DATA SECURITY FOR HP WEB JETADMIN

CONTENTS

INTRODUCTION

HP Web Jetadmin uses different techniques to make sure that the sensitive data it handles cannot be compromised. This white paper explains how HP Web Jetadmin treats data.

CLIENT DOWNLOAD AND CLIENT COMMUNICATION INITIATED OVER HTTP

HP Web Jetadmin uses the Microsoft® ClickOnce Smart Client technology. This technology runs a Microsoft .NET Framework application by automatically downloading and launching the application through a web browser. The Smart Client application runs as a local .NET Framework application on the host and communicates with the HP Web Jetadmin service via .NET Remoting. After the Smart Client application launches, the web browser is no longer required. Although HP Web Jetadmin also uses the web browser to deliver online Help and proactive Product Update notifications, the HP Web Jetadmin client application runs locally on the computer. The default HTTP port is 8000. The default HTTPS port is 8443. The client installer software comprises the client desktop Internet Explorer (IE) browser and client software or files that are distributed via an HTTP or HTTPS channel on the HP Web Jetadmin server application. The user experience is very simple and consists of the following steps:

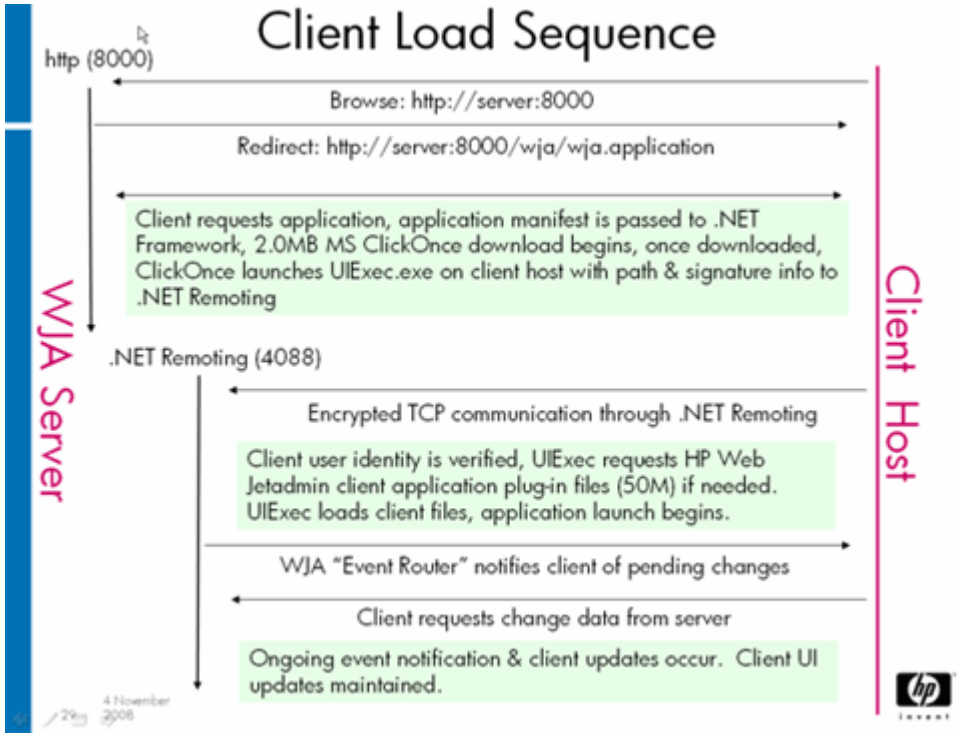
1. A user opens IE and browses to the HP Web Jetadmin URL (example: http://servername:8000 or https://servername:8443).
2. An initial .NET installation is started along with an installation manifest from the server.
3. The client application core (UIExec.exe) is started through a secure .NET communication path known as .NET Remoting. The .NET Remoting application governs the encryption method.
4. Files are downloaded from the client if needed (about 50 MB). The remainder of the application is loaded and displays the credentials UI or the initial HP Web Jetadmin screen if the single sign on was successful.

Note HP Web Jetadmin uses NTLM authentication during the client log-on process for the single sign on.

If the user is not found in the HP Web Jetadmin database, a screen displays asking for the user credentials.

Note The client software is always the same version as the HP Web Jetadmin server application. Each time the server application is updated to a newer version, the client is also updated and a new set of files are downloaded. The client application is downloaded to the user's home directory in an area known as the Click Once cache. Administrator rights are not required to install the client application.

The following illustration shows the client load sequence.



Note The HP Web Jetadmin online Help is transferred via a web browser session (HTTP or HTTPS), not via .NET Remoting.

CLIENT DOWNLOAD AND CLIENT COMMUNICATION INITIATED OVER HTTPS

Because some environments require server authentication through the more secure HTTPS protocol rather than HTTP, the Administrator can use HP Web Jetadmin to sign a request for an HP Web Jetadmin certificate for the purposes of HTTPS communication when the client browser opens the HP Web Jetadmin server address. In this case, the product generates a public/private key pair as part of the certificate request. After a third party signs this request, the certificate can then be installed in HP Web Jetadmin to allow communication with the HP Web Jetadmin server over HTTPS.

The certificate also reduces intrusions and middle-man attacks. A certificate can be added to HP Web Jetadmin to enforce only HTTPS transactions. The following are a few points about certificates:

- Certificates are added after HP Web Jetadmin is installed by going to **Tools** > **Options** > **Application Management**.
- HP Web Jetadmin does not self-generate certificates. A certificate must be signed by a CA after a certificate signing is requested in HP Web Jetadmin.
- Certificates can be added only via a client that runs locally on the HP Web Jetadmin server.
- When navigating to HP Web Jetadmin after installing a certificate, the hostname of the HP Web Jetadmin server is used in the URL to prevent certificate warning errors in the web browser. Because the original certificate signing request contains the hostname, the final installed certificate also contains the hostname inside the certificate.

COMMUNICATION BETWEEN THE HP WEB JETADMIN CLIENT AND SERVER

HP Web Jetadmin uses .NET Remoting for communication between the HP Web Jetadmin client and server. This communication uses port 4088 with the protection level set to EncryptAndSign.

Client event routing between the HP Web Jetadmin client and server

This section describes the event routing interactions that facilitate display accuracy.

Event routing is a term used to describe the mechanism that updates the HP Web Jetadmin client whenever the server has new information to share. For instance, Joe runs a different client than Raul. Joe just added four device groups and ran a discovery that captured 1,000 new devices. Raul can detect this new information through the client display because the HP Web Jetadmin server notifies his client that updated information is available. When the client receives this notification, the client uses the .NET Remoting channel to retrieve the updated information. The update notification, however, comes via a different channel known as Client Event Routing. Client Event Routing uses a static port (4089). This port is configured in the Global.config.xml file. This file is located in the following directory:

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\HP Inc\HPWebJetadmin\WjaService\config

DATA IN TRANSIT BETWEEN THE HP WEB JETADMIN SERVER AND A REMOTE SQL SERVER DATABASE

By default, HP Web Jetadmin uses port 1433 for communication to the remote Microsoft SQL Server database via .NET Remoting.

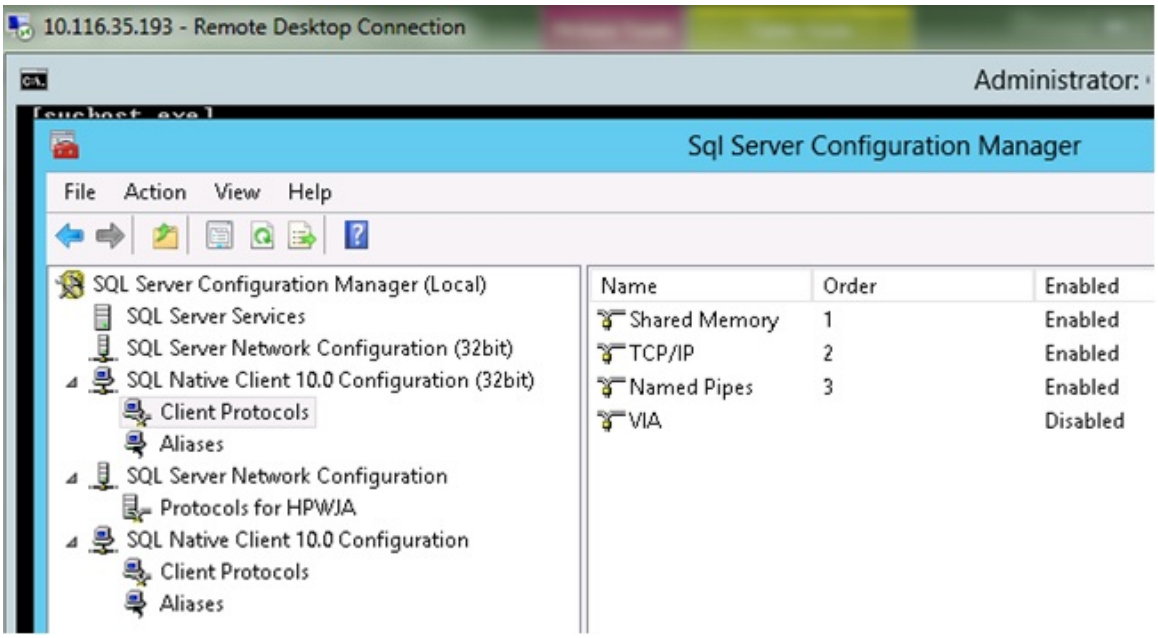
Note The port number can be configured. For more information, see the *Using Microsoft SQL Server with HP Web Jetadmin* white paper. This white paper is available from the HP Web Jetadmin support page (EN only).

HP Web Jetadmin encrypts all the sensitive data that it sends. For username/password protection to encrypt and decrypt data for the database, HP Web Jetadmin uses the Microsoft Data Protection API (DPAPI). Specifically, CryptProtectData() and CryptUnprotectData() are called. The actual encryption code called is provided as part of the Microsoft operating system.

DATA IN TRANSIT BETWEEN THE HP WEB JETADMIN SERVER AND THE LOCAL SQL SERVER DATABASE

Data transmission between the HP Web Jetadmin server and the local SQL Server database is the same as data transmission between the HP Web Jetadmin server and a remote SQL Server database.

However, because the SQL Server database is local, the communication to the database might be changed to use only Shared Memory as shown in the following example.



DATA AT REST IN THE SQL SERVER DATABASE (STORED DATA)

All sensitive data is stored encrypted. For username/password protection to encrypt and decrypt data for the database, HP Web Jetadmin uses the Microsoft Data Protection API (DPAPI). Specifically, CryptProtectData() and CryptUnprotectData() are called. The actual encryption code called is provided as part of the Microsoft operating system. For more information, see the *Windows Data Protection* article. This article is available from the Microsoft Developer Network.

WARNING! When you change the account for the HP Web Jetadmin service, HP Web Jetadmin can no longer decrypt the sensitive data that was stored in the SQL Server database before you changed the account for the HP Web Jetadmin service.

DATA IN TRANSIT BETWEEN THE HP WEB JETADMIN SERVER AND THE DEVICE

HP Web Jetadmin uses different protocols to communicate with the devices. Depending on the device, device firmware, and configuration settings, HP Web Jetadmin uses one of the following protocols:

- SNMPv1/SNMPv2 or SNMPv3
- Web Services
- PJL
- XDM
- DSMP
- LEDM

SNMPv1/SNMPv2 or SNMPv3

HP Web Jetadmin can use SNMPv1/SNMPv2, which is unencrypted, or SNMPv3. For encrypting over SNMPv3, HP Web Jetadmin supports AES-128 and DES for the Privacy Protocol and supports MD5 and SHA-1 for the Authentication Protocol.

Web Services

HP Web Jetadmin uses Web Services, which is a SOAP-based protocol, especially with HP FutureSmart devices.

This communication uses port 7627. HP Web Jetadmin communicates over HTTPS to ensure that all the data is encrypted during the transmission. HP Web Jetadmin is dependent on .NET Remoting for this communication. To encrypt and decrypt the data, .NET Remoting uses a symmetric key that is generated during the handshake operation between HP Web Jetadmin and the device.

Even if no password is set on an HP FutureSmart device, HP Web Jetadmin uses Web Services over HTTPS.

PJL

HP Web Jetadmin can use PJL for some disk operation, such as macro and font installation, and for firmware upgrades. This communication goes over port 9100.

Note HP Web Jetadmin uses the Web Services protocol for firmware upgrades on HP FutureSmart devices.

XDMP

XDMP is an HP-proprietary protocol. HP Web Jetadmin uses XDM during the IPsec configuration.

DSMP

DSMP is a proprietary protocol that HP Web Jetadmin uses for some configuration options in the Digital Sending category for legacy HP Enterprise printers. DSMP is sent over HTTP.

LEDM

For the configuration of some non-HP FutureSmart devices, HP Web Jetadmin uses Low-end Data Model (LEDM). LEDM is based on the Representational State Transfer (REST) style architecture, which is a design that describes a simple interface for transmitting XML data over HTTP or HTTPS without an additional messaging layer. This configuration is done over HTTP or HTTPS depending on the device configuration and device firmware. Because HTTP traffic is unencrypted and unsecure, HP recommends enforcing HTTPS communication on the device.

Note Setting the administrator password on the devices that allow HTTP traffic prevents unauthorized access. However, the communication continues over HTTP unless HTTPS redirection is enforced on the device.

PRODUCT INTEGRITY PROTECTION

HP Web Jetadmin uses the Windows .NET Strong Naming capability. This feature allows the signing of assemblies that are part of the product. This prevents someone from replacing product assemblies with rogue assemblies that can impersonate existing assemblies and harm the customer's interests.

c04894262EN, Rev. 2, April 2016