# Implementing TLP 2.0 in STIX 2.1

## Some Caveats

* Versioning cannot be used because marking-definitions cannot be versioned.
* The new TLP 2.0 objects could be specific objects, like the ones in the spec for TLP 1.0 – i.e., there would never be a need to create your own TLP 2.0 data marking object – just use the STIX TLP 2.0 id.

## **Option 1**: Create new TLP objects using Extension Definitions

{

"id": "extension-definition--60a3c5c5-0d10-413e-aab3-9e08dde9e88d",

"type": "extension-definition",

"spec\_version": "2.1",

"name": "TLP 2.0",

"description": "This defines TLP 2.0 as a STIX extension",

"created": "2022-10-01T00:00:00.000Z",

"modified": "2022-10-01T00:00:00.000Z",

"created\_by\_ref": "identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01",

"schema": "https://github.com/oasis-open/cti-stix-common-objects/tree/master/extension-definition-specifications/tlp-2.0",

"version": "1.0.0",

"extension\_types": [

"property-extension"

]

}

{

"type": "marking-definition",

"spec\_version": "2.1",

"id": "marking-definition--94868c89-83c2-464b-929b-a1a8aa3c8487",

"created": "2022-10-01T00:00:00.000Z",

"name": "TLP:CLEAR",

"extensions": {

 "extension-definition--60a3c5c5-0d10-413e-aab3-9e08dde9e88d": {

 "extension\_type": "property-extension",

 "tlp\_2\_0"[[1]](#footnote-1): "clear"

 }

 }

}

TLP:GREEN, TLP:AMBER, TLP:AMBER+STRICT, TLP:RED are similar

Notice that this marking-definition's id is not the same as corresponding TLP 1.0 object, as defined in the specification. It might be desirable to generate a relationship object relating the TLP 1.0 object to the TLP 2.0 object. See option 2 for an example of the relationship object.

The TLP 1.0 marking definitions objects could still be referred to using the ids defined in the STIX 2.1 specification.

## **Option 2**: Create new TLP objects using deprecated properties, with relationships to existing TLP objects

The description in the spec for definition\_type says, "Any new marking definitions **SHOULD** be specified using the extension facility described in section 7.3." Additionally, the definition and definition\_type properties are deprecated. This is inconsistent because there is no way to express tlp-1.0 or statement marking-definition objects in a future release that isn't deprecated. This might be a reason to not choose this option.

TLP:WHITE

Original TLP:WHITE

{

"type": "marking-definition",

"spec\_version": "2.1",

"id": "marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9",

"created": "2017-01-20T00:00:00.000Z",

"definition\_type": "tlp",

"name": "TLP:WHITE",

"definition": {

"tlp": "white”

 }

}

TLP 2.0 TLP:CLEAR

{

"type": "marking-definition",

"spec\_version": "2.1",

"id": "marking-definition--94868c89-83c2-464b-929b-a1a8aa3c8487",

"created": "2022-10-01T00:00:00.000Z",

"definition\_type": "tlp-2-0"[[2]](#footnote-2),

"name": "TLP:CLEAR",

"definition": {

"tlp\_2\_0": "clear”

 }

}

An SRO could be included to inform consumers of the relationships between TLP 1.0 and TLP 2.0 instances.

{

"type": "relationship",

"description": "relating TLP 1.0 WHITE to TLP 2.0 CLEAR"

"spec\_version": "2.1",

"id": " relationship-- b139a86c-f47c-48c6-920b-06142e525530",

"created": "2022-10-01T00:00:00.000Z",

"source\_ref": "marking-definition--94868c89-83c2-464b-929b-a1a8aa3c8487",

"target\_ref": "marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9",

"relationship\_type": "new-version-of"

}

TLP:GREEN (TLP:AMBER and TLP:RED are similar)

Original TLP:GREEN

{

"type": "marking-definition",

"spec\_version": "2.1",

"id": "marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da",

"created": "2017-01-20T00:00:00.000Z",

"definition\_type": "tlp",

"name": "TLP:GREEN",

"definition": {

"tlp": "green”

 }

}

TLP 2.0 TLP:GREEN

Note different id.

{

"type": "marking-definition",

"spec\_version": "2.1",

"id": "marking-definition--8147960c-b4e9-44bb-ac9b-3299f26b4fbb ",

"created": "2022-10-01T00:00:00.000Z",

"definition\_type": "tlp-2.0",

"name": "TLP:GREEN",

"definition": {

"tlp\_2\_0": "green”

 }

}

{

"type": "relationship",

"description": "relating TLP 1.0 GREEN to TLP 2.0 GREEN",

"spec\_version": "2.1",

"id": " relationship--3ba204bc-2cf1-457f-9a61-81ecd064aebe",

"created": "2022-10-01T00:00:00.000Z",

"source\_ref": "marking-definition--8147960c-b4e9-44bb-ac9b-3299f26b4fbb",

"target\_ref": "marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da",

"relationship\_type": "related-to"

}

TLP: AMBER+STRICT

No Original TLP:AMBER+STRICT

TLP 2.0 TLP:AMBER+STRICT

{

"type": "marking-definition",

"spec\_version": "2.1",

"id": "marking-definition--7bfbffc5-0874-4bd0-9922-42e293d07a04",

"created": "2022-10-01T00:00:00.000Z",

"definition\_type": "tlp-2.0",

"name": "TLP:AMBER+STRICT",

"definition": {

"tlp\_2\_0": "amber+strict”

 }

}

## Using Existing TLP 1.0 Instances in Future Releases

As mentioned in the previous section, because the definition and definition\_type properties will be deprecated in future versions, the TLP 1.0 marking definitions objects defined in the STIX 2.1 specification could not be expressed "as is" in a future release.

Therefore, the following object must remain in spec\_version 2.1:

{

"type": "marking-definition",

"spec\_version": "2.1",

"id": "marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9",

"created": "2017-01-20T00:00:00.000Z",

"definition\_type": "tlp",

"name": "TLP:WHITE",

"definition": {

"tlp": "white"

}

}

This id could still be referred to by other objects, regardless of their spec\_version as most TLP 1.0 objects are upwards compatible (acknowledging the name change from TLP:WHITE to TLP:CLEAR, and the addition of TLP:AMBER-STRICT), because they have no underlying properties. Additionally, there is no need to share any TLP 1.0 object, because it is defined in the specification.

Bundles can contain or refer to STIX objects from various spec\_versions, although this might not be a desirable solution.

1. According to section 3.1 of the spec, only underscores are allowed in a property name. [↑](#footnote-ref-1)
2. For consistency, it makes sense to use the string "tlp-2-0", because STIX string literals can only contain "-" (definition\_type is defined as an open-vocab – but there is no vocabulary for it in the spec). [↑](#footnote-ref-2)