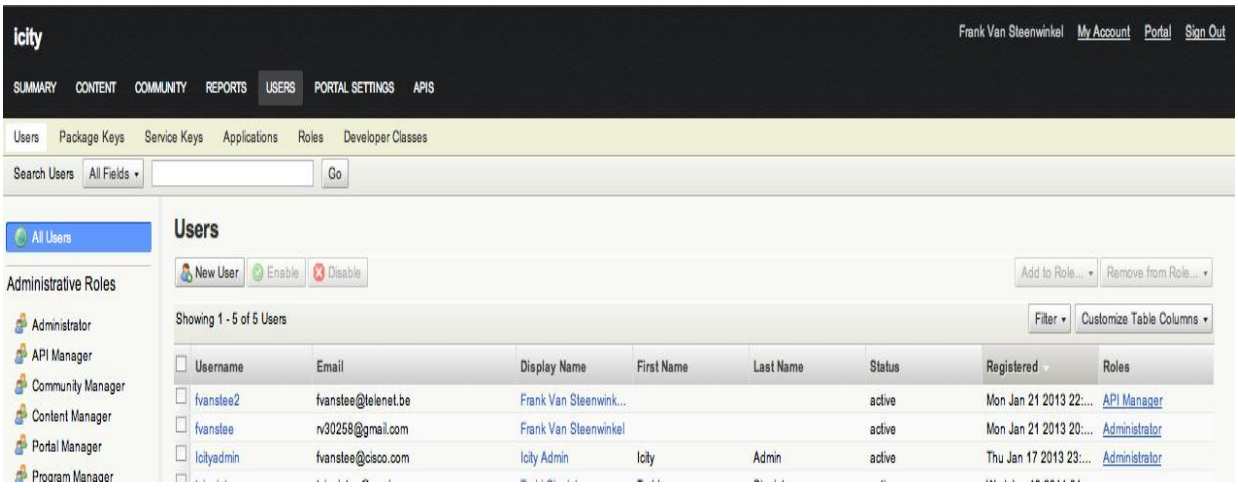

Figure 2 Example of user role assignment

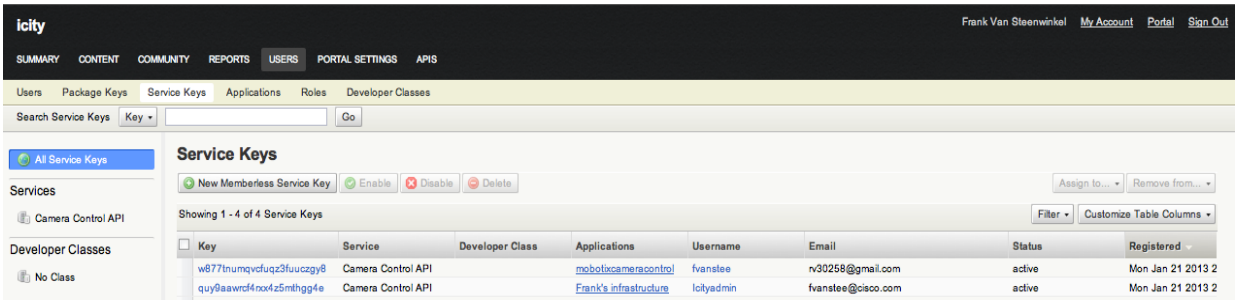

Figure 3 Example of Service Keys linked to Developers

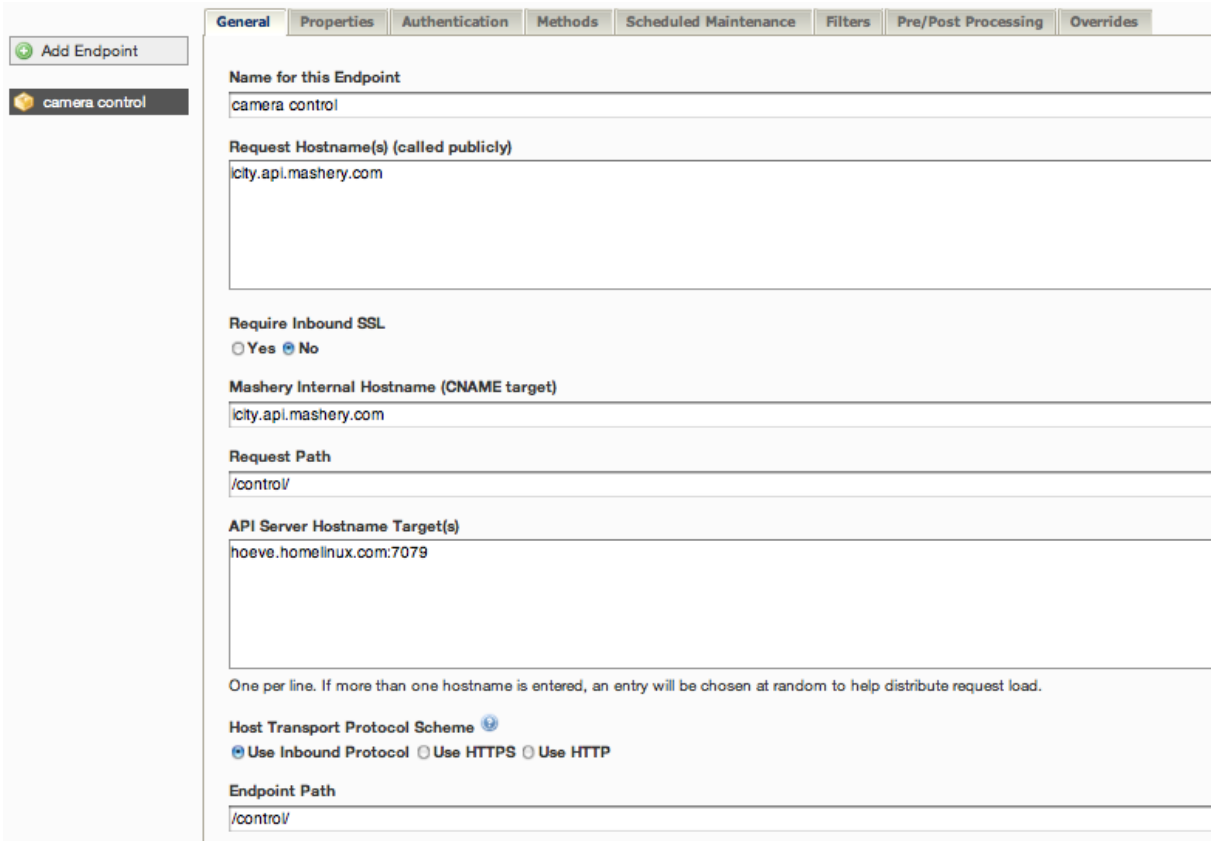

Figure 4 Example of endpoint (camera) configuration

Figure 5 Example of endpoint Authentication configuration

3.1.2 iCity System Management

This system permits the management of all the iCity Platform elements and services as well as the creation, erase and administration of the System Management users and groups.

The Advanced menu makes possible the visualization and the management of all the users and groups of the system.

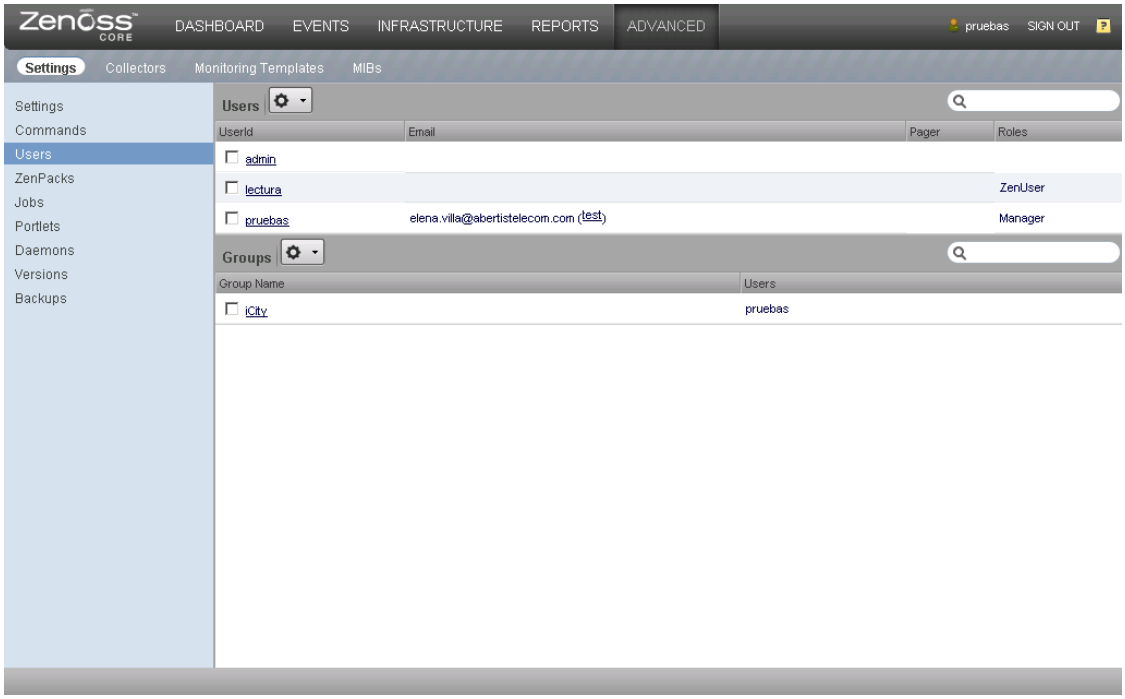

Figure 6 Example of management system

The administrators can create new users assigning to them different roles or groups and modifying its properties.

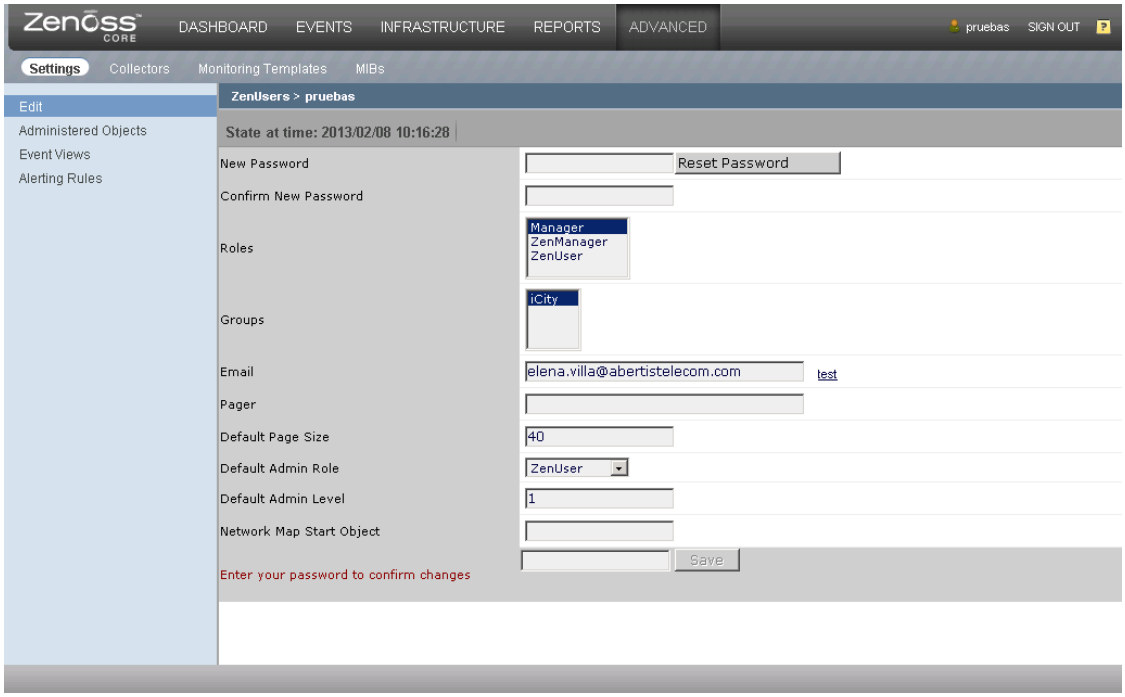

Figure 7 Example of user's creation

In addition, the administrator users can create groups to allocate and agglutinate the different users of the System Management and facilitate their administration and permissions.

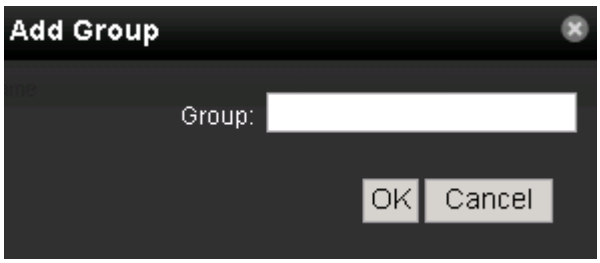

Figure 8 Example of group creation

The administrator users can manage and edit the existent ones and change their properties (passwords, group, e-mail, etc.).

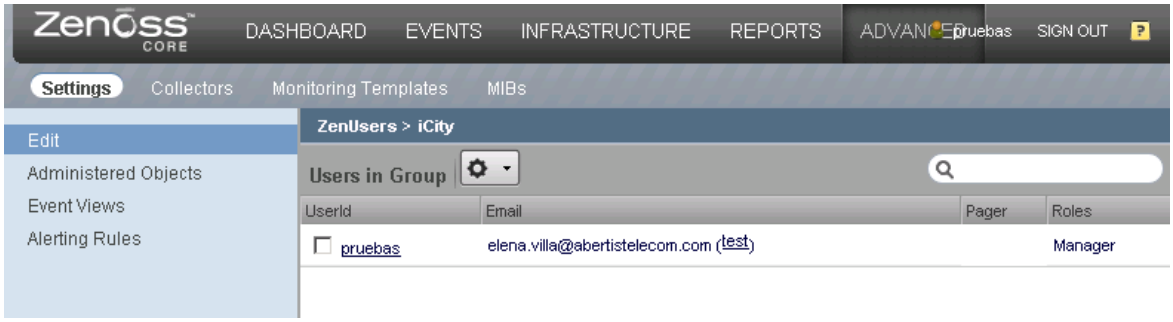

Figure 9 Example of editing users

The System Management permits the visualization of the number of events, separated by their severity level, of the iCity Platform elements and services associated to this user or group of users.

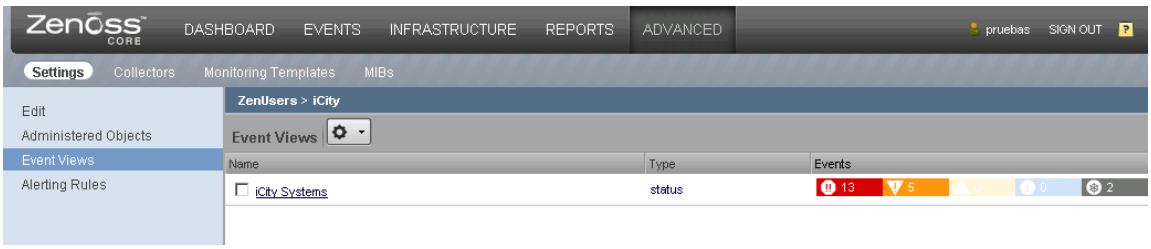

Figure 10 Example of editing event views

4. Conclusions

This first year, a preliminary system has been included in the prototype in order to allow, in a short time, the deployment of pilots and also the development of apps, with basic system management adaptation that would provide access to different urban service delivery platforms for each external authentication process.

System Management adaptation offers the following benefits:

- Reduce risk of denial-of-service attacks.
- Permits graceful, linear scaling.
- Improved customer experience through easy service access, and streamlined service delivery.
- Reduced operational costs and prospective investments through flexibility and simplicity of service delivery.
- Provides extensive capabilities for integrated management of identity, rules, en-user devices, content and partners.

Future evolutions of the prototype (D4.6 & D4.11) will follow inputs coming from WP3, WP5 and WP7.