TECHNICAL / SECURITY

Safeguarding JD Edwards EnterpriseOne

Advanced Security Techniques and Best Practices

By Alex Rodriguez, Premier Group

E1 Editor's Note: It just gets better and better. In this article, Alex Rodriguez writes about new security features in JDE, such as SSL over JDENET and Password Encryption and how to implement them. He then shares, based on years of experience, security best practices for the various servers and applications, including those pertaining to the newer features.

Introduction

JD Edwards EnterpriseOne has been maturing rapidly over the past decade and now includes several new advanced features to allow customers to further safeguard and secure their deployment. Implementation of additional security has become critical in today's hyper-connected world and is also required for many companies in order meet new and ever-changing security compliance requirements. Among the new features that will be reviewed here are SSL over JDENET and password encryption within configuration files. This article will also cover general security best practices for all aspects of EnterpriseOne and also include specific examples on how to configure and use some of the new features.

Typical Security Challenges

Over time, a typical JD Edwards EnterpriseOne environment can grow to a point where it can seem as complex as the anatomy of the human body. One of the key benefits of JD Edwards Configurable Network Computing (CNC) is that it gives system administrators the ability to mix and match servers running diverse operating system platforms. This ease of flexibility coupled with the wealth of third-party applications and tools available for JD Edwards EnterpriseOne can lead to an expansion of the architecture footprint. This larger footprint can lead to a much more complex environment to secure.

Before beginning the process of defining any security model, several key questions need to be answered:

- What are we trying to protect and how are we going to protect it?
- What are the threats and who is involved with them?
- What acts are allowable and which are not?
- How do we know if the policies and practices are clearly implemented and was it effective enough?

Once these questions are answered, then a plan can be created to provide for a secure and easy to use system. Security without a plan is a constant series of patchwork changes and headaches. Remember that proper security can make things simple! Too many options can make for user frustration and lack of focus and productivity.

Many times security is not considered a key part of an EnterpriseOne system; but rather it's an afterthought. My mission with this article will be to provide key insight on how to plan and develop security that will actually improve the overall functionality of the software, lead to more system stability, provide more audit information, assist with meeting compliance requirements and simply provide for better control and management of system resources.

SSL over JDENET

With the steady and never ending growth of connected systems comes the need to be able to secure sensitive traffic that is flowing between all systems, even those that are not exposed to the public Internet. Prior to the release of the January 2013 Oracle CPU (Critical Patch Update) – CVE-2012-1678 (Common Vulnerabilities and Exposures) there was no way to encrypt or secure data that was being passed between JD Edwards servers via the proprietary JDENET protocol. This vulnerability allows for potential unauthorized access to JD Edwards by an attacker using a network sniffer to retrieve user and password data. Given the ease of configuration of SSL over JDENET, I highly recommend enabling this feature within your EnterpriseOne environments to help mitigate this potential threat and also help to facilitate compliance requirements. The table below (Figure 1) lists the minimum Tools Release required for the various supported releases.

JD Edwards Release	Minimum Tools Release for SSL over JDENET
Xe/ERP8	24.2.1
8.10/8.11/8.12/9.0	8.98.4.11
9.0/9.1	9.1.2.1
9.2	9.2.0.0

Figure 1 – Support for SSL over JDENET

Quick Guide to Enable SSL over JDENET for Windows

1. Login to your JD Edwards Windows Enterprise Server and open a command prompt. Make sure to Run as Administrator.
2. Navigate to the path shown in Figure 2 and run the gencert.cmd program. **Note:** Your path may vary slightly depending on the drive letter and path you chose during the installation process.