The Actuate Professional Services Security Integration Package is designed to provide new and existing Actuate customers with the implementation of Actuate user authentication and authorization that will function with the requirements of most security applications.

Authentication is the process of identifying an individual based on a username and password, and Authorization is the process of giving individuals access to the system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

The e.Reporting Server’s Open Security Directory Integration feature eliminates the need to replicate user and security information in Actuate, making user administration a scalable process. User information including authorization, authentication, roles, and access privileges can be externalized. As you define, change and control user access to your other computing resources (email systems, applications, file servers, etc.) via a central directory, you can also control user access to Actuate.

To assure success in implementing your Actuate security integration solution, Actuate’s Professional Services organization will employ a team approach and a flexible methodology. Actuate will staff this 20-day engagement with a highly qualified, certified Actuate consultant and will assign an Actuate Professional Services Project Manager to lead the engagement.
What This Package Will Give You

- **Website Integration**: Access to your Actuate report environment will not require an additional login as a user moves to it from your website.
- **Simpler User Administration**: Maintenance of user information (e.g., username, password, role) can be done from an external directory store (e.g., directory server, database) without being duplicated in the Actuate environment.
- **Knowledge Transfer**: Familiarity with key components and capabilities of Actuate products, as well as an understanding of best practices in planning, design and implementation of successful information delivery solutions.

Getting Started

Prior to the start of the Actuate Professional Services Security Integration Package engagement, the Actuate Sales Team will work with you to identify your security integration requirements and to document the information summarized below. This information will allow the Actuate Professional Services Project Manager to select the appropriate resources to meet your needs.

- **Information Delivery Requirements**: Pertaining to any area of security (e.g., use of directory store, database, Actuate out-of-the-box Lightweight Directory Access Protocol [LDAP] configuration, customized LDAP configuration, etc.)
- **Infrastructure Profiles**: Hardware platforms, operating systems, database servers, application servers, LDAP configuration or database model, information technology standards and methodologies.
- **Project Resources**: Any internal resources that will be involved in the engagement such as Developers or Business Analysts and System, Database or Application Administrators

Typical Agenda

**Week 1: Project Start**

- **Introduction**
- **Confirm currently defined security requirements**
- **Discuss environment where security integration will be implemented**

**Analysis and Design**

- **Analyze the environment to define best approach to meet security requirements**
- **Identify the authentication approach (e.g., cookie authentication, NT authentication)**
- **Identify the authorization approach (e.g., out-of-the-box LDAP configuration, customized directory configuration)**
- **Generate a design document with approaches defined**
- **Review of the design document with customer**

**Development – Initial**

- **Develop framework for security deliverables**

**Week 2: Development - Authentication**

- **Configure development environment, if required**
- **Develop ReportCast Security Extension (RCSE) library, and/or ReportCastAgent Security Extension (RCASE) library**

**Development - Authorization**

- **Configure development environment, if required**
- **Develop Report Server Security Extension (RSSE) library using LDAP API's (RSSE is an optional DLL or shared library and requires the Advanced e.Reporting Server product)**

**Week 3: Further Development and Unit Testing**

- **Complete development of security deliverables**
- **Unit test authentication and authorization deliverables together**

**Week 4: System Test and Deployment**

- **System testing of authentication and authorization deliverables**
- **Develop deployment document for use during system installations**