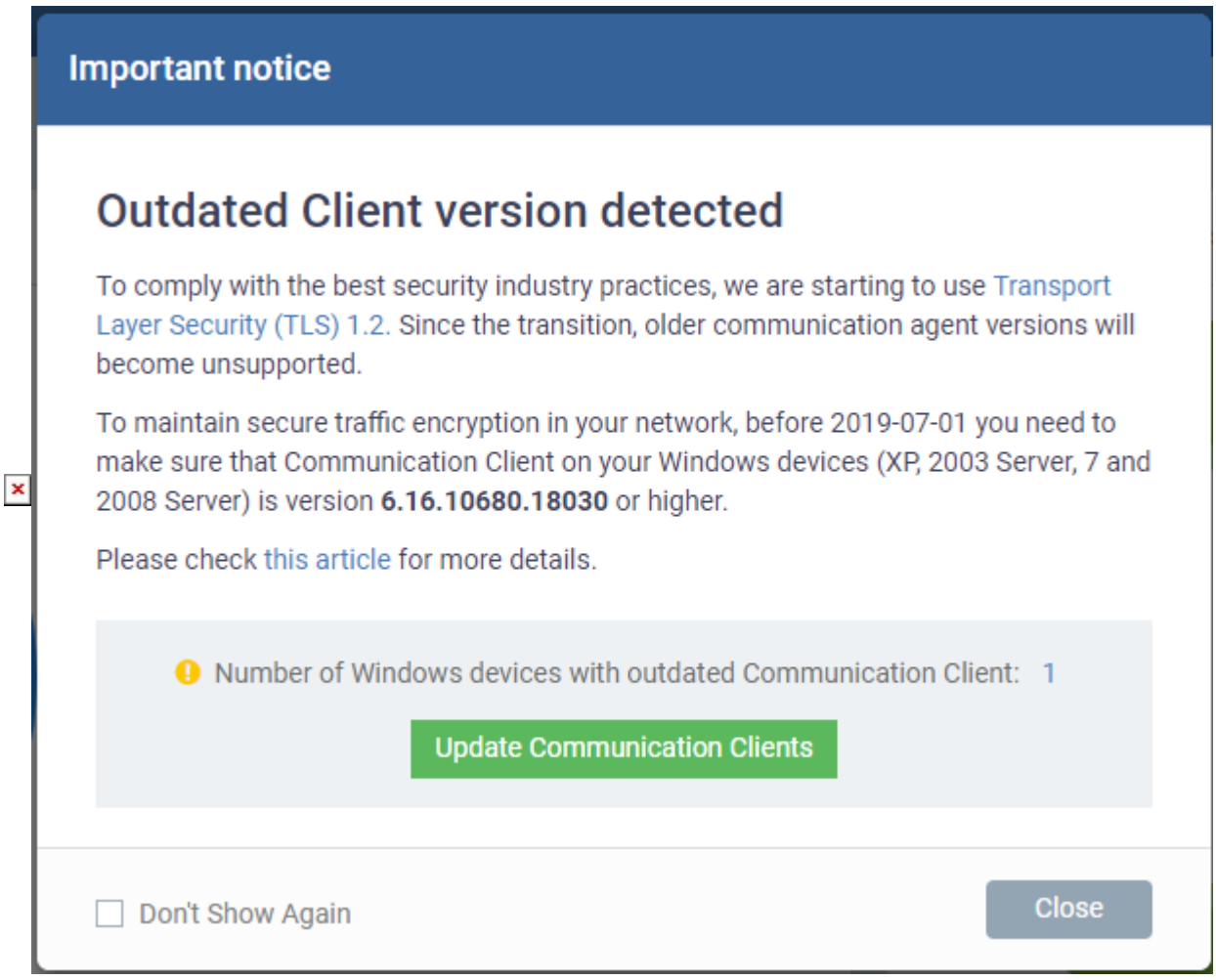
# Notification. We are upgrading the Communication Client to use TLS 1.2

To comply with sector-leading security practices, we are upgrading the protocol used in our communication client (CC) to Transport Layer Security (TLS) 1.2. Industry standards bodies such as the Payment Card Industry (PCI) council recommend TLS 1.2 is used for secure communications.

**What action do I need to take?**

- Devices which have automatic updates enabled in a profile will seamlessly receive the client upgrade on or near February 16th 2019.

- We will also show an upgrade prompt in Endpoint Manager if we detect outdated clients. Users should click the upgrade button to install the latest client:




- To maintain secure traffic encryption in your network, by 2019-07-01 you need to make sure that Communication Client on your Windows devices (XP, 2003 Server, 7 and 2008 Server) is version 6.16.10680.18030 or higher, in order to be compatible with Transport Layer Security (TLS) v.1.2 protocol.

**What is Transport Layer Security (TLS)?**

Transport Layer Security (TLS) is a protocol that encrypts the connection between communicating applications over the internet. When a server and a client communicate, TLS ensures that no third party can intercept the communication and steal the data passed between the two.

For example, it is TLS that secures the connection between your computer and a website order-form when you make an online purchase. Similarly, it is TLS that secures the connection between our client on a managed device and the Endpoint Manager server.

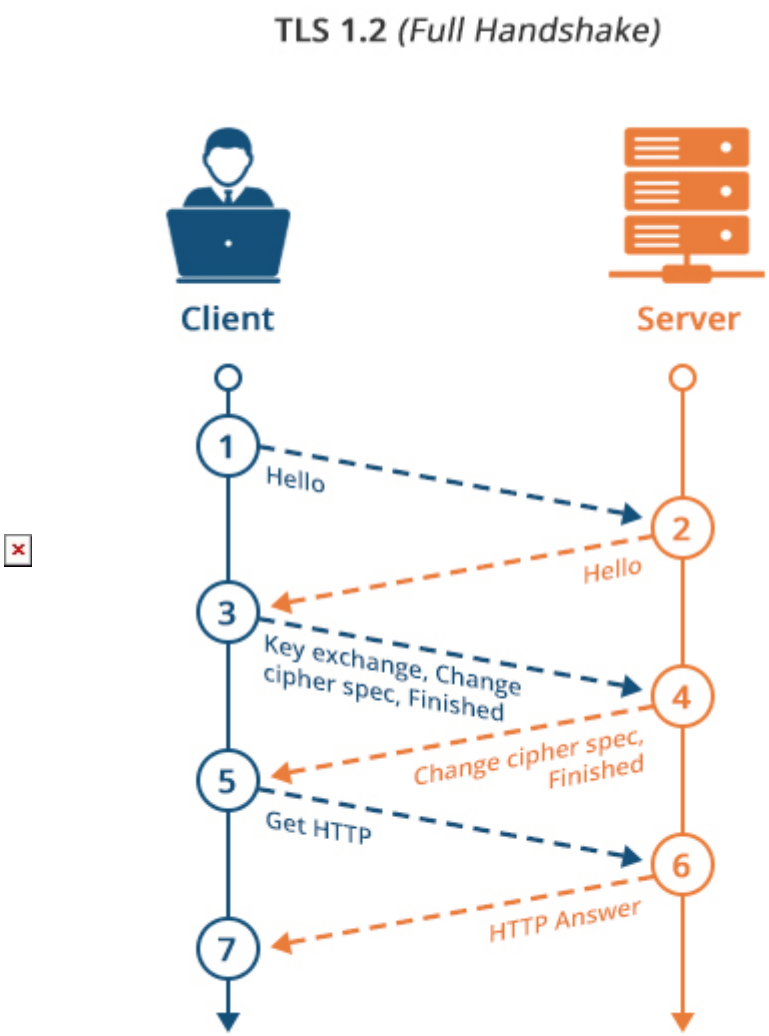
**Why is this upgrade needed?**

Because earlier versions of TLS contain security vulnerabilities for which there are no known fixes. The widespread POODLE and BEAST exploits are a couple of examples of how attackers have taken advantage of weaknesses in SSL and early TLS. While both exploits are more theoretical than practical for an attacker, and Comodo systems have always had multiple layers of security in place to prevent this attack anyway, we are still implementing the upgrade as best practice.

**Why is TLS 1.2 better?**

TLS 1.2 contains several security and flexibility improvements over earlier versions of TLS. Major differences include:

- The MD5/SHA-1 combination in the pseudorandom function (PRF) was replaced with cipher-suite-specified PRFs.
- The MD5/SHA-1 combination in the digitally-signed element was replaced with a single hash. Signed elements include a field explicitly specifying the hash algorithm used.
- There was substantial cleanup to the client's and server's ability to specify which hash and signature algorithms they will accept.
- Addition of support for authenticated encryption with additional data modes.
- TLS Extensions definition and AES Cipher Suites were merged in.
- Tighter checking of EncryptedPreMasterSecret version numbers.
- Many of the requirements were tightened.
- Verify_data length depends on the cipher suite.


TLS 1.2 (Full Handshake)
Client
Server
1
Hello
2
Hello
3
Key exchange, Change cipher spec, Finished
4
Change cipher spec, Finished
5
Get HTTP
6
HTTP Answer
7