TECHNICAL NOTE

OutSystems® Platform

Security Overview

The OutSystems® Platform has an extensive set of built-in security features. This datasheet focuses on how every application created using the OutSystems Platform is secured over its entire lifecycle.

Table of Contents

1 Application Security Vulnerability Prevention & Detection

All applications built using the OutSystems Platform include a number of vulnerability prevention measures that are applied at different stages of the application development and deployment process.

1.1 Application Design

During application design, developers set configuration attributes that direct the code generator and the deployment service to set the way in which applications can be accessed.

- **HTTP / SSL encryption** per page and web service when data encryption is required
- **Windows Integrated Authentication** to use operating system credentials to automatically login into a given page or application
- **Active Directory / LDAP Authentication** to centralize all of the end-users' login information in a single Active Directory / LDAP server
- **Role-Based Access Control** restricting access to pages depending on specific application level roles
- **Network-Based Security** when access needs to be restricted to a specific IP range

Developers define application level permissions by using visual access control building blocks (called Roles) to declare a set of capabilities under a given access restriction. These can, for instance, aggregate access to every application page that involves changing a specific database table.

Developers can also create access control logic to implement flow control for users who are not authorized to access a specific resource. These requests will raise an exception that can be handled by presenting an error message or directing the users to a different area of the application.

1.2 Application Validation

Before submitting any application to the code generator and the deployment service, Service Studio performs a validation that contains a number of security checks, including:

- **Potential violation of data isolation** warning when defining queries to different databases
- **Developer access control validation** to ensure individuals have permission to generate and deploy the application and to use any external components, APIs and data models

1.3 Code Generation, Optimization and Compilation

The OutSystems Platform generates, optimizes and compiles C# and Java code using secure code patterns, as well as introducing the enhancements to the base framework outlined below:

- **HTTPS support** to prevent eavesdropping and session hijacking
- **Strong session identifier validation mechanisms** leveraging those provided by the Java and .NET frameworks to prevent intrusion on existing sessions from multiple devices
- **Cross-site scripting prevention** by automatically escaping the generated HTML and providing built-in functions to sanitize HTML when developers handcraft HTML code
- **Encrypted password for database connections** to securely create and manage database accesses
- **SQL code injection prevention** by using SQL parameterization and providing built-in functions to sanitize the strings that developers include in their queries
- **C# and Java code injection prevention** as the generated code does not allow any type of late binding or runtime access to any pre-compiled code
- **Dedicated and isolated database connection pools** per each pair of application / database preventing cross application and cross database access in runtime

- **Total runtime isolation and containment** by using code generation patterns that ensure there is no way to take advantage of low level process or thread configurations
- **Full exception handling** as all exceptions (including encryption, authentication and authorization) are handled in the generated code and logged for later auditing even when handling was not created during development – this prevents the exploitation of any vulnerability arising from specific exception or error code in the responses provided to the browser

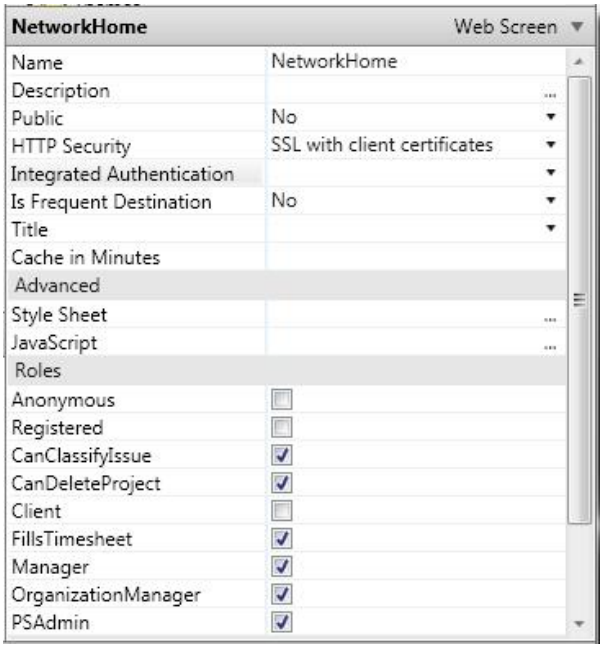

Figure 1. Set your user profiles access rights and enable authentication and/or encryption using a graphical utility.

1.4 Application Deployment

The OutSystems Platform's deployment engine configures Microsoft's Internet Information Services (IIS) security settings according to the most demanding application design and security best practices including:

- **SSL certificates** configured on a per site, per virtual directory and per page level
- **Client-side SSL certificates** management and configuration to enable stronger authentication of selected clients
- **Windows Authentication** configured on a per site and per virtual directory level
- **Override of security and access control defaults** to files placed in virtual directories to prevent "by default" vulnerabilities of IIS
- **Deployment of applications across multiple farms in different network zones** according to centrally managed configurations to ensure intranet functionality binaries are never installed in internet or extranet servers
- Optional **use of operating system credentials** to execute the application processes

1.5 Database Network Data Encryption

The OutSystems Platform is fully operational with Oracle's network data encryption using the RC4 algorithm, the international standard for high-speed data encryption, up to 256-bit key length.

1.6 Generated Code Vulnerability Scanning

In order to systematically ensure high-security standards for its generated applications, OutSystems leverages security assessment tools as part of its automated quality assurance process on every product release.

Integration with HP Fortify Static Code Analyzer has been setup to perform automatic code vulnerability scans during regression testing. These tests, supported by an aggressive criteria for release acceptance– fix all critical, high and medium reported code vulnerabilities – ensures that the generated code is inherently secure.

As new code vulnerabilities are found in the generated code, a security patch is issued that permanently fixes them for all applications, on all customers.

2 IT Security Management & Auditing

The OutSystems Platform includes access control management for all application resources, providing flexible permissions to define the access rights for any given resource. This helps you to manage large teams with different profiles, as well as clearly separate the access to the platform's integration, assembly, deployment and change services in multiple development, quality and production environments. Moreover, it provides you with full access to the system audits required for IT-level SOX / ITIL controls and control deployment zones.

2.1 Role-Based Resource Access Control

Define IT Teams' responsibilities through Roles. For each role you can configure which applications they can access and if they are allowed to create and change them. Built-in access levels range from List Only (to inform IT users the resources exist) to Full Control (to allow IT users to fully change, manage and deploy resources).

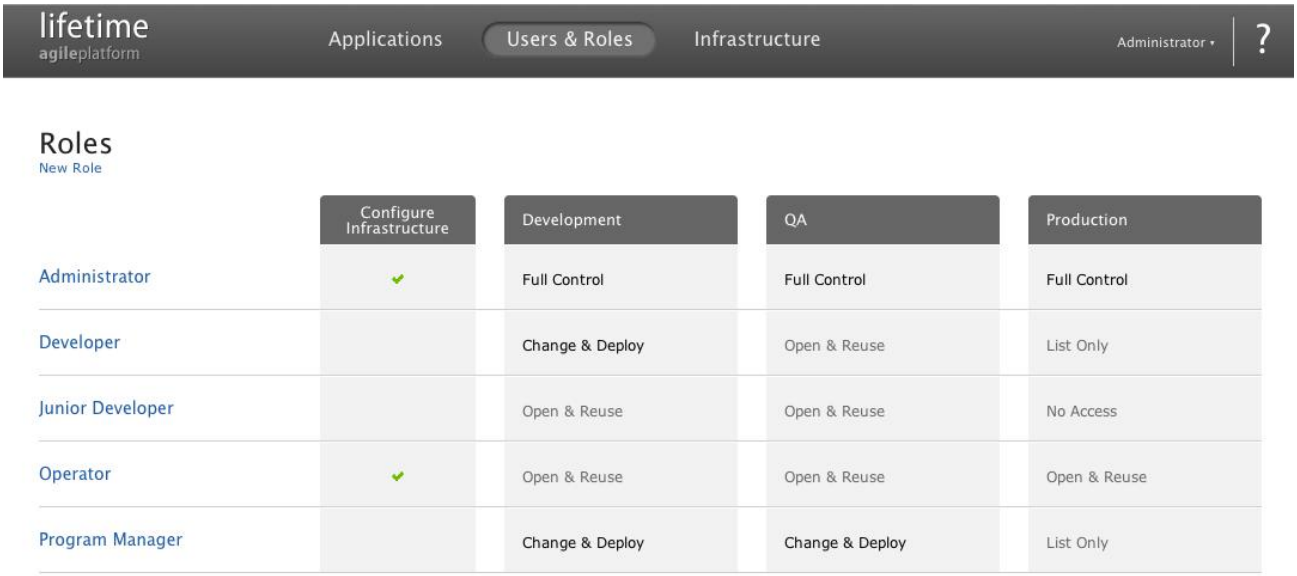

Figure 2. Easily review the access levels of each role in your IT team.

Each built-in access level incrementally builds upon each other in determining the development and management capabilities that are available to IT users with that Role.

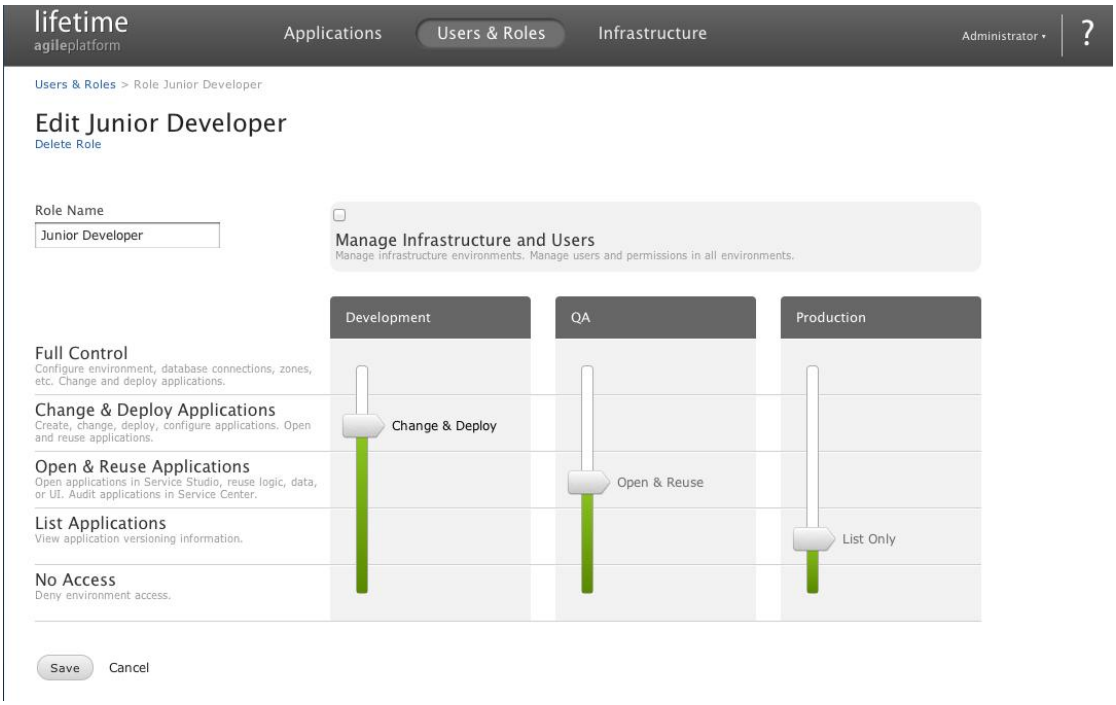

Figure 3. Easily define the level of access that should be provided to each role in your IT team.

2.2 IT Process Auditing

Every activity performed by developers, application managers or system administrators is tracked in a system log for future audit. Events tracked include:

- Storing a new version of an application or component
- Deleting an application or component
- Deploying a new version
- Modifying user configurations
- Logging into the system

Furthermore, the System Audits and Version Control subsystems of the OutSystems Platform allow auditors to identify when a modification to an application was applied, by whom, and even inspect the exact content of that change using OutSystems' Service Studio visual difference & merge tool.

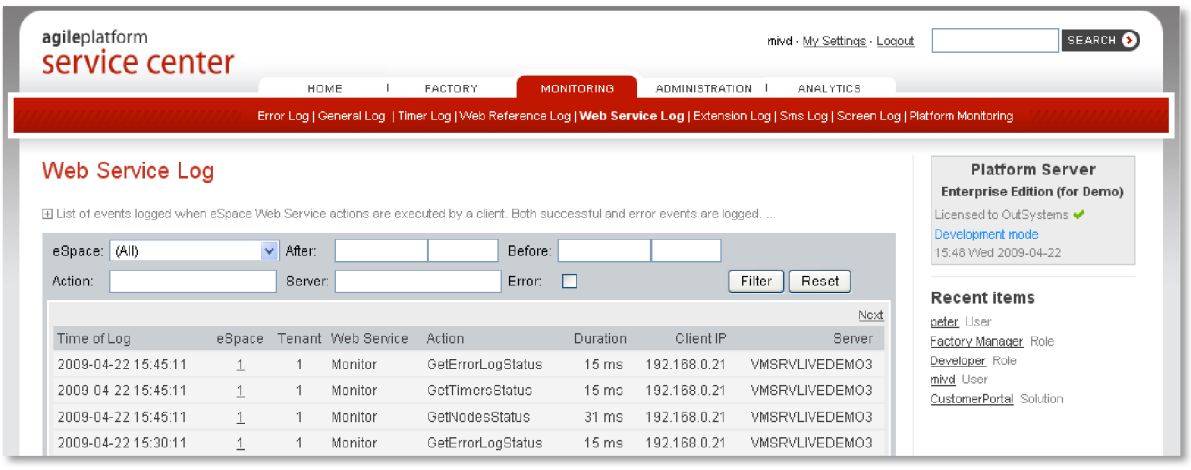

Figure 4. Detailed logs of all web service calls by external systems.

2.3 IT Runtime Auditing

The OutSystems Platform logs all access to external systems performed through web services or custom integration logic, and all web service requests addressed to applications in the Platform. The logs keep a record of who made the request, the request's target, the method called, how long the request took and the exact time of the request. This allows you to efficiently and effectively track down any security issues that may arise.

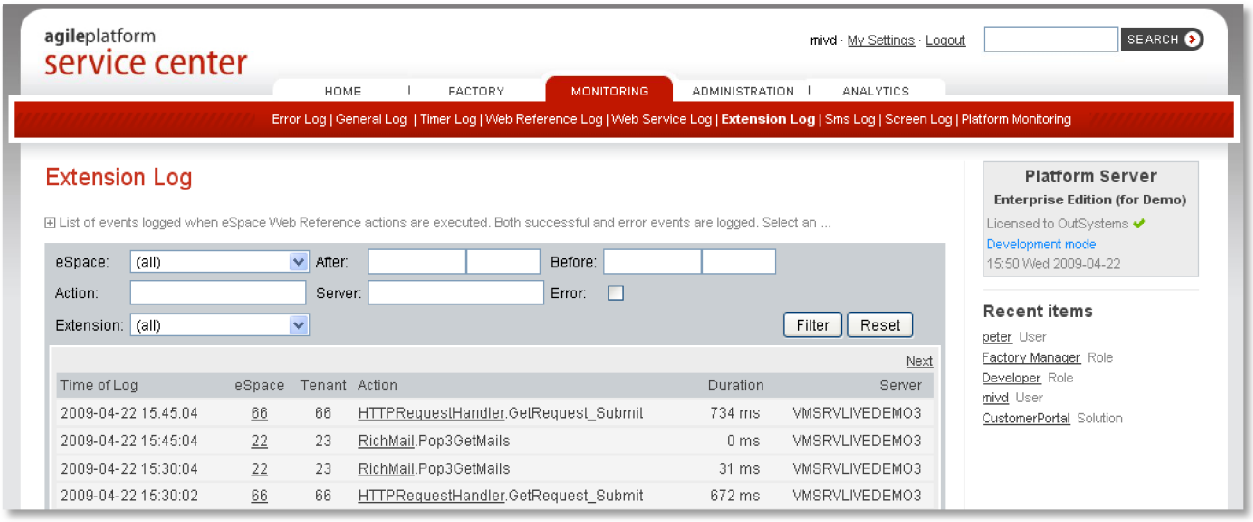

Figure 5. Detailed logs of all calls to external systems.

2.4 Network Zones Management

Configure the way in which front-end servers are spread across the various configured networks (Internet, Intranet, and Extranet) and define which applications are deployed to which clusters of the front-end servers. You can, for instance, have your internal applications running on the internal network zone and your websites running on a demilitarized zone.

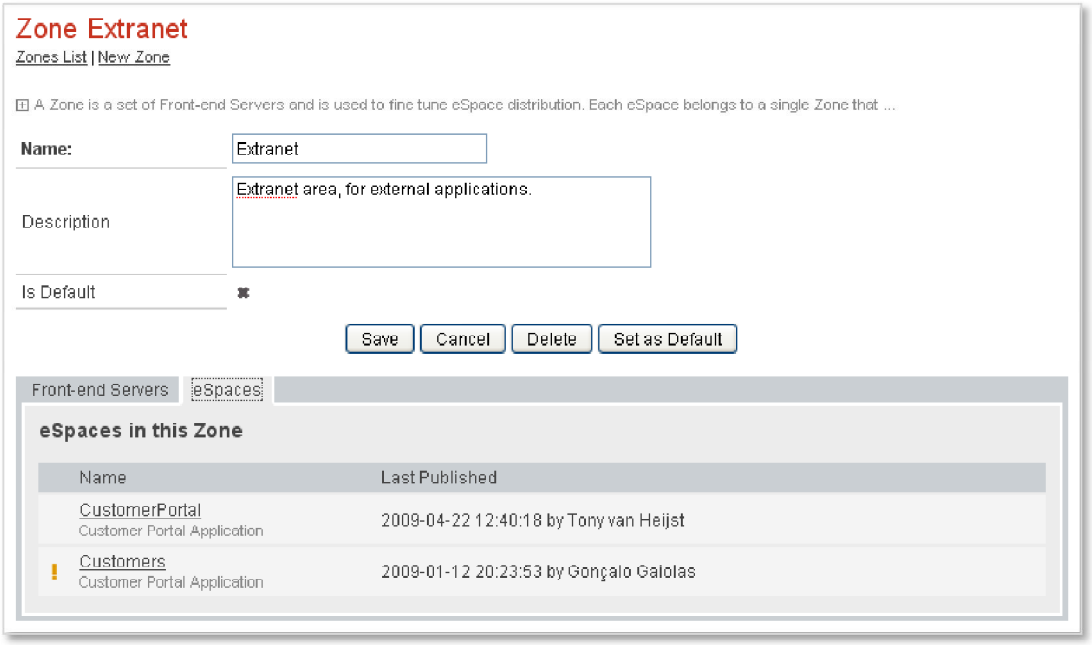

Figure 6. Detailed configuration of front-end Servers and eSpaces associated with a network Zone.

3 End User Security Management & Auditing

Once users are registered to use an application, proper access control measures need to be setup to ensure that only authorized users are allowed to perform specific business functions.

3.1 Role Based Access Control

Users can be provisioned and granted access to one or more roles. User management can be done from the back-office or through the applications using APIs that are available to developers. Application managers can use a meta-data driven back-office to create and configure specific user roles. The definition of a user role is completely dynamic and independent of the application development phase.

3.2 Single Sign-On

The out-of-the-box single sign-on capability allows you to unify logins across all the applications you choose. The user is then able to move seamlessly across applications without additional logins being required.

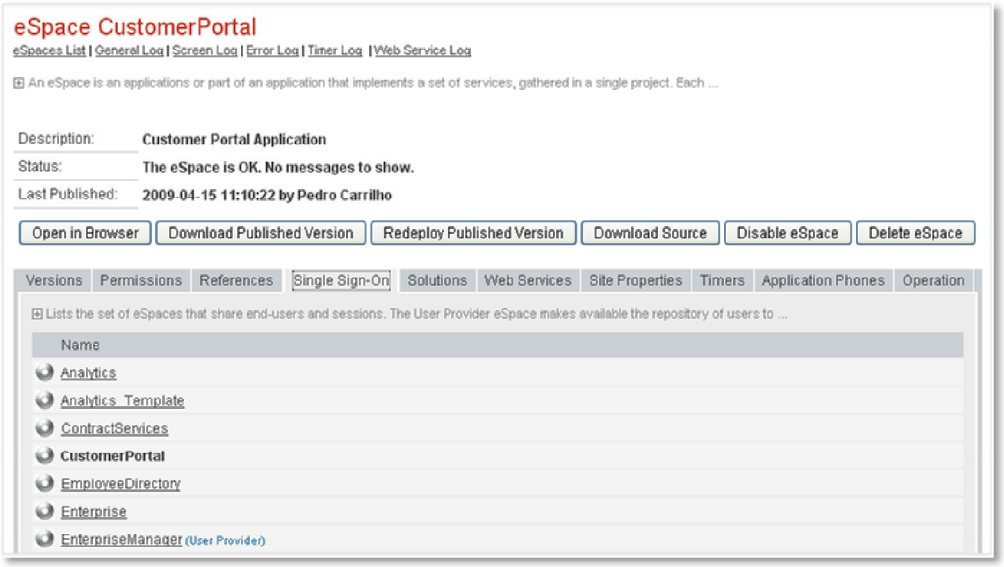

Figure 7. The end-user login can be unified across any number of eSpaces.

3.3 End User Access Auditing

Every access to your applications' screens is tracked in detail by default in the OutSystems Platform. These logs include the component and screen accessed, which user accessed it, when the access occurred and exactly which node served the screen. This allows you to effectively track down any security issues that may arise.