

CREATING DATA MARKINGS

When creating a data policy, you can narrow the policy's scope to only include certain types of data. Data Markings are how you can distinguish which types of data to encrypt. Ionic provides two data markings: Classification and Ionic Detected Content. The Classification data marking applies to encrypted content in Microsoft Office Ionic Protected documents and the Ionic Detected Content data marking applies to Internet Explorer Ionic Protected content. At this time, the only data marking that can be applied to content in the Internet Explorer browser is the Ionic Detected Content data marking. If you create a new data marking, it can only be applied to Microsoft Office Ionic Protected documents. The documents must have the data marking applied for the data policy to be enforced.

BEFORE CREATING DATA MARKINGS

- Create an Application that enforces encryption in Microsoft Office documents.

To create a data marking

1. On the **Data Markings > Manage** tab, click the **+Create Data Marking** button.

NAME	DESCRIPTION	VALUES	DATA POLICIES	ACCESS	UPDATED
Classification	Classification	7	5 data policies reference this marking.	Visible	a month ago
Department	None	2	0 data policies reference this marking.	Hidden	a month ago
Filename	None	1	0 data policies reference this marking.	Hidden	a month ago

2. Enter a Name for your Data Marking in the text field provided.



The Data Marking Name is used to create the Data Policy and tag the Microsoft Word Ionic Protected Document.

3. Enter a Description for your Data Marking in the text field provided.

Create Data Marking

Name

Description

Default Value

Access
 Hidden Visible
 By selecting "Visible" Ionic-enabled applications can make this marking and its values available to their users when protecting content.

Admin Control
 Do not collect values provided by clients.
 When checked, the list of values for this marking can only be defined by administrators.

Create **Cancel**

4. [Optional] You can designate a value of a public data marking as the preferred default value to be used by an Ionic-enabled client to make the end-user experience easier, while also encouraging a standard classification on all protected data. For example, enter a **Default Value** of 'High'.
 - Only one value of a public data marking can be set as the default value
 - Setting a default value is not required
 -  The new Default Value will be generated and will display in the Values section of the Data Marking detail page.
 -  When you go back to update the Default Value, a drop-down menu will become available to select a value from the list. You can also clear the value by clicking the **x**.
5. Select either **Hidden** or **Visible** in the **Access** field to determine if the Data Marking will be visible or hidden to Ionic-enabled applications.
6. Click the **Create** button.
7. To view and access the policies that are referencing individual Data Markings, select a data marking, and click the link either to Relevant or Referenced Policies from the Data Marking **Values** table.

classification

NAME: classification
 DESCRIPTION: Classification
 CREATED: May 29, 2015, 12:48 pm (a year ago)
 UPDATED: Sep 06, 2016, 07:07 am (a day ago)
 COLLECTS CLIENT-DEFINED VALUES: Yes

Values History

Search 16 Values

NAME	DESCRIPTION	DATA POLICIES	Relevant	DATA PROTECTED Last 30 days	DATA ACCESSED Last 30 days
top secret	None	2 data policies will be applied. 1 data policy references this value.		0	
secret	None	2 data policies will be applied. 1 data policy references this value.	Referenced	0	
confidential	None	2 data policies will be applied. 1 data policy references this value.		0	
restricted	None	2 data policies will be applied. 1 data policy references this value.		2	

- To view previous versions of data markings, select a data marking, and click the **History** tab.

Policy Marking Update Order Delete

NAME: Policy Marking
 DESCRIPTION: None
 DEFAULT VALUE: None
 DATA POLICIES: 0 data policies reference this marking.
 CREATED: Jul 11, 2017 (9 days ago)
 UPDATED: Jul 11, 2017 (9 days ago)
 ACCESS: **HIDDEN**
 COLLECTS CLIENT-DEFINED VALUES: No
 VERSION: 2 of 2

Values History

Search Action All Add Search 2 records

ACTION	TIME	CHANGED BY	VERSION
UPDATED	Jul 11, 2017 (9 days ago)	John Doe	2
CREATED	Jul 11, 2017 (9 days ago)	Test User	1

- To view the Data Marking history details, hover your mouse over the Data Marking history record and click **Inspect**.

CREATING DATA MARKING VALUES

To use the Classification Data Marking or a newly created Data Marking, you must create values. Data Marking Values are groupings or categories of data. For instance, for the Classification data marking you might add a value of Restricted. Then you can set a data policy allowing only certain people access privileges to that document or any document with that data marking and value. You can also create Values while creating a Data Policy by entering a value in the text field provided. Furthermore, values can be created upon saving a Microsoft Ionic Protected Document in the Save As dialog.

The Ionic Detected Content data marking comes with five values: CCN (credit card number), ip-address-v4 (internet provider address), ip-address-v6 (IPv6 address), usa-federal-ssn (social security number – USA), and usa-federal-taxid (tax identification number – usa). These values are automatically detected in content entered into an Internet Explorer browser and be encrypted if encryption is being enforced through Application Policy.

BEFORE CREATING VALUES

- Create an Application that enforces encryption.

To create a value

1. On the **Data Markings > Manage** tab, select a data marking.

<input type="checkbox"/>	NAME	DESCRIPTION	VALUES	DEFAULT VALUE	DATA POLICIES	ACCESS	UPDATED
<input type="checkbox"/>	Classification	Classification 1	3	None	0 data policies reference this marking.	HIDDEN	16 days ago
<input type="checkbox"/>	Department	xxxxxx	6	User Dashboard	1 data policy references this marking.	VISIBLE	a month ago
<input type="checkbox"/>	Test	Test 1	1	None	0 data policies reference this marking.	VISIBLE	16 days ago
<input type="checkbox"/>	Chrome 1	Fake	1	Fake 1234	0 data policies reference this marking.	HIDDEN	a month ago

2. Click the **+Create Data Marking Value** button.

Classification Update

NAME: Classification

DESCRIPTION: Classification

DATA POLICIES: [5 data policies reference this marking.](#)

CREATED: Aug 26, 2015, 05:35 pm (a year ago)

UPDATED: Nov 07, 2016, 03:00 pm (2 months ago)

ACCESS: Visible

COLLECTS CLIENT-DEFINED VALUES: Yes

Values History ➔ + Create Data Marking Value Order Values

Search by Name Search - Add Search 7 values

NAME	DESCRIPTION	DATA POLICIES	DATA PROTECTED Last 30 days	DATA ACCESSED Last 30 days
------	-------------	---------------	--------------------------------	-------------------------------

3. Enter a Name for the Value.
 - i Name is a required category.
4. [Optional] Enter a Description for the Value.

Create Data Marking Value

Name

Description

[Order Values](#)

Create Cancel

5. Click the **Create** button.

You can delete data marking values that are no longer needed.

To delete values

1. Select one or multiple values from the data marking detail page.

New Marking update list Update Order Delete

NAME: New Marking update list
DESCRIPTION: Test 1234
DEFAULT VALUE: v2
DATA POLICIES: 0 data policies reference this marking.
CREATED: Jul 19, 2017, 10:42 am (a month ago)
UPDATED: Jul 24, 2017, 01:31 pm (a month ago)
ACCESS: VISIBLE
COLLECTS CLIENT-DEFINED VALUES: Yes
VERSION: 15 of 15

Values History + Create Data Marking Value Order Values

Search for values by name... + Add Search << < 1 - 3 of 3 > >>

Action Apply to Selected Cancel

v1 *None* 2 data policies will be applied.
0 data policies reference this value. DATA PROTECTED
Last 30 days 0 DATA ACCESSED
Last 30 days

v2 *None* 2 data policies will be applied.
0 data policies reference this value. DATA PROTECTED
Last 30 days 0 DATA ACCESSED
Last 30 days

v3 *None* 2 data policies will be applied.
0 data policies reference this value. DATA PROTECTED
Last 30 days 0 DATA ACCESSED
Last 30 days

2. Select **Delete** from the **Action** drop-down list.
3. Click **Apply to Selected**.