Securing iDashboards

IMPORTANT: The following is a standard best practices document designed to addresses the various areas associated with securing any web related software application. It should be noted that while this document addresses many major areas as they relate to securing the iDashboards product, these steps are best practices and should be followed for any web based product. All statements made by this document are provided purely as recommendations, iDashboards will not be responsible for implementation associated with any of the following.

- **Infrastructure**
  - Physical Security
    - Adequate physical security, where possible, should be implemented. This should include but is not limited to the use of demilitarized zone (DMZ) networks, VLANs, as well as firewall rules limiting communication to only those ports and source/destination addresses which are required for operation.
    - Gateway Security: Proper physical gateway security devices should also be in place. Adequate security should include Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), intent based protection services (prevention of things like denial of service attacks, packet sniffing, port scanning, etc.), data loss prevention (DLP), antivirus/anti-spam/anti-spyware security controls with properly updated signatures, as well as virtual private network (VPN) availability. There are many devices available as all-in-one units and are commonly referred to as Unified Threat Mangaement (UTM) devices.
    - If access to iDashboards via the internet is available VPNs should be in place where possible to ensure a secure channel of communication, in addition, to further fortify this channel, SSL certificates should be in place to secure the HTTP traffic.
  - Access Control
    - Access Control Lists (ACLs) should be in place to safeguard access to the iDashboards environment. These ACLs will control by rule those that can access the application and deny all others. In addition implicit deny rules can be put in place as well to deny access.
    - A decision should be made as to whether or not the iDashboards application will be hosted in an environment which supports *intranet* access, *internet* access or both. Intranet only access inherently comes with more security as the application is not available to the internet at large. If access is required via the internet, additiontal steps should be taken to further secure the environment (outlined here).

- **Communications**
  - iDashboards runs in a J2EE compliant application server which is capable of being run on a secured port (typically 443), also known as HTTPS, and requires the use of an SSL certificate. Restricting access to HTTPS will prevent any information from being sent in plain/clear text and in all cases of deployment iDashboards should be secured using this

method. This will require the generation of a certificate from a certificate authority (CA). Examples of these CAs include Comodo, Symantec (formarly Verisign), and Go Daddy.
    - In addition, all J2EE application servers support filtering or "access lists". These access lists can be implemented much like those in a firewall to control exactly what that application server is allowed to communicate with as well as explicitly what it cannot communicate with.

- **Authentication**
    - iDashboards supports external authentication and has a module based on the Lightweight Directory Access Protocol (LDAP). To further leverage existing infrastructures as well as leverage password policies already in existence iDashboards highly recommends that LDAP be used. The most common example of the LDAP technology is Microsoft's Active Directory, however Novell's eDirectory and many other applications leverage this technology as well.
    - By default, much like standard HTTP traffic, LDAP communication is not secured. Certificate authorities, mentioned above, can generate certificates to allow communication using the LDAPS protocol as well which, just like HTTPS, creates a secured channel of communication so that nothing is sent in plain/clear text. iDashboards also recommends that this be implemented in any environment to further secure the information being transmitted back and forth by the application so that security credentials cannont be compromised.
    - Most implementations of Microsoft's Active Directory allow just about anyone or anything to "browse" the directory. In other words, logon is not required to browse. Changes cannot be made, however, this can still be considered a security vulnerability as access to view is still granted. In addition to securing the physical machine where iDashboards is located, the utmost precautions should be taken with all other physical machines that can or will be communicating with iDashbaords at the infrastructure level to safeguard the entire environment.

- **Java/Flash/Tomcat**
    - As is the case with all software code bases, vulnerabilities do and will contintue to always exist. It is highly recommended that the latest versions always be analyzed and run and that an update policy be in place to regularly evaluate/update ALL machines running these. Although keeping up to date on patches and bug fixes will never guarantee against attack, as "zero day threats" will always exist in any code base, putting together proper policies and procedures to keep these applications update to date to prevent their codebases from being leveraged against its users will minimize these threats.
- **iDashboards Application and Communication Auditing**
    - iDashboards logs all application and communication activity and provides a dashboard solution. This will allow administrators access to that aggregated information so that should the system become compromised a formal audit can take place. This solution can also be used to simply monitor activity in the application as well.