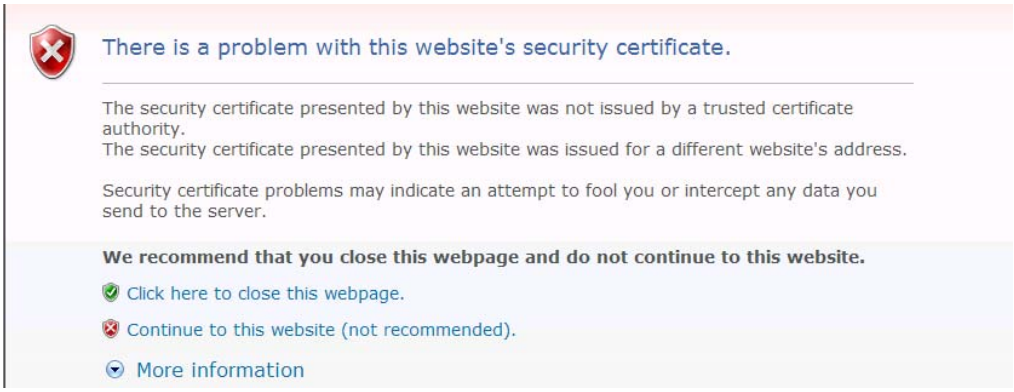
whitepaper

Security warnings when browsing to JetDirect Print Servers

May 2011 (revised June 2011)

Security warnings when browsing to JetDirect Print Servers



A user browsing to an HP JetDirect print server on a Laserjet printer or MFP will encounter a warning that the website cannot be trusted. Microsoft Internet Explorer will give a warning that, "**There is a problem with this website's security certificate**", while Mozilla Firefox reports that, "**This Connection is Untrusted**". Other browsers will give similar warnings. When browsing to JetDirect print servers, these warnings indicate that though the exchanges with the Laserjet printer are secure, the browser cannot identify it as a trusted web server. *Unless the printer has been specifically configured with an identity certificate signed by a certificate authority, these warnings **can** be safely ignored.*

When browsing to a public or commercial website, such warnings indicate that the browser cannot adequately validate the identity of the web site based on the security credentials (i.e. the identity certificate) it presents. *In commercial or public settings (i.e. browsing to commercial or public web sites), these warnings should **not** be ignored.*

Any web site, whether a public/commercial site or the web server of an HP Laserjet printer or MFP, uses the HTTPS protocol to secure the exchanges with the browser. The HTTPS protocol provides two protections: confidentiality, i.e. preventing eavesdropping between the browser and web site, and authenticity of the web site. Exchanges over the HTTPS protocol, whether in the HP Laserjet web server or any public web server, will always be encrypted assuring their confidentiality. However, the

authenticity of the web site depends on verifying a "chain of trust" between the browser and server; the failure of the chain of trust results in the warnings.

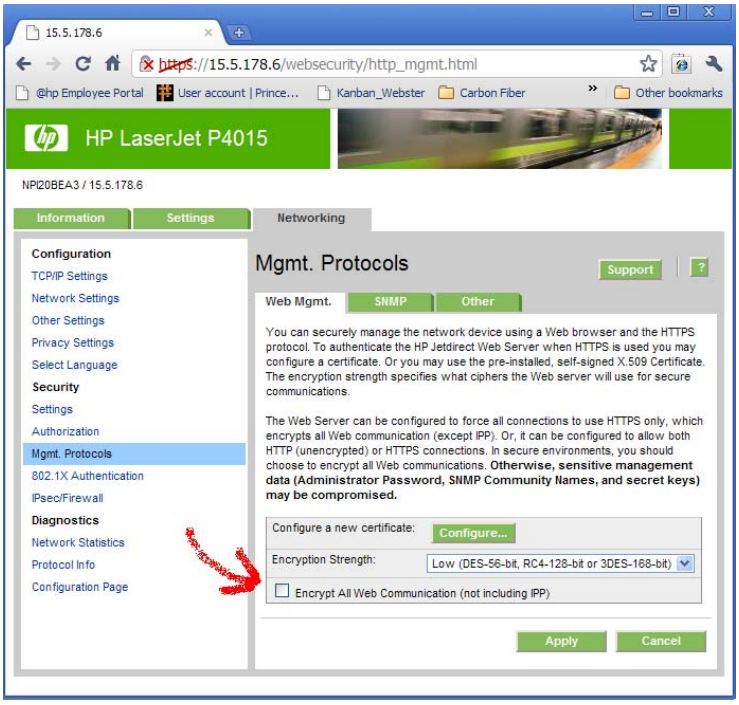
The chain of trust between the browser and the web server is established by linking the identity *certificate* from the web server to a *Certificate Authority* (CA) certificate that is installed in the browser. Commercial and public web sites will purchase and install an identity certificate from a well-known Certificate Authority such as Thawte, Verisign, Entrust etc; the issuing CA essentially makes a statement, with the certificate, that the web site is genuine. Browsers are configured by default to trust the well-known CAs and thus can establish the validity of the identity certificates presented by the web servers.

An HP Laserjet cannot, by default, present credentials as robust as the identity certificates presented by a public or commercial web site. First it is a matter of scale: the logistics and expense of providing robust (signed by well-known CA) identity certificates for hundreds of thousands of devices is prohibitive. Secondly, it is a matter of configuration: since the identity of an HP Laserjet is determined by the user at installation, a certificate cannot be issued until after installation and configuration.

HP Laserjet printers and MFPs, nevertheless, assure the best possible security given these constraints by creating a default *self-signed* certificate which assures confidentiality but does not robustly provide authenticity. (A *self-signed* certificate, rather than issued by a CA, is issued by the device itself, and thus cannot establish a chain of trust to a well-known CA.)

If desired, an HP Laserjet can be configured to provide both robust confidentiality and authenticity by purchasing and installing an identity certificate from a well-known CA. The HP Laserjet will generate a *Certificate Signing Request* (or equivalently, *Certificate Request*) that is submitted, along with supporting identity documentation, to the CA which will return a signed certificate to be installed in the HP Laserjet. This process is detailed on pages 88ff. of the JetDirect Administrator's Guide (http://h20000.www2.hp.com/bc/docs/support/SupportManual/c01502097/c01502097.pdf).

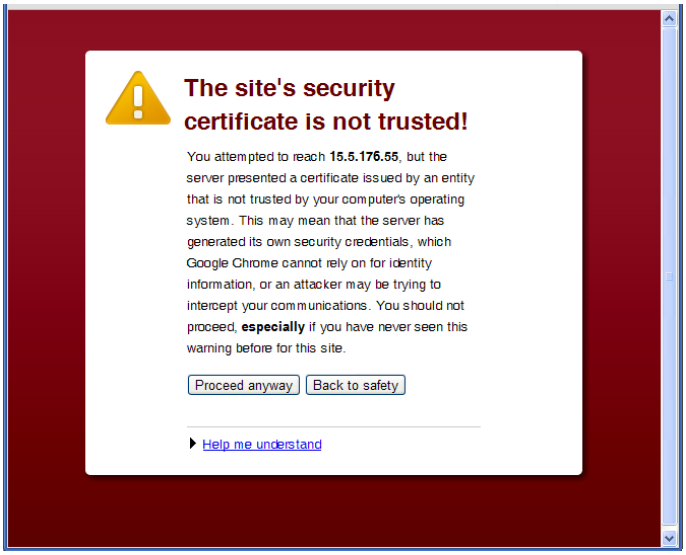
Alternatively, if security is not required, secure web communications can be disabled on the **Mgmt Protocols** page of the JetDirect print server by unchecking the checkbox:



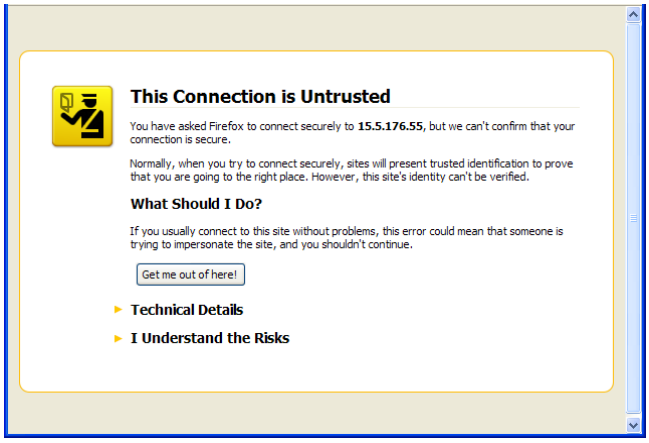
*HP does **not** recommend disabling (unchecking) this feature.*

Appendix: Warnings from other browsers

Google Chrome:



Mozilla Firefox:



Microsoft Internet Explorer version 6 (IE6) launches a dialog box: