Landscape Setup for SAP Enterprise Threat Detection
Content

1 Getting Started ................................................................. 3

2 What Is SAP Enterprise Threat Detection .......................... 4

3 System Landscape for Productive Use ............................... 5

4 System Landscape for Developing, Testing, and Productive Use ............................. 6

4.1 Overview: Replicating Development Objects ..................... 7

Marking Attack Detection Patterns for Export .......................... 9
Marking Anomaly Detection Patterns for Export ......................... 10
Marking Productive Rules for Export ...................................... 11
Marking Monitoring Pages for Export ................................. 12

4.2 Replicating Context Data ................................................. 12

Replicating System Contexts ............................................... 13
Replicating Locations ....................................................... 13
Replicating Subnets ......................................................... 14
Replicating User Contexts .................................................. 14
1 Getting Started

By reading this document, you will learn how to set up your SAP Enterprise Threat Detection system landscape for productive use and parallel development and test activities.


To learn how to operate and customize the configuration of SAP Enterprise Threat Detection, see the SAP Enterprise Threat Detection Operations Guide on SAP Help Portal at http://help.sap.com/sapetd.

Note
Check for the latest version of this documentation on SAP Help Portal at http://help.sap.com/sapetd.


For the current release note and other SAP Notes about SAP Enterprise Threat Detection, see SAP Note 2441230.

We welcome your feedback under the support component BC-SEC-ETD.

SAP Enterprise Threat Detection enables you to do real-time evaluation of security threats in your IT landscape. SAP Enterprise Threat Detection itself consists of a set of components deployed on SAP HANA and SAP HANA smart data streaming. To this infrastructure you can connect log providers.
What Is SAP Enterprise Threat Detection

SAP Enterprise Threat Detection enables you to do real-time evaluation of security threats in your IT landscapes by leveraging SAP and non-SAP log data.

Firewalls, virus scanners, and security policies are important parts of your arsenal to keep attackers out of your network, but they are not enough. You must harden every possible avenue of attack, while the attacker only needs to find a single weakness. SAP applications hold your most important business data. It is vitally important that you protect your SAP applications from people who want to damage or exploit your information.

SAP Enterprise Threat Detection detects potential attacks on SAP systems at the application level by gathering and analyzing log data. Whether the threat is internal or external, SAP Enterprise Threat Detection alerts you to potential attacks in real time. You have the opportunity to investigate and either dismiss the alert or pursue an actual incident.

SAP Enterprise Threat Detection provides graphical tools to enable you to navigate the log data. With the log data, you can support forensic analyses or gain new insights into your system landscape. From these new insights, you can create new attack detection patterns and run them regularly against log data as the log data comes in. Any matches to the patterns generate alerts.
3 System Landscape for Productive Use

The following figure is a model of the system landscape of a productive SAP Enterprise Threat Detection.

The log event providers provide the logs monitored by SAP Enterprise Threat Detection. We provide additional software so you can connect log providers, such as SAP HANA and SAP NetWeaver Application Server. SAP Enterprise Threat Detection also enables you to connect other log providers that provide unstructured log formats, such as syslog.


The context providers are systems such as SAP Identity Management (SAP IDM). SAP IDM contains information about users in your system landscape, the persons the users represent, and the systems where these users are located. To learn more about how SAP IDM is connected to SAP Enterprise Threat Detection see the chapter about the technical system landscape in SAP Enterprise Threat Detection Implementation Guide available on SAP Help Portal at http://help.sap.com/sapetd.
4 System Landscape for Developing, Testing, and Productive Use

In your SAP Enterprise Threat Detection system landscape, you have to meet the following requirements:

- Guarantee trouble-free productive use of SAP Enterprise Threat Detection
- Enable development and test activities without interrupting operations
- Enable update and upgrade activities

Development activities in SAP Enterprise Threat Detection can only be carried out with real data in the system. For example, if you want to develop or test new attack detection patterns, you need to have an idea of the log data that you can base the patterns on. Only when relevant log entries are available, you can see whether a pattern actually produces meaningful alerts.

For these purposes, SAP Enterprise Threat Detection offers interfaces for the replication of data from a productive system. These interfaces allow sending and/or receiving replicated data to/from additional SAP HANA smart data streaming and SAP HANA systems. The following types of data will have to be replicated or exchanged.

- **Unidirectional Replication of Log Data**
  Log data from a productive SAP HANA smart data streaming system can be replicated and sent to a second SAP HANA smart data streaming system that is used for developing and testing.

- **Unidirectional Replication of Context Data**
  Context data such as system or user data, IP subnet data, and locations can be sent from the productive SAP HANA system to a second SAP HANA used for development and testing.

- **Bi-Directional Replication of Development Objects**
  Development objects such as forensic workspaces, attack detection patterns, value lists, knowledge base content, and monitoring pages can be exchanged between the productive SAP HANA system and a second SAP HANA system that is used for developing and testing.

We recommend installing new service packs in the development and test system. When you have ensured that SAP Enterprise Threat Detection runs as expected, you can push the content to your productive system.
4.1 Overview: Replicating Development Objects

You usually replicate development objects from a development/test system to the productive system after you have tested them.

Prerequisites

- The `sap.secmon.services.util/job/userInterface` job must be active in your source system.
- The `sap.secmon.services.replication::exportImport` job and the job scheduler must be active in both the source and the target system.
You can check this in the XS Job Dashboard at https://<host>:<port>/sap/hana/xs/admin/jobs. For more information about the jobs of SAP Enterprise Threat Detection, see chapter 2.3.3 of the SAP Enterprise Threat Detection Implementation Guide at https://help.sap.com/sapetd. For more information about the XS Job Dashboard, see the documentation for SAP HANA platform on SAP Help Portal.

Context

Transporting development objects from your development (source) system into your productive (target) system essentially comprises four steps: configuration of the connection between the systems, marking the objects to be exported, exporting them from the source system, and then importing them into the target system.

The following development objects can be exported from your source system and imported into your target system:

- Attack detection patterns (note that to export attack detection patterns, you actually need to export the forensic workspaces in which the patterns are located)
- Anomaly detection patterns
- Value lists
- Productive rules from log learning
- Semantic events that you have created in the knowledge base
- Monitoring pages

Procedure

1. In both the source and the target system, configure the connection for the replication of data.
   
   From SAP Enterprise Threat Detection launchpad, choose the Settings tile and then Content Replication and enter the required data:
   
   ○ Choose Development Objects
   
   ○ Specify the source and the target system
   
   ○ Set the status to Active

2. In the source system, mark the development objects for export.

   Marking objects for export creates an entry in the export table in the Content Replication user interface. The chapters below provide detailed procedures for each development object. After marking the objects for export, proceed with step 3.

   Note that when you delete an object, the deletion does not have to be marked for export, but will be available in the export table right away.

3. In the source system, from SAP Enterprise Threat Detection launchpad, choose Content Replication.

   1. Select the objects that you want to export and choose Start Export. The status changes from Export to Exporting.
   
   2. Choose Refresh. When the export is finished, the status changes to Exported, which means that the objects have been replicated to the Import table in the target system.

   Note that these table entries are deleted 14 days after the export.
4. Log on to the target system. From SAP Enterprise Threat Detection launchpad, choose Content Replication. 
   1. Select the objects you want to import and choose Start Import. The status changes from Import to Importing.
   2. Choose Refresh. When the import is finished, the status changes to Imported, which means that the objects are ready for use in your productive system. Note that these table entries are deleted 14 days after the import.

4.1.1 Marking Attack Detection Patterns for Export

To export an attack detection pattern, you have to export the forensic workspace and the value lists that are used by the pattern.

Context

Marking the objects for export is only one step in the replication of development objects. Please refer to the overview procedure.

Procedure

1. From SAP Enterprise Threat Detection launchpad, choose Patterns and then open the pattern user interface by clicking its name.
2. In the pattern user interface, choose Open to open the forensic workspace.
3. In forensic lab, choose Open and search for the forensic workspace that you just opened. Search for the name that you see in the upper left corner.
4. Select the forensic workspace from the list and choose Export at the bottom of this dialog window.
   The forensic workspace is marked for export.
5. Go back to the pattern user interface to check if the pattern uses value lists. If so, choose the Value Lists tab and click the first value list to open it.
6. In the value list, choose Export.
   The value list has been marked for export. If the pattern uses more than one value list, repeat this step for each one.
4.1.2 Marking Anomaly Detection Patterns for Export

When you export an anomaly detection pattern, all forensic workspaces from which charts are referenced in the anomaly detection pattern are automatically exported. However, the value lists that are used in the anomaly detection pattern must be exported separately.

Context

Marking the objects for export is only one step in the replication of development objects. Please refer to the overview procedure.

Procedure

1. From SAP Enterprise Threat Detection launchpad, choose *Anomaly Detection Lab* and then open the anomaly detection pattern by selecting it from the list.

2. Choose the ![Export](Export) icon to export the anomaly detection pattern.
   
   The anomaly detection pattern and all referenced forensic workspaces have been marked for export. This means that they have been added to the export table in the *Content Replication* user interface.

3. From SAP Enterprise Threat Detection launchpad, choose *Patterns* and then open the anomaly detection pattern you just marked for export by clicking its name.

4. Choose the Value Lists tab to check whether the anomaly detection pattern uses value lists. If so, click the first value list to open it.

5. In the value list, choose *Export*.

   The value list has been marked for export. This means it has been added to the export table in the *Content Replication* user interface. If the pattern uses more than one value list, repeat this step for each one. Note that if you delete an anomaly detection pattern, the deletion operation will be added to the export table automatically.
4.1.3 Marking Productive Rules for Export

When you are finished with log learning in your test system, you can export the productive rules to your productive system. Note that you have to export new semantic events that you have created in the test system separately.

Context

To export productive rules, you select a log type and replicate all productive rules for this log type simultaneously. If there are already productive rules for this log type in your target system, note that these are overwritten. Marking the objects for export is only one step in the replication of development objects. Please refer to the overview procedure.

Procedure

1. From the Log Learning tile in the SAP Enterprise Threat Detection launchpad, choose Productive Rules.
2. Choose Export Rules and select the log type.
3. Choose OK to confirm that you want to export the productive rules of this log type.
   - The productive rules are marked for export. This means that they are added to the export table in the Content Replication user interface.
4. You now have to check if the log type uses semantic events that you have created. In the Productive Rules user interface, choose Show Filter Bar, type in the log type and choose Go.
   - You now see the semantic events from this log type. The ones that you have created have to be exported.
5. From the SAP Enterprise Threat Detection launchpad, choose Knowledge Base.
6. On the Events tab, select the first event that you want to export and choose Export.
   - The event has been marked for export. This means it has been added to the export table in the Content Replication user interface. Repeat this step for each event you want to export. It is not possible to export multiple events in a mass operation. Note that if you delete productive rules, the deletion operation will be added to the export table automatically.
4.1.4 Marking Monitoring Pages for Export

You can transport monitoring pages from your source system to the target system.

Context

Marking the objects for export is only one step in the replication of development objects. Please refer to the overview procedure.

Procedure

1. From the SAP Enterprise Threat Detection launchpad, choose Monitoring.
2. Choose the icon (Configure the layout and behavior of the UI) in the upper right corner.
3. Choose Export.

The monitoring page is marked for export. This means that it is added to the export table in the Content Replication user interface. Note that if you delete a monitoring page, the deletion operation will be added to the export table automatically.

4.2 Replicating Context Data

Context

Following configuration is required in the Source SAP Enterprise Threat Detection system and in the target system to replicate the Contexts.

- Object Type Area: Contexts
- Source System: <SourceETDSystem>
- Target System: <TargetETDSystem>
- Status: Active

Procedure

1. Export Import Job

Make sure that the following job is active in source and target SAP Enterprise Threat Detection system.
4.2.1 Replicating System Contexts

Procedure

1. Create and save a new system context in Source SAP Enterprise Threat Detection system.
2. Export Import Job will push this newly created context in export table which is then replicated in import table of target SAP Enterprise Threat Detection system.
3. Export Import Job will create/update this newly created system in target SAP Enterprise Threat Detection system.
   Step 2 and 3 may take up to 2 minutes.
4. Newly created system should be available in target SAP Enterprise Threat Detection system.
5. Change an existing system context in Source SAP Enterprise Threat Detection system.
6. This change should be replicated in target SAP Enterprise Threat Detection system.

4.2.2 Replicating Locations

Procedure

1. Create and save a new location in Source SAP Enterprise Threat Detection system.
2. Choose button Export on location UI so that it gets written in export table.
3. Select the desired context on Replication UI on EXPORT tab and choose Export function so that this object gets replicated in the import table of target SAP Enterprise Threat Detection system. https://<host>:<port>sap/secmon/ui/replication/?sap-language=en
4. Export Import Job will create/update this newly created context in target ETD system.
   Step 4 may take up to 2 minutes.
5. Newly created context should be available in target SAP Enterprise Threat Detection system.
6. Change an existing context in Source SAP Enterprise Threat Detection system.
7. This change should be replicated in target SAP Enterprise Threat Detection system.

### 4.2.3 Replicating Subnets

**Procedure**

1. Create and save a new Subnet in Source SAP Enterprise Threat Detection system.
2. Choose button Export on Subnet UI so that it gets written in export table.
3. Select the desired context on Replication UI on **EXPORT** tab and choose Export function so that this object gets replicated in the import table of target SAP Enterprise Threat Detection system [https://<host>:<port>/sap/secmon/ui/replication/?sap-language=en](https://<host>:<port>/sap/secmon/ui/replication/?sap-language=en)
4. Export Import Job will create/update this newly created context in target SAP Enterprise Threat Detection system.
   - Step 4 may take up to 2 minutes.
5. Newly created context should be available in target SAP Enterprise Threat Detection system.
6. Change an existing context in Source SAP Enterprise Threat Detection system.
7. This change should be replicated in target SAP Enterprise Threat Detection system.

### 4.2.4 Replicating User Contexts

**Procedure**

1. Create a user in ABAP system.
2. Start the master data report so that the user gets published in Source SAP Enterprise Threat Detection system.
3. This can be checked with the following SQL statement in source system.

   ```sql
   SELECT * FROM "SAP_SEC_MON"."sap.secmon.db::User.UserSystemData"
   WHERE "SystemType" = 'ABAP'
   AND "System" = '<SYSTEM>/<CLIENT>' -- e.g. YI3/000
   AND "SystemUser" = '<USERNAME>'  -- e.g. MUELLER
   ```

4. Export Import Job will create/update this newly created user context in target SAP Enterprise Threat Detection system.
Step 3 may take up to 2 minutes.

5. Check the result with the same SQL as mentioned above in the target SAP Enterprise Threat Detection system.

Content replication will not replicate namespaces created in the source system.
Important Disclaimers and Legal Information

Coding Samples
Any software coding and/or code lines / strings (“Code”) included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended to better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, unless damages were caused by SAP intentionally or by SAP’s gross negligence.

Accessibility
The information contained in the SAP documentation represents SAP’s current view of accessibility criteria as of the date of publication; it is in no way intended to be a binding guideline on how to ensure accessibility of software products. SAP in particular disclaims any liability in relation to this document. This disclaimer, however, does not apply in cases of willful misconduct or gross negligence of SAP. Furthermore, this document does not result in any direct or indirect contractual obligations of SAP.

Gender-Neutral Language
As far as possible, SAP documentation is gender neutral. Depending on the context, the reader is addressed directly with “you”, or a gender-neutral noun (such as “sales person” or “working days”) is used. If when referring to members of both sexes, however, the third-person singular cannot be avoided or a gender-neutral noun does not exist, SAP reserves the right to use the masculine form of the noun and pronoun. This is to ensure that the documentation remains comprehensible.

Internet Hyperlinks
The SAP documentation may contain hyperlinks to the Internet. These hyperlinks are intended to serve as a hint about where to find related information. SAP does not warrant the availability and correctness of this related information or the ability of this information to serve a particular purpose. SAP shall not be liable for any damages caused by the use of related information unless damages have been caused by SAP’s gross negligence or willful misconduct. All links are categorized for transparency (see: http://help.sap.com/disclaimer).