

# ESET Tech Center

Knowledgebase > ESET LiveGuard Advanced (ESET Dynamic Threat Defense) > How to enable and configure the ESET LiveGuard Advanced (ESET Dynamic Threat Defense) service

## How to enable and configure the ESET LiveGuard Advanced (ESET Dynamic Threat Defense) service

Steef | ESET Nederland - 2022-04-25 - Comments (0) - ESET LiveGuard Advanced (ESET Dynamic Threat Defense)

To enable the ESET LiveGuard Advanced (ESET Dynamic Threat Defense) service on a client machine, a user needs to fulfill [requirements](#) and create a [policy](#) to set the service up.

In the ESET PROTECT (Cloud) Web Console create a new policy or edit an existing one and assign it on machines where you want to use the ESET LiveGuard Advanced (ESET Dynamic Threat Defense).



### Note




If you enable the ESET Dynamic Threat Defense on a machine where the service is not **activated** by the license, the setting will not apply. Other settings in the policy would apply.

### ESET LiveGuard Advanced (ESET Dynamic Threat Defense) Settings

1. Log in to Web Console and create or edit a [policy](#).
2. In the Settings section select your product and navigate to:

| Policy  | Setting                                   |
|---|---|
| ESET Endpoint for Windows                       | Detection Engine > Cloud-Based protection |
| ESET Mail Security for Microsoft Exchange (V6+) | Computer > Cloud-Based protection         |
| ESET File Security for Microsoft Server (V6+)   | Detection Engine > Cloud-Based protection |

3. To enable the ESET LiveGuard Advanced (ESET Dynamic Threat Defense) you have to switch on all 3 settings in the Cloud-Based protection section.

|   |   |                                     |
|---|---|-------------------------------------|
| Enable ESET LiveGrid® reputation system (recommended) |  ≥ 7.0 | <input checked="" type="checkbox"/> |
| Enable ESET LiveGrid® feedback system                 |  ≥ 7.0 | <input checked="" type="checkbox"/> |
| Enable ESET Dynamic Threat Defense                    |  ≥ 7.0 | <input checked="" type="checkbox"/> |

| Section: Cloud-Based protection                       | Description   |
|---|---|
| Enable ESET LiveGrid® reputation system (recommended) | Using reputation information from ESET LiveGrid®.             |
| Enable ESET LiveGrid® feedback system                 | Submitting files to ESET cloud.                               |
| Enable ESET Dynamic Threat Defense                    | Submitting files for analysis in ESET Dynamic Threat Defense. |

4. You can define which files are sent automatically to ESET cloud when suspicious.

| Section: Submission of samples  | Description and recommendation  |
|---|---|
| Submit infected samples   | Submitting infected samples for further detection. It is recommended to allow this function.  |
| Executables, Archives, Scripts, Other   | Submitting of certain file types. It is recommended to allow submitting of all files types.   |
| Possible Spam emails  | Submitting of possible Spam emails. (ESET Endpoint for Windows only)  |
| Delete executables, archives, scripts, other samples and possible spam emails from ESET's servers | Action after the analysis is done.  |
| Documents   | Submitting of documents.  |
| Delete documents from ESET's servers  | Action after the analysis is done.  |
| Exclusions  | List of file extensions which excludes files from submitting. Extensions are added in the following format: *. <b>ext</b> ? where:<br>* stands for the file name<br><b>ext</b> stands for the file type extension<br>? stands for one optional character. This is optional. |
| Maximum size of samples (MB)  | Maximum size of a submitted file.   |

5. Set up detection threshold and actions taken after a file has positive result above the threshold.

| Section: ESET Dynamic Threat Defense     | Description and recommendation   |
|--|--|
| Detection threshold                      | <b>Status</b> of the result of the analysis which triggers the <b>Action after detection</b> .                               |
| Action after detection                   | Action which the ESET security product does, if the analyzed file has result equal or above the <b>Detection threshold</b> . |
| Maximum wait time for the analysis (min) | Maximum wait time for the analysis result before the mail is delivered or the downloaded file is made available.             |
| Proactive protection                     | <b>Proactive protection</b> setting. You can allow execution of files which analysis is not yet finished.                    |

6. Finish the [policy](#) by selecting computers or groups to be assigned by the policy. New settings are applied after next replication between Server and Agents (usually few minutes).

#### Related Content

- [Mail security in onze security sandbox oplossing | ESET Dynamic Threat Defense \(EDTD\)](#)
- [Security sandbox van de optimale instellingen voorzien | ESET Dynamic Threat Defense](#)
- [Wat kan ik met onze security sandbox oplossing | ESET Dynamic Threat Defense \(EDTD\)?](#)