

Adaptive Trust Engine

Upgrading to the new 4.7 version of ESG, Libraesva introduced the new “Adaptive Trust Engine” feature.

It shows sender/recipient trust and relationship.

First Time Sender

The concept: our idea is to alert a recipient when someone is writing to him for the first time. It will sound like “be careful of who is writing to you”.

How it works: when enabled, this feature takes **7 days** to build a list of usual interlocutors.

Subsequently, a sender remains in the state of FTS for the first **24h**.

Impact on the end user: a warning message will be applied to the top of the email received.

×This is the first time you’ve received an email from this sender. Make sure this is someone you trust.

You can enable this feature following the menu:

system > content analysis > impersonation protection > external warning

Impersonation Protection

Phishing is the practice of sending email to users with the purpose of tricking them into clicking on a link or revealing personal information. Spear phishing and whaling are targeted phishing attacks.

Whaling Protection External Warning Phishing Highlight

External Warning

A message coming from outside your Organization from a First Time Sender may be dangerous. Libraesva ESG can place an inline warning at the top of the body when a message is from an external source and the sender is the first time he is writing to you.

Add External Warning: Do you want to tag external mail with an inline warning?

Save & Apply

Relationships

It is mandatory to setup ESG also as outbound to exploit this feature.

You can analyze the relationships between two interlocutor, also between two domains.

Relationships:	Identity	Related	First seen	Strength
	user1@domain1	user2@domain2	2020-02-10 13:46	<input type="range"/>
	domain1	domain2	2020-02-10 13:46	<input type="range"/>

You can find it into *message info* tab.