Tachyon Quarantine

Summary

A description of the quarantine feature provided in the Tachyon Agent and implemented in the quarantine instructions present in the 1E-Explorer-TachyonCore.zip file.

On this page:

What is Quarantine?

On Windows, the Tachyon Agent is able to prevent communications to or from a target device. This is intended to be reserved for security breaches and other rare circumstances.

What will it do?

Quarantine will prevent all communications except those to the Tachyon server(s). This allows a Tachyon administrator to investigate and remove possible malicious software on the device.

> Devices that have been quarantined will only be able to contact Tachyon. CRL checks must be set to soft. Certificate expiry can cause the agent to fail to connect to the switch. If an agent is no longer connected to Tachyon after quarantine, it will remain in quarantine. Please use with care, and please read this documentation carefully before use.
>
> It is possible to quarantine Tachyon Server like any other device therefore please exercise caution before using this feature.

How do I quarantine a device?

You either need to load the **1E-Explorer-TachyonCore.zip** file into Tachyon or download the quarantine product pack from the Tachyon Exchange and then define an Instruction set for the instructions. We recommend that you create an instruction set specifically for the quarantine instructions and permission this separately, for that you'll need to define a custom role and assign at least one management group to the role, for more details please refer to Instruction sets, Tachyon Exchange and custom roles - tutorial. The quarantine instructions are described in the following table:

Instruction	Description
Are my devices quarantined? Warning: Please read the description before use.	This question returns a list of devices.
Quarantine selected devices. Warning: Please read the description before use.	This action quarantines all the devices in the scope of the action. Do not run this action without restricting the coverage to the devices you want to quarantine.
Release selected devices from quarantine. Warning: Please read the description before use.	This action releases all the devices in the scope of the action from quarantine.

As you can see there is a warning attached to the name of each instruction. Quarantine is a powerful solution for use in extreme circumstances and should be used with care. We therefore recommend that Actioner permissions associated with the instruction set defined to contain the quarantine instructions should be assigned only to specific users. Users with Actioner permissions to use the quarantine instructions should also be warned that the instructions must be used carefully.

What do I need to know before I quarantine a device?

- Quarantine is available only on Windows, but not available on Windows XP.
- Quarantine requires that at least one switch URI and one background channel URI each resolve to IPv4 addresses.
- Quarantine will only work if a device's connection to the switch is over IPv4. This is because IPv6 is disabled by the quarantine mechanism.
- The **CRLChecks** setting in the agent configuration file should be set to soft.
  - As the device will be unable to contact anything but the tachyon server(s), the agent will be unable to retrieve CRLs for certificates requiring validation.
  - **CRLChecks** can be set to hard, but this can cause the agent to lose connection to the switch when the CRL validity period is exceeded.
- Quarantine will persist until the **Release selected devices from quarantine** instruction is received.
  - If an agent cannot be connect to the Tachyon Server, it will not be possible to issue this command.
- Any changes to the routing tables, IPv6 bindings or the hosts file made during quarantine will be reverted when the **Release selected devices from quarantine** instruction is received.
- If the persistent storage of the agent is deleted or modified by anything other than Tachyon whilst in quarantine, the agent will not be able to release the device from quarantine properly.
- Upgrading, uninstalling, installing or modifying the Tachyon agent installation during quarantine is not supported. Do not upgrade, uninstall or install Tachyon, or issue an extensibility update whilst the agent is under quarantine.
- After a release from quarantine the IPv4 loopback address will not be resolvable. A restart is required to fix this.

- Quarantining a device will also stop it from being able to see Domain Controllers, so this may cause problems with logging on to the workstation. Cached logons should still work though.