Device Criticality and Status

Summary

Device Criticality and how it relates to Guaranteed State and Device Status

Device Criticality

You will notice that the **Overview** screen makes reference to **Criticality** in various views. By default, the value of device criticality is set to **Undefin ed**. Device criticality is intended as a mechanism for classifying endpoints into degrees of criticality, or importance. For example, endpoints which support mission-critical functionality within an organisation can be classified appropriately. This allows you to manage devices based on criteria you define, associated with their criticality.

Device criticality is an attribute of a device that defines its importance within an organisation. As defined by default in Tachyon, criticality has the following default settings

- Undefined (or not set).
- Non-critical
- Low
- Medium
- High
- Critical

At present, device criticality is not directly used by Guaranteed State, though you can define it and view it.

Tachyon also supports the use of the criticality setting when defining coverage for an instruction. For example, you can choose to target an instruction to be sent only to devices whose criticality is set to any state except **Critical**.

Setting Device Criticality

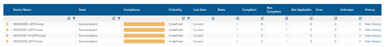
Device criticality is set using the instruction **1E-Explorer-TachyonAgent-SetCriticality** to set device criticality.

From the Tachyon Explorer, enter: **Set the criticality of my devices**.

Select the instruction and then choose the desired criticality from the dropdown.

Select the coverage for the instruction. Then submit it. After approval, devices which match the specified coverage value will have their criticality set to the specified value.

Device Status



	Device Name	State	Compliance	Criticality	Last Seen	Rules	Compliant	Non Compliant	Not Applicable	Error	Unknown	History
●	WKSHM001.URTH.local	Noncompliant	▬	Undefined	Current	1	0	1	0	0	0	View History
●	WKSSC001.URTH.local	Noncompliant	▬	Undefined	Current	1	0	1	0	0	0	View History
●	WKSSC001T4.URTH.local	Noncompliant	▬	Undefined	Current	1	0	1	0	0	0	View History
●	WKSSV002.URTH.local	Noncompliant	▬	Undefined	Current	1	0	1	0	0	0	View History

The device status view in Guaranteed State shows the status of policies and rules for each device.

A device is shown as either **Compliant** or **Noncompliant**. The associated columns show more information on the status of rules on the endpoint.

- The **Rules** column shows the number of rules which are active for the device. If there are several active policies applicable to the device, the rules count will be the sum of all the distinct rules associated with those policies. (i.e, if the same rule is included in two active policies against the device, the count of distinct rules is 1).
- The **Compliant** column shows the number of rules which returned a compliance status of success (specifically each rule which returned a boolean value of **True** when the rules were last evaluated)
- The **Non-compliant** column shows the number of rules which returned a compliance status of failure (specifically each rule which returned a boolean value of **False** when the rules were last evaluated)
- The **Not applicable** column shows the number of rules for which the precondition for the rule meant that for this device, the rule was not regarded as applicable and hence was not evaluated.
- The **Error** column shows the number of rules for which an error was raised during the execution of the rule. This means that the SCALE code associated with the rule failed with an error that caused the code to be terminated, or that the code deliberately raised an error using the SCALE Error function.
- The **Unknown** column shows the number of rules for which no status has yet been returned from the endpoint.