

Hands-on experience with SAP Enterprise Threat Detection, cloud edition

Exercise: Working with SAP Enterprise Threat Detection Version

**Based on SAP Enterprise Threat Detection, cloud edition, Version
November 2025**

**Get Hands-On with the New
*SAP Enterprise Threat Detection, cloud
edition***

Contents

Overview & Touring SAP Enterprise Threat Detection, public cloud.....	3
1. Logon to the Monitoring Console of SAP Enterprise Threat Detection, public cloud	4
1.1 Got a Warning ‘Select a Tenant’	6
1.2 UI Round trip	7
2. First Log Events from SAP S/4HANA	13
2.1 Logon & Preparation Steps.....	13
2.2 Creating a User With High Privileges	14
3. Checking Alerts and Creating Investigations.....	16
3.1 Check for Log Events.....	16
3.2 Search for Alerts	17
3.3 Interpreting the Investigation Entries	18
4. Trigger a Critical Action from SAP S/4HANA: Download of a Critical Database Table.....	19
5. User & Environment Behavioral Analysis – Identify the Critical Action in the Forensic Lab	21
5.1 Build up a Workspace	21
5.1.1 Assigning a Chart	21
6. From Workspace to Pattern to Alerts	21
6.1 Understanding Patterns	21
7. Finalize the Investigation	21
7.1 Information: Maintain your email ID to receive investigation reports	21
7.2 Finalize the investigation	21
8. Consumer/Processor role: Work with Investigation reports.....	21

Overview & Touring SAP Enterprise Threat Detection, public cloud

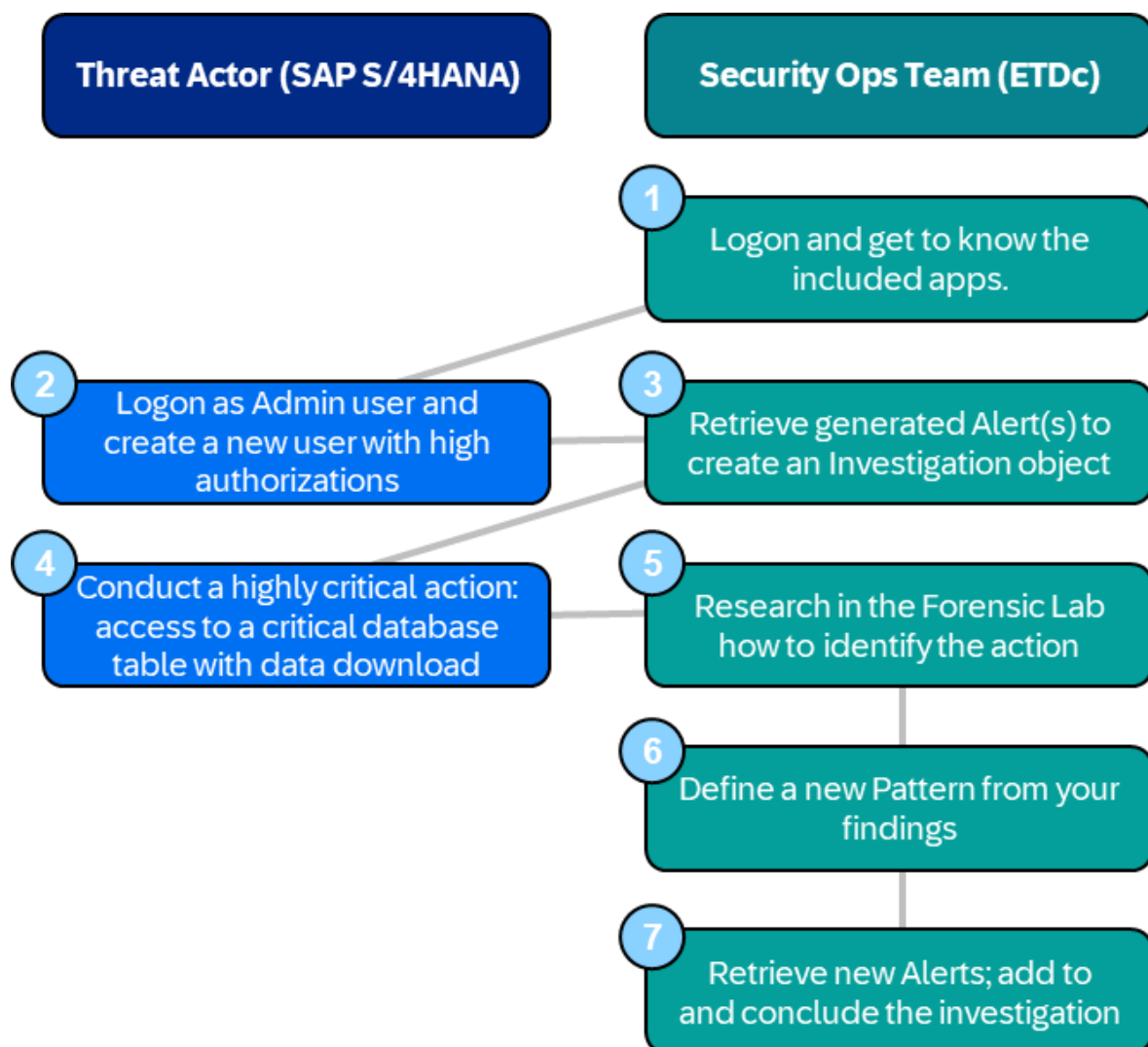
In this hands-on session and workshop of about 1.5 – 2h, you will get to know the basic functioning of *SAP Enterprise Threat Detection, public cloud*, including the terminology employed.

You will switch back and forth between 3 roles. In a first role, you will be a (potential) threat actor in an SAP S/4HANA system and conduct actions resulting in system responses in *SAP Enterprise Threat Detection, public cloud*.

In a second role, you will act as a security specialist in charge to identify potential threats, pin down what has happened and determine the relevance, as well as ensure that the knowledge about the attack vector is added to the repository on which *SAP Enterprise Threat Detection, public cloud* will automatically alert going forward.

In a 3rd role, you will act as a consumer/processor of the results (Investigation Report), that was created by you in your second role as a security specialist.

Here's the flow of the following exercises in your roles as threat actor and security specialist (the numbers relate to the chapters in this document:



Chapters 1 to 7 are related to these to roles. Chapter 8 is related to the consumer/processor role

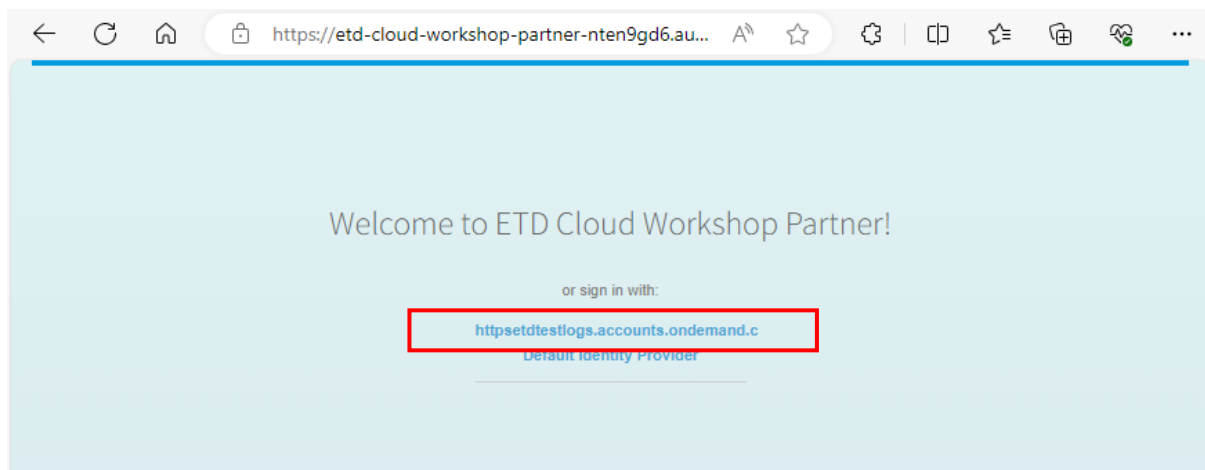
1. [Login to the Monitoring Console of SAP Enterprise Threat Detection, public cloud](#)

This system & credentials are available during the planned workshop hours only.
Please let us know if you'd like to have access afterwards; we're happy to check how long we can extend your access.

Access the [SAP Enterprise Threat Detection, public cloud monitoring console](#)

IMPORTANT:

- You should get the below start page (if not, please empty your browser cache and try again).
- Here, select the first entry ("httpsetdtestlogs.accounts.ondemand") to log on with the generic workshop users below (not any personal credentials – they won't be recognized in this cloud application).
Do **NOT** choose the "Default Identity Provider" (here, the generic users won't work).



In the ensuing (login) screen, use the ID indicated to you (01-35; afterwards referred to as "##").

User: teched##@etdsap.com

Password: will be provided in the session

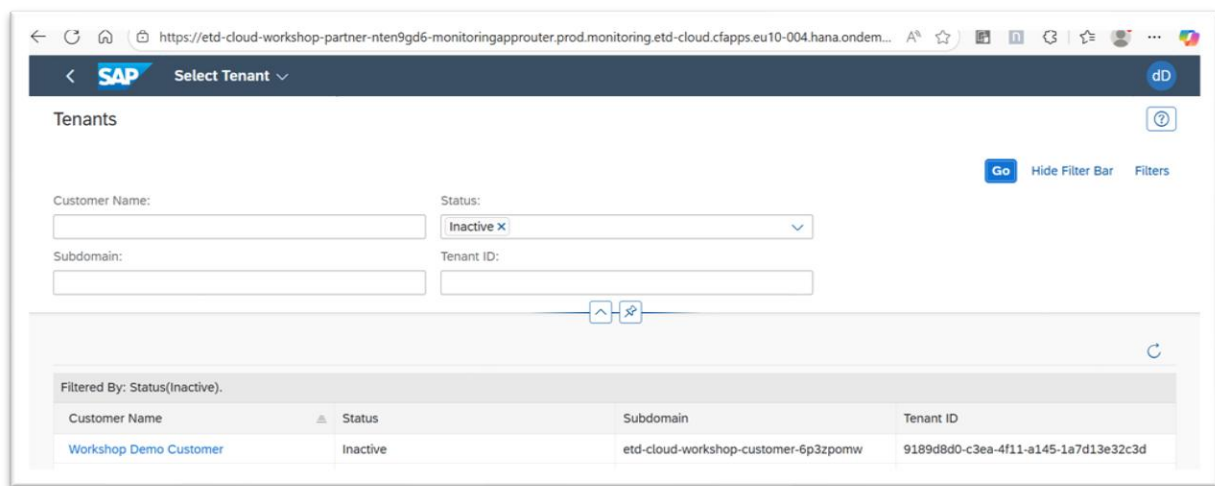
If you inadvertently lock the password, please notify the instructor.

If you receive a blank screen saying "Where to", please clear the cache, then close and restart the browser. If you may also open an private browsing window (often "incognito" or "InPrivate"). Log on again.

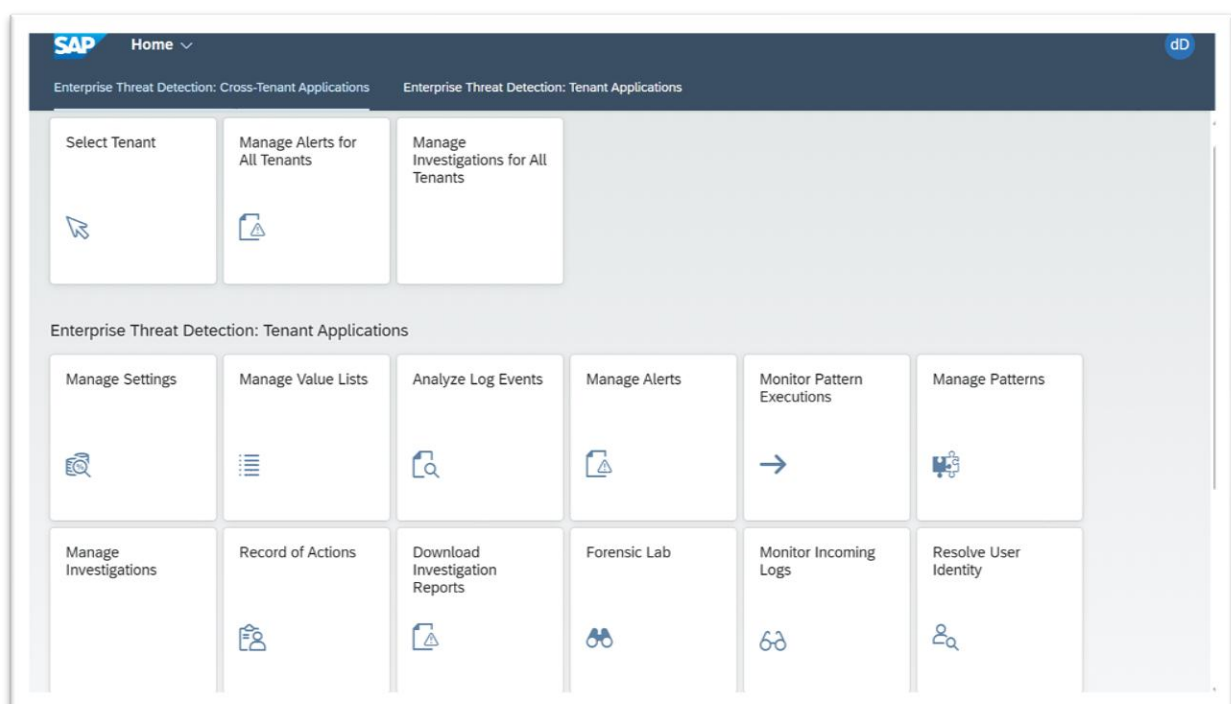
Upon initial logon, In case you get pop-up message to select a Tenant, than click the Select Tenant screen for selecting a specific Tenant:

As a monitoring agent providing services to multiple clients, you will log on to your organization's own productive Tenant; however from here commonly access and work in the specific Tenant of a client, which you can select from this list reflecting all clients/Tenants linked to your organization.

For this hands-on there is only one customer system linked. Click on the blue hyperlink and select "Workshop Demo Customer".

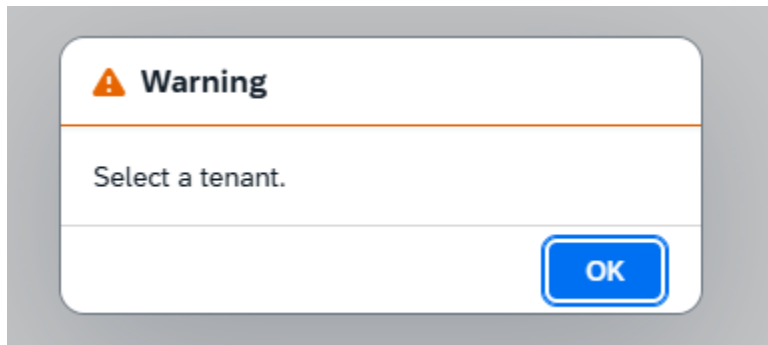


You will then see the *SAP Enterprise Threat Detection, public cloud* monitoring console. Take a bit of time to check by a few apps and how they behave.



1.1 Got a Warning ‘Select a Tenant’

If you encounter a the warning popup

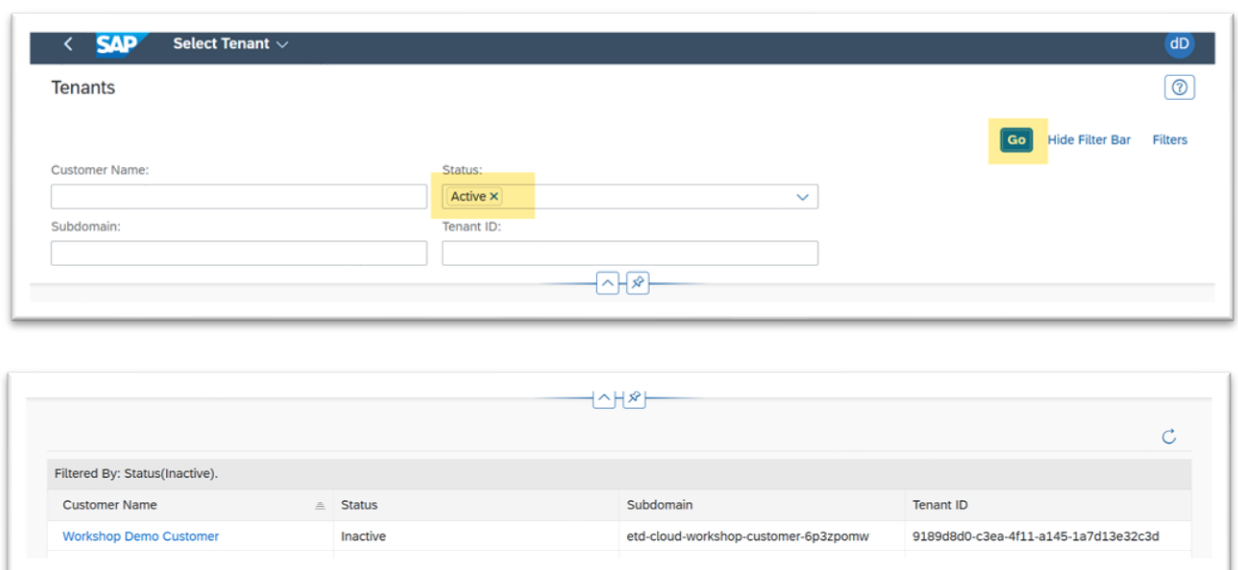


the system has lost the information which Tenant you’ve been working on (most likely you had been logged out).

In this case, either start the *SAP Enterprise Threat Detection, public cloud* console again via the above link.

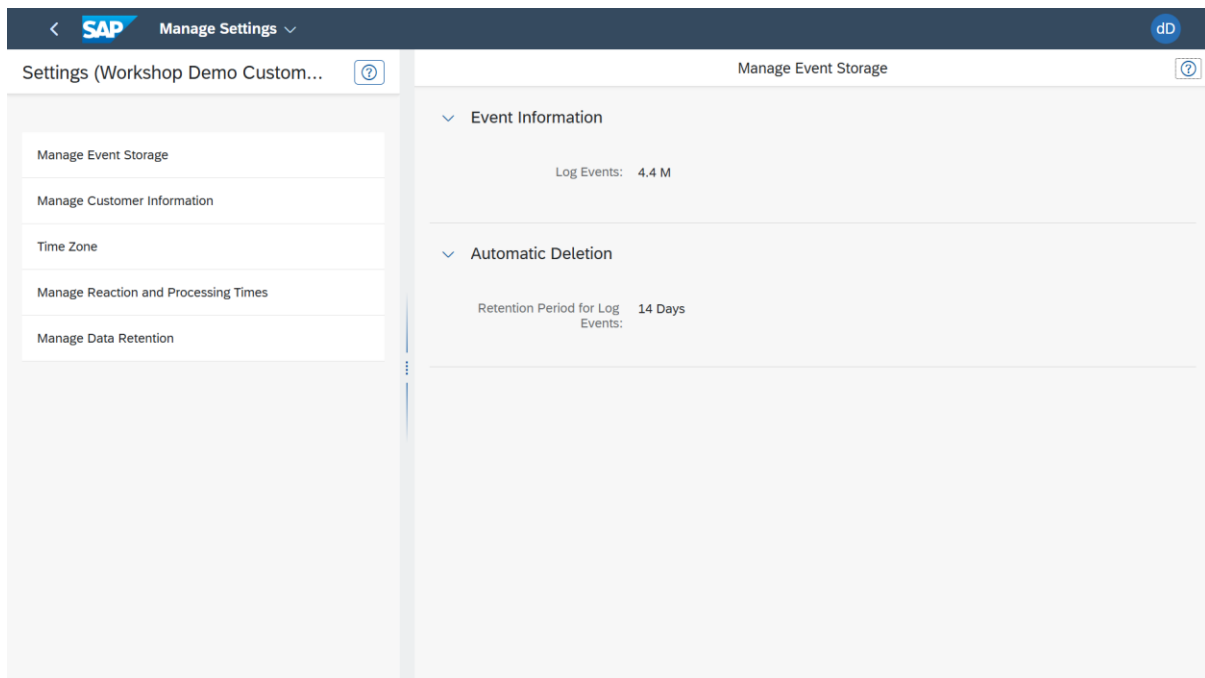
Alternatively, you can manually set the correct tenant:

- In the section for “Cross-Tenant Applications”, open the app “Select Tenant”.
- Remove filters “active” and press “go”.
- The entry “Workshop Demo Customer” will show; select this so the system is aware which Tenant you are working on – which is relevant in case you’re a partner providing monitoring services to multiple clients)

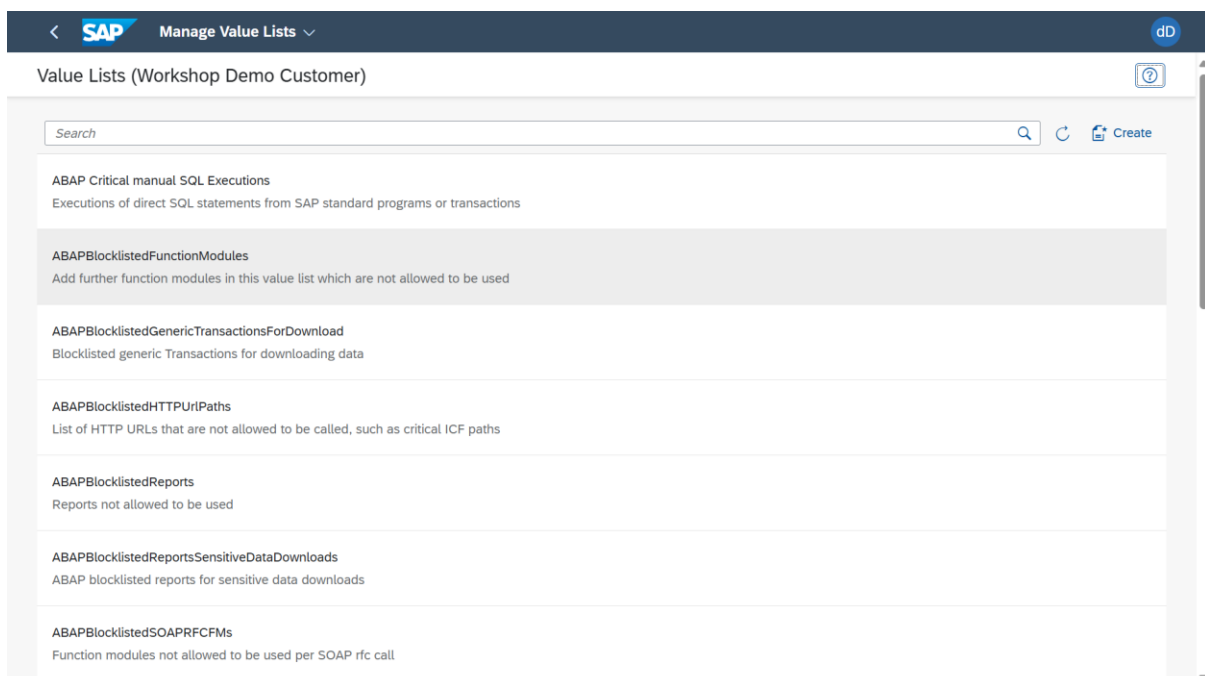


1.2 UI Round trip

In Manage Setting tab, users can manage system setting like retention times and time zone etc.



In Value list tab, users can manage value lists which are allow or disallow list where system analyst and put custom values and even can create custom value lists



In Analyze Log Events tab, system analyst and view and analyze customers normalized log data.

SAP Analyze Log Events dD

Log Events (Workshop Demo Customer) ?

Go Hide Filter Bar Filters

Creation Time Range: User: System: Service: Semantic Event:

Event, Log Type: Service, Instance Name: Service, Program Name: Service, Transaction Name:

2025/10/10 00:16:44 AM GMT+05:30 - 2025/10/20 00:16:44 AM GMT+05:30 User System Service

<input type="checkbox"/>	Timestamp	Semantic Event	Event, Log Type	User	
<input type="checkbox"/>	2025/10/18 05:43:30 AM GMT+05:30	Indicator From Pattern	Indicator	ETDADMIN (Target)	>
<input type="checkbox"/>	2025/10/18 01:50:02 AM GMT+05:30	Indicator From Pattern	Indicator	ETDADMIN (Target)	>
<input type="checkbox"/>	2025/10/18 01:43:30 AM GMT+05:30	Indicator From Pattern	Indicator	ETDADMIN (Target)	>
<input type="checkbox"/>	2025/10/18 01:40:02 AM GMT+05:30	Indicator From Pattern	Indicator	ETDADMIN (Target)	>
<input type="checkbox"/>	2025/10/18 01:30:52 AM GMT+05:30	Indicator From Pattern	Indicator	TMSADM (Target)	>
<input type="checkbox"/>	2025/10/18 01:30:50 AM GMT+05:30	Indicator From Pattern	Indicator		>
<input type="checkbox"/>	2025/10/18 01:30:50 AM GMT+05:30	Indicator From Pattern	Indicator		>
<input type="checkbox"/>	2025/10/18 01:30:02 AM GMT+05:30	Indicator From Pattern	Indicator	ETDADMIN (Target)	>
<input type="checkbox"/>	2025/10/18 01:29:57 AM GMT+05:30	Executable, RFC-enabled Function Module, Run	SecurityAuditLog	NODK_35740 (Acting)	>
<input type="checkbox"/>	2025/10/18 01:29:56 AM GMT+05:30	Database, Data, Select, Generic	SecurityAuditLog	NODK_35740 (Acting)	>

In Manage Alerts tab, system analyst and view and analyze generated alerts.

SAP Manage Alerts dD

Alerts (Workshop Demo Customer) ?

Go Hide Filter Bar Filters

Creation Time Range: Pattern:

Status: Severity:

Trigger Value 1: Trigger Value 2:

Alerts (1,289) Create Investigation Add to Investigation Set to Open Set to No Reaction Needed Mass Status Change Direct Access to Alert: ...

Filtered By: alerts.creationTimeRange(2025/10/10 00:17:27 AM GMT+05:30 - 2025/10/20 00:17:27 AM GMT+05:30)

<input type="checkbox"/>	Severity	ID	Pattern	Trigger	Events	St
<input type="checkbox"/>	High	132952	Logon from internal with SAP standard users (alerts)	Measurement 25 exceeded threshold 1 for ('System ID, Actor' = 'S4H/100', 'User Pseudonym, Target' = 'ETDADMIN')		O1
<input type="checkbox"/>	High	132951	Logon from internal with SAP standard users (alerts)	Measurement 48 exceeded threshold 1 for ('System ID, Actor' = 'S4H/100', 'User Pseudonym, Target' = 'ETDADMIN')		O1
<input type="checkbox"/>	High	132950	Logon from external with SAP standard users	Measurement 1 exceeded threshold 1 for ('Event (Semantic)' = 'User, Logon', 'Network, Hostname, Initiator' = '10.0.0.7', 'System ID, Actor' = ...)		O1
<input type="checkbox"/>	Medium	132948	Successful logon from same Terminal ID with different users	Measurement 3 exceeded threshold 2 for ('Network, Hostname, Initiator' = '10.79.59.150', 'System ID, Actor' = 'S4H/000')		O1
<input type="checkbox"/>	Medium	132949	Successful logon from same Terminal ID with different users	Measurement 4 exceeded threshold 2 for ('Network, Hostname, Initiator' = '10.79.59.150', 'System ID, Actor' = 'S4H/100')		O1
<input type="checkbox"/>	High	132947	Logon from external with SAP standard users	Measurement 1 exceeded threshold 1 for ('Event (Semantic)' = 'User, Logon', 'Network, Hostname, Initiator' = '10.0.0.7', 'System ID, Actor' = ...)		O1
<input type="checkbox"/>	High	132946	Logon from external with SAP standard users	Measurement 1 exceeded threshold 1 for ('Event (Semantic)' = 'User, Logon, Failure', 'Network, Hostname, Initiator' = '10.79.59.150', 'System ID, Actor' = ...)		O1
<input type="checkbox"/>	High	132945	Logon from external with SAP standard users	Measurement 1 exceeded threshold 1 for ('Event (Semantic)' = 'User, Logon, Failure', 'Network, Hostname, Initiator' = '10.79.59.150', 'System ID, Actor' = ...)		O1

In Pattern Executions tab, system analyst and view and check status of pattern executions

<

SAP

Monitor Pattern Executions

dD

Pattern Executions (Workshop Demo Customer)

Go Hide Filter Bar Filters

Execution Time Range:
Last 1 day

Pattern:
Enter the name of a pattern (at least 2 characters)

Pattern Namespace:

Status:

Execution Mode:

Pattern Executions (23,762) 2025/10/18 18:47:59 PM UTC - 2025/10/19 18:47:59 PM UTC

Pattern	Namespace	Execution Time	Run...	St...	E
DoS attack against different RFC destinations	http://sap.com/secmon/basis	2025/10/20 00:15:59 AM GMT+05:30	26	OK	Jk >
Security relevant Policy Changes	http://sap.com/secmon/basis	2025/10/20 00:15:59 AM GMT+05:30	14	OK	Jk >
Change of HR Critical Role	http://sap.com/secmon/content	2025/10/20 00:15:59 AM GMT+05:30	37	OK	Jk >
Calls from non-productive to productive systems via RFC	http://sap.com/secmon/basis	2025/10/20 00:15:58 AM GMT+05:30	26	OK	Jk >
Critical Function module call in Test framework calls	http://customer.com	2025/10/20 00:15:57 AM GMT+05:30	22	OK	Jk >
DoS attack against different HTTP URLs	http://sap.com/secmon/basis	2025/10/20 00:15:56 AM GMT+05:30	16	OK	Jk >
Debugging in critical systems	http://sap.com/secmon/basis	2025/10/20 00:15:55 AM GMT+05:30	32	OK	Jk >
New Report ceated in critical system role	http://customer.com	2025/10/20 00:15:54 AM GMT+05:30	14	OK	Jk >
Critical manual in-ABAP SQL statement execution	http://customer.com	2025/10/20 00:15:54 AM GMT+05:30	45	OK	Jk >

In Pattern tab, system analyst and view and create patterns(i.e. use cases)

<

SAP

Manage Patterns

dD

Patterns (Workshop Demo Customer)

Go Hide Filter Bar Filters

Name:
Enter the name of a pattern (at least 2 characters)

Namespace:

Status:

Execution Output:

Test Mode:

Patterns (176)

Create Pattern Activate Deactivate Execute Delete Pattern Test Mode On Test Mode Off

Name	Namespace	Description
04_PWHashAttack	http://customer.com	Angriff von Demo-User 04
99_PWHashAttack	http://customer.com	Fake user accessing PW Hashes
ABAP critical Function Module Calls per SOAP RFC	http://sap.com/secmon/basis	Client calls critical ABAP function modules per SOAP rfc interface.
ABAP deactivated or deleted function modules	http://sap.com/secmon/basis	A user has tried to execute a function module that should not be executed remotely the function module was deactivated or deleted by an SAP Security Note.
ABAP deactivated or deleted reports	http://sap.com/secmon/basis	A user has tried to execute a report which was deactivated or removed by an SAP Se Note.
ABAP function modules with removed RFC enablement	http://sap.com/secmon/basis	A user has tried to execute a function module that should not be executed remotely. enablement of remote function call was removed by an SAP Security Note.

In Investigations tab, system analyst and view and manage investigations.

SAP Manage Investigations dD

Investigations (Workshop Demo Customer)

Go Hide Filter Bar Filters

Status: Severity: Management Visibility: Created By: Processor: Description:

Investigations (63) Direct Access to Investigation: Enter ID Open

Severity	Management Visibility	ID	Description	Status	Remaining Processing Time (RPT)
Medium	Not Needed	148	test	Open	38 Hours 31 Minutes 15 Seconds
Medium	Not Needed	147	jh	Open	38 Hours 34 Minutes 14 Seconds
Medium	Not Needed	146	yii	Open	38 Hours 35 Minutes 10 Seconds
Medium	Not Needed	145	test33	Open	38 Hours 39 Minutes 39 Seconds
Medium	Not Needed	144	test	Open	50 Hours 1 Minutes 24 Seconds
Medium	Not Needed	143	Std User Access	Open	293 Hours 54 Minutes 21 Seco...
High	Not Needed	142	Critical user cativities	Completed	465 Hours 50 Minutes 15 Seco...
High	Not Needed	141	Sensitive Data download	Completed	535 Hours 1 Minutes 24 Seconds
High	Not Needed	140	Critical Data Download	Completed	538 Hours 54 Minutes 46 Seco...

In Records tab, system analyst and view use activity logs of ETD system

SAP Record of Actions dD

Records (Workshop Demo Customer)

Go Hide Filter Bar Filters

Time Range: Last 1 day User: Entity Type: Entity Namespace: Entity Operation: Entity Name: Enter the name of an entity (at least 3 characters)

Records (2,899) 2025/10/19 00:19:15 AM GMT+05:30 - 2025/10/20 00:19:15 AM GMT+05:30

Timestamp	User	Entity Type	Entity Namesp...	Entity Name	Entity Operation	Text
2025/10/20 00:18:58 AM	system	Investigation			Read	Request URL = https://etdcloudprod-004-prod-etc-cloud-data-retrieval-service.cfapps.eu10-004.hana.on... Show More
2025/10/20 00:18:58 AM	system	Alert			Read	Request URL = https://etdcloudprod-004-prod-etc-cloud-data-retrieval-service.cfapps.eu10-004.hana.on... Show More
2025/10/20 00:17:59 AM	system	Investigation			Read	Request URL = https://etdcloudprod-004-prod-etc-cloud-data-retrieval-service.cfapps.eu10-004.hana.on... Show More
2025/10/20 00:17:58 AM	system	Alert			Read	Request URL = https://etdcloudprod-004-prod-etc-cloud-data-retrieval-service.cfapps.eu10-004.hana.on... Show More
2025/10/20 00:16:59 AM	system	Investigation			Read	Request URL = https://etdcloudprod-004-prod-etc-cloud-data-retrieval-service.cfapps.eu10-004.hana.on... Show More
2025/10/20 00:16:58 AM	system	Alert			Read	Request URL = https://etdcloudprod-004-prod-etc-cloud-data-retrieval-service.cfapps.eu10-004.hana.on... Show More
2025/10/20 00:15:59 AM	system	Investigation			Read	Request URL = https://etdcloudprod-004-prod-etc-cloud-data-retrieval-service.cfapps.eu10-004.hana.on... Show More
2025/10/20 00:15:58 AM	system	Alert			Read	Request URL = https://etdcloudprod-004-prod-etc-cloud-data-retrieval-service.cfapps.eu10-004.hana.on... Show More
2025/10/20 00:14:59 AM	system	Investigation			Read	Request URL = https://etdcloudprod-004-prod-etc-cloud-data-retrieval-service.cfapps.eu10-004.hana.on... Show More

In Investigations Report tab, system analyst and view investigations

< **SAP** Download Investigation Reports ▼ dD

Investigation Reports (Workshop Demo Customer) ?

Investigation Reports Monthly Reports

Go Hide Filter Bar Filters

Severity: Description: ID:

Customer Notification: Investigator: Report Status:

Report Severity: Closing Remarks: Tags:

	Severity	ID	Report Crea...	Description	Customer N...	Completion ...	Investigator	Report Status	Report Sev...	Closing Re...	Tags
<input type="checkbox"/>	High	142	2025/09/29 14:53:00 PM GMT+05:30	Critical user activities	No	2025/09/29 14:53:58 PM GMT+05:30	m.schmitt@sap.com	Open	High		teche...
<input type="checkbox"/>	High	141	2025/09/26 17:41:51 PM GMT+05:30	Sensitive Data download	No	2025/09/26 17:50:01 PM GMT+05:30	m.schmitt@sap.com	In Process	Medium		LOB A
<input type="checkbox"/>	High	140	2025/09/26 13:48:28 PM GMT+05:30	Critical Data Download	No	2025/09/26 13:57:05 PM GMT+05:30	m.schmitt@sap.com	Open	Medium		
<input type="checkbox"/>			2025/09/26	Critical Data		2025/09/26	(Unassigned)				

In Workspace tab, system analyst and view and create Workspace

< **SAP** Forensic Lab ▼ dD

Workspaces (Workshop Demo Customer) ?

Name: Namespace: Use Case: Charts: Patterns:

Process Status:

Go

Custom Workspaces SAP Workspaces

Workspaces (61) Create Workspace Delete Workspaces

	Name	Namespace	Use Case	Charts	Patterns	Process Sta...	Editing Status
<input type="checkbox"/>	02_PWHash_Attack	http://custome	Admin creates a new user with which they attack passwords hashes.			Finished	>
<input type="checkbox"/>	04_Demo_no ch ein Test	http://custome	Admin creates a new user with which they attack passwords hashes.			New	>
<input type="checkbox"/>	04_Golden_P WHash Atta	http://custome	Admin creates a new user with which they attack passwords hashes.	07_PWHashAtt	05_Golden_PW 04_PWHashAt	Finished	>
<input type="checkbox"/>	04_PWHash_ Attack	http://custome	Admin creates a new user with which they attack passwords hashes.	04_Golden PW tack		Finished	>
<input type="checkbox"/>	04.2_PWHash Attack	http://custome	Admin creates a new user with which they attack passwords hashes.			Finished	>
<input type="checkbox"/>	07_PWHash_ Attack	http://custome	Useful for the analysis of singular events of user behavior based on an incident alert.	04_PWHashAtt	04.2_PWHashA	Finished	>
<input type="checkbox"/>	10_PWHash_ Attack	http://custome	Admin creates a new user with which they attack passwords hashes.	DataTheftWithF	07_PWHashAtt	Finished	>
<input type="checkbox"/>	1001_PWHas h Attack	http://custome	Admin creates a new user with which they attack passwords hashes.	10_PWHashAtt		Finished	>
<input type="checkbox"/>	1005_PWHas h Attack	http://custome	Admin creates a new user with which they attack passwords hashes.			Finished	>
<input type="checkbox"/>	95_PWHash_ Attack 2	http://custome	Admin creates a new user with which they attack passwords hashes.			New	>
<input type="checkbox"/>				95_PWHashAtt		Finished	>

In Manage Incoming logs tab, system analyst and view incoming logs

Monitor Incoming Logs

dD

Monitor Incoming Logs (Workshop Demo Customer)

System Name:

Log Status:

Go

Adapt Filters

Systems (7)

System Name	Last Log Received	Log Status
S4H	3 days ago	Not Received Last Day
PM0/000	2 days ago	Not Received Last Day
S4H/000	2 days ago	Not Received Last Day
S4H/200	2 days ago	Not Received Last Day
S4H/400	2 days ago	Not Received Last Day
S4H/100	2 days ago	Not Received Last Day
PM0/100	2 days ago	Not Received Last Day

In Resolve user identity tab, system analyst and view and pseudonymize and pseudonymize user name

Resolve User Identity

dD

Resolve User Identity

Resolve

Reverse

Resolve pseudonym to account name

Enter pseudonym

Resolve

Account Name

Result will appear here...

2. First Log Events from SAP S/4HANA

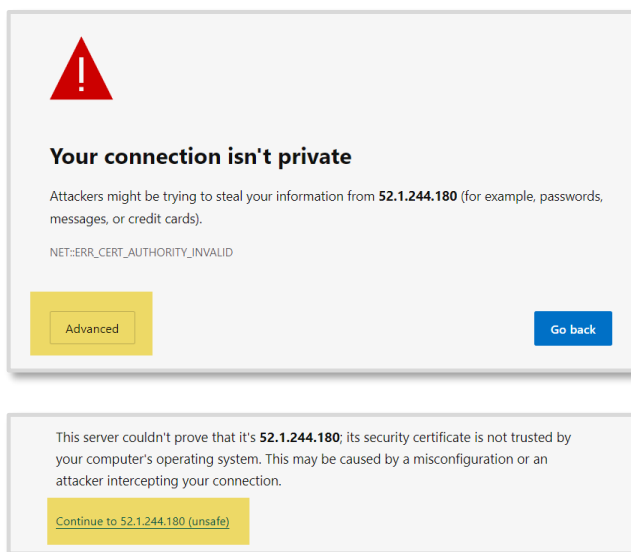
Please note: in this exercise, every workshop station/computer has a designated set of users already existing; throughout the description, “##” is the number of your workshop computer ID.

This system & credentials are available during the planned workshop hours only.
Please let the instructor know in case you'd like to have access afterwards; we're happy to check how long we can extend your access.

In this section, you will conduct actions in SAP GUI to generate Log Events which in return will result in Alerts in *SAP Enterprise Threat Detection, public cloud*.

2.1 Logon & Preparation Steps

- access the WebGUI interface: <https://52.1.244.180:44301/sap/bc/gui/sap/its/webgui>
- Proceed through the “advanced” mode in case you get a warning of unsafe/non-private connection – which might look like this:

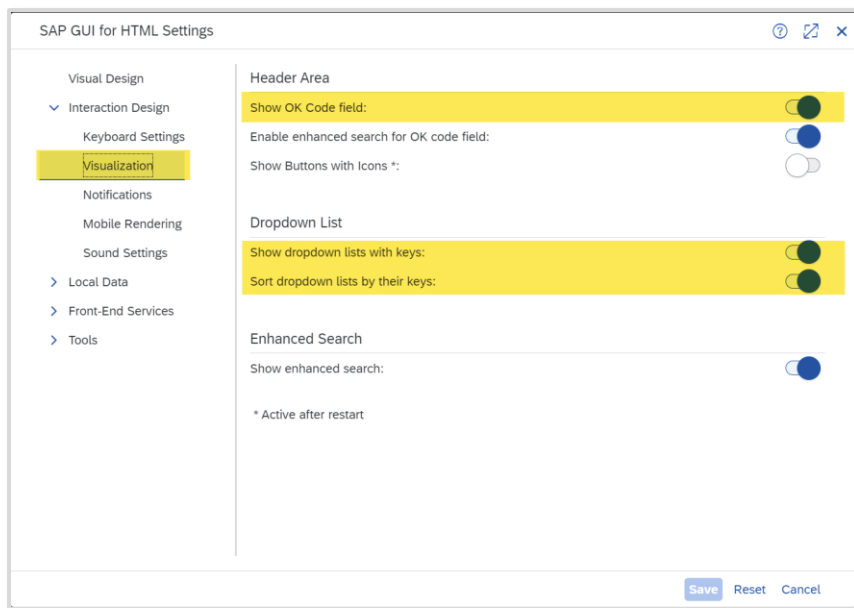


Log on credentials: **User: ETDADMIN##**

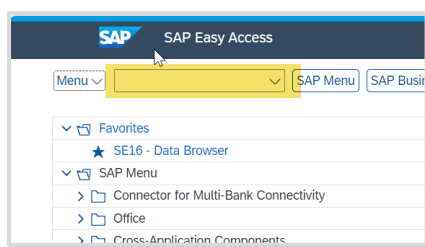
Password: Will be provided in the session

If you inadvertently lock the password, please notify the instructor.

- Activate the display of the “transaction code entry” field for easier navigation:
Go to Menu → Settings → Visualization.
Activate “Show OK Code field” as well as “Show dropdown lists with keys” and “Sort dropdown lists by their keys” and save.



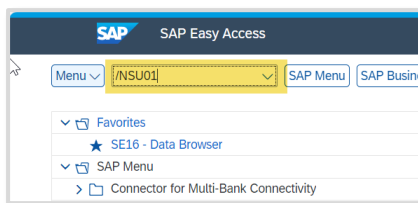
- Leave the menu. Your start screen should now show the transaction code entry field:



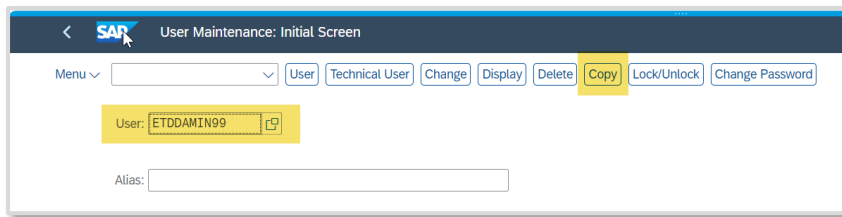
2.2 Creating a User With High Privileges

You will now conduct an action which triggers your first logs into *SAP Enterprise Threat Detection, public cloud*: creating a highly privileged user.

- In the transaction code entry, enter "SU01" (User Maintenance), and hit enter.



- In the User Maintenance transaction start screen, enter your user ETDADMIN## in the User field, and select "copy".



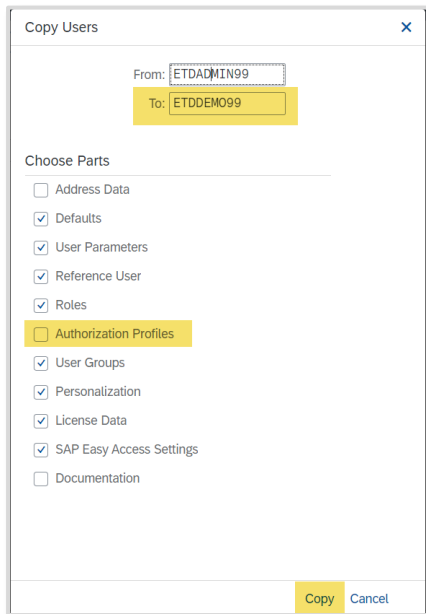
SAP User Maintenance: Initial Screen

Menu ▾ User Technical User Change Display Delete Copy Lock/Unlock Change Password

User: ETDDADMIN99

Alias:

- In the pop up screen, maintain the new user name “ETDDemo##” in the “To:” field; deselect the option to copy authorization profiles, and press “copy”:



Copy Users

From: ETDDADMIN99

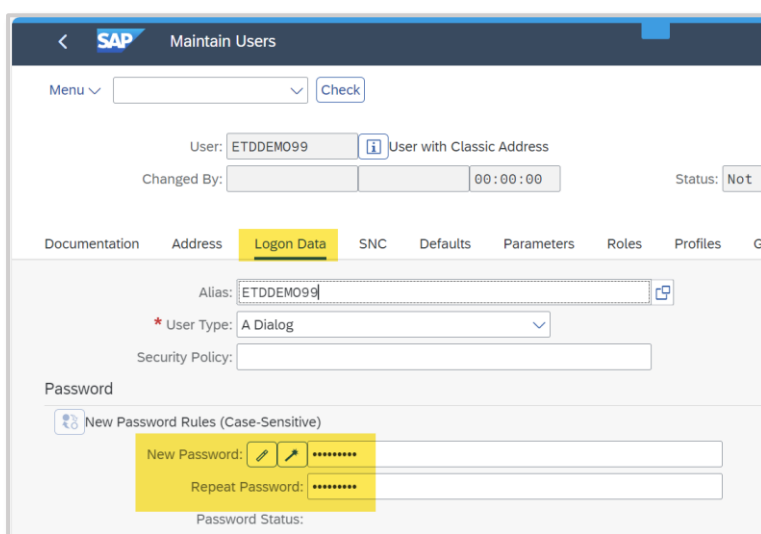
To: ETDDemo99

Choose Parts

- ☐ Address Data
- ☒ Defaults
- ☒ User Parameters
- ☒ Reference User
- ☒ Roles
- ☐ Authorization Profiles
- ☒ User Groups
- ☒ Personalization
- ☒ License Data
- ☒ SAP Easy Access Settings
- ☐ Documentation

Copy Cancel

- In the resulting screen set, on tab “Logon Data”, assign an initial (temporary) password (it is suggested to note down this password as you will need this to log on with ETDDemo##). Then save the user.



SAP Maintain Users

Menu ▾ Check

User: ETDDemo99 User with Classic Address

Changed By: 00:00:00 Status: Not s

Documentation Address Logon Data SNC Defaults Parameters Roles Profiles Gr

Alias: ETDDemo99

* User Type: A Dialog

Security Policy:

Password

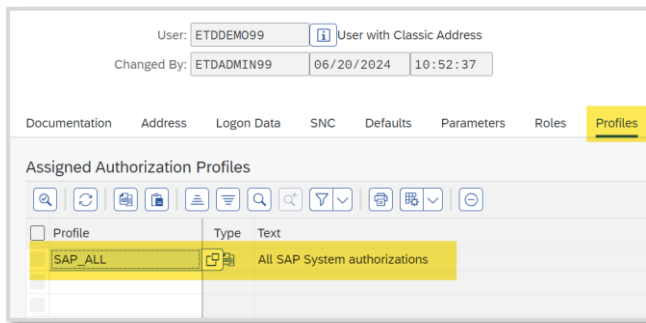
New Password Rules (Case-Sensitive)

New Password:

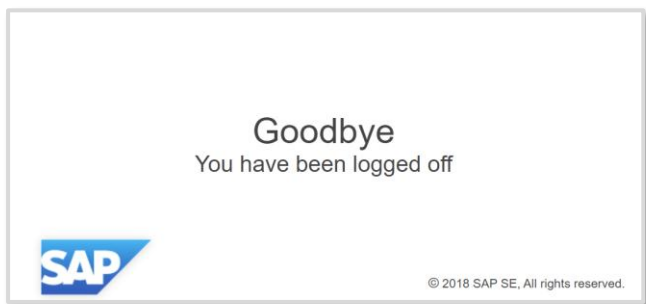
Repeat Password:

Password Status:

- Back in the SU01 initial screen, put in your user ETDDEMOxx and select the button “Change”. Move to the tab “Profiles”, add the profile “SAP_ALL” (making this user a super user basically without restrictions), and hit enter. Then press “Save”.



- This has been the first set of noteworthy actions. Exit the SAP Web GUI (button “Exit” in the top right; or hit Shift+F3; or in the transaction code entry field, type “/nex”).



3. Checking Alerts and Creating Investigations

You will now look at alerts in *SAP Enterprise Threat Detection, public cloud* and create an Investigation object out of it.

Return to the *SAP Enterprise Threat Detection, public cloud* Monitoring Console. If necessary, log on again with your user techedxx@etdsap.com, and in the Select Tenant app, select the tenant “Workshop Demo Customer”.

If you receive the ‘Select a Tenant’ popup, refer to section [1.1](#) how to resolve.

3.1 Check for Log Events

- Choose the app “Analyze Log Events” to check that your activities have generated log entries. Filter for your Admin user ETDADMIN##. If there are too many entries, additionally filter for semantic Events about “user” or “user admin” and you should see a shorter list.

- Note how the “user” column refers to the **ETDADMIN##** user as “acting”, but there is also an entry for “Target”: this is a pseudonym for your newly generated **ETDDemo##** user. Note down this pseudonym for later use.

- Choose the app “Manage Alerts”. The list should be populated with several recent entries. If yours is not in the system yet, give a little time – generation for these Alerts is triggered by a job every few minutes.
- Then, filter for your user ETDADMIN## in the Trigger Value 1 or 2 fields, and press “go”. Mark some Alerts you find relevant (or all), and in the bottom right corner, click on “Create Investigation”.

- In the ensuing “Create Investigation” screen, maintain a description referring to your demo ID so you can identify the object later. For “processor”, there are only few options available; just assign any email address.
- What else you enter is not of relevance in the demo flow. Of course, in a productive system these settings determine how the Investigation, if confirming a problem, will be made visible and which follow-on actions it triggers.
- Next, click on “Add and Show Investigation”.

You will then proceed to the main screen of the Investigation you have just created, resembling this example:

3.3 [Interpreting the Investigation Entries](#)

What is the meaning of the different parts of the Investigation object?

- In the Investigation screen, you will find the header information you have maintained before. You can choose to “edit” in case you wish to change the information.

- In the middle section, click on “Alerts”. Here, you can research the Alerts, have a look at some of the complete triggers explanation texts and how they codify the core findings in this text. You may also review some of the triggering Events.

ID	Pattern	Trigger	Events	Severity	Creation Time
132632	Logon from external with SAP stan...	Measurement 1 exceeded threshold 1 for ('Event...	View	High	2025/10/16 22:20:52 PM GMT+05:30
132624	Logon from internal with SAP stan...	Measurement 48 exceeded threshold 1 for ('System ID...	View	High	2025/10/16 21:43:31 PM GMT+05:30
132570	Logon from internal with SAP stan...	Measurement 39 exceeded threshold 1 for ('System ID...	View	High	2025/10/16 21:43:31 PM GMT+05:30
132563	Blocklisted transactions in producti...	Measurement 9 exceeded threshold 1 for ('Service,...	View	High	2025/10/16 21:43:31 PM GMT+05:30

Measurement 9 exceeded threshold 1 for ('Service, Transaction Name' = 'SU01', 'System ID, Actor' = 'S4H/100', 'User Pseudonym, Acting' = 'ETDADMIN11')

- In the Trigger text, you should also come across at least one additional user – in the form of a “User Pseudonym, Target”. Note down the pseudonym of this user (which you will later see refers to your ETDDEMO## user that was granted high level authorizations).
- In a real life scenario (but beyond the scope of a demo like this), user pseudonyms or other specific pointers like IP addresses, terminal ID/computer name etc. would be used to extend the search for alerts which are relevant for an investigation.
- Return to the tab “Actions”. Here, you may document anything - actions you have been performing, preliminary findings etc. and deductions these allow. These insights will be rendered in the investigation report later and can strongly increase the value and actionability of an investigation.

4. Trigger a Critical Action from SAP S/4HANA: Download of a Critical Database Table

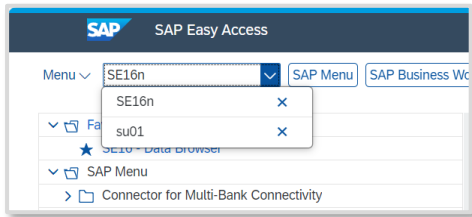
In this section, you will return into the role as a rogue actor and conduct several more actions resulting in Log Events flowing into *SAP Enterprise Threat Detection, public cloud*.

First, you need to log on to the SAP S/4HANA with the newly generated user ETDDEMO##.

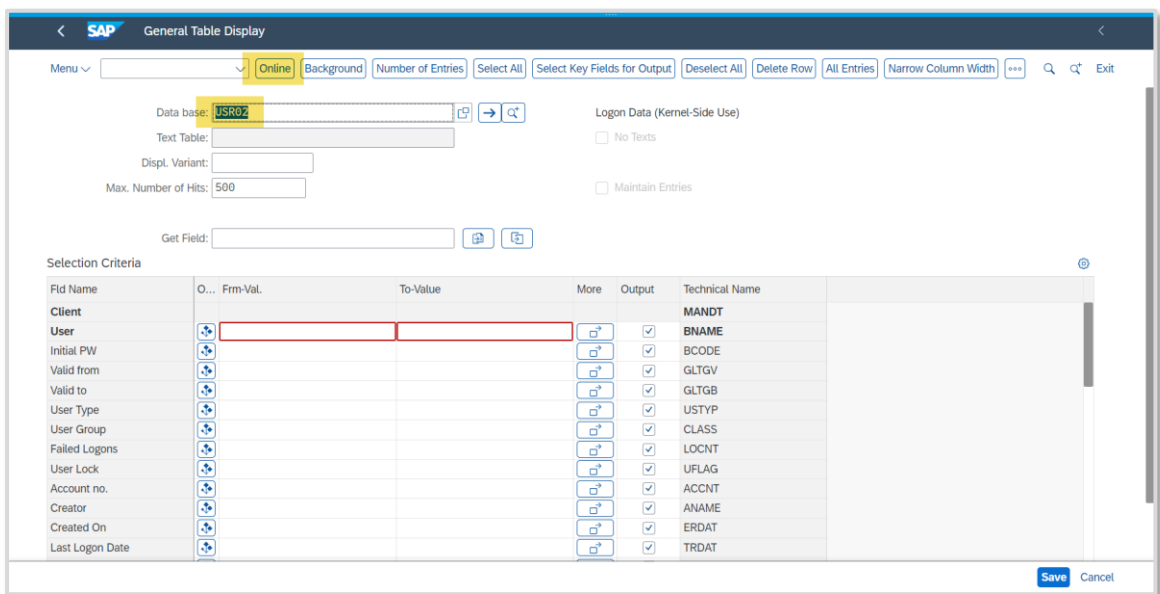
- In order to log on with your new user ETDDEMO##, you need to either open a new “incognito”/“private” session in your browser.
Alternatively, you may also switch to another browser.
Emptying the browser cache is also an option. Here, mark at least history, cookies, and password sections, then confirm).
- Now, call the Web Gui console <https://52.1.244.180:44301/sap/bc/gui/sap/its/webgui>, logon with your new user ETDDEMO## and the password you have chosen. At start, you need to set a new password (suggestion to take a note).

Executing a critical action:

- With the transaction code entry, navigate to transaction SE16N. This is a table display/download transaction (and a tool so powerful that it should generally not be made available in a productive system...).



- In the transaction, call table USR02. USR02 is a table which holds personal information (bad enough) and stores user password hashes (very critical: Although the passwords are hashed out, this would not stop a determined attacker. They may either crack simple passwords and, if they have identified out one single password from any user, they can take the respective hash value to overwrite the hashed password of any other user, allowing them to log on as that user i.e. impersonate the other user. Theoretically the password hashes should be “salted” however, in practice, this attack vector has been working quite reliably. (That said, think about the value of MFA and other tools independent from passwords).
- Access with the function “Online”:



- Search for your user ETDDMO## and display details. Check out Password Hash Value (real table attribute name PWDSALTEDHASH), towards the end of the table.
- Return to the table display and trigger a download with the icon “Export”, then choose “local file” and confirm the following two interactions. The file can be stored anywhere – in case you need to indicate a directory, pick any that you like.

Menu ▾ Refresh Display Selection Criteria Selection Criteria: Business View Display Selection as ABAP

Search in Table: USR02 Logon Data (Kernel-Side Use)

Number of Hits: 115

Runtime: 0 Maximum No. of Hits: 500

Insert Column:

User Name	Initial Password	Valid from	Type	User Group	Failed	Lock	Account number	Creator
BGRFCUSER	0000000000000000	10/04/2017	Service		0	0		BPINST
BGRFC_SUPER3	0000000000000000	11/03/2021	Service		0	0		BPINST
BPINST	0000000000000000		Dialog		0	0		DDIC
DDIC	0000000000000000		Dialog		0	0		
DELAY_LOGON	0000000000000000		Service		0	0		BPINST
DEMO01	0000000000000000		Dialog		0	0		ETDADMIN
DEMO02	0000000000000000		A Dialog		0	0		BPINST
DEVELOPER_5	0000000000000000		A Dialog		0	0		BPINST
ETDADMIN	0000000000000000		A Dialog		0	0		SAP*
ETDADMIN01	0000000000000000		A Dialog		0	0		ETDADMIN
ETDADMIN02	0000000000000000		A Dialog		0	0		ETDADMIN
ETDADMIN03	0000000000000000		A Dialog		0	0		ETDADMIN

You have conducted a seemingly simple but dangerous activity which should be resulting in at least one Alert in *SAP Enterprise Threat Detection, public cloud*.

Let's continue to retrieve and process them!

5. [User & Environment Behavioral Analysis – Identify the Critical Action in the Forensic Lab](#)

5.1 [Build up a Workspace](#)

5.1.1 [Assigning a Chart](#)

6. [From Workspace to Pattern to Alerts](#)

6.1 [Understanding Patterns](#)

7. [Finalize the Investigation](#)

7.1 [Information: Maintain your email ID to receive investigation reports](#)

7.2 [Finalize the investigation](#)

8. [Consumer/Processor role: Work with Investigation reports](#)

Thank you for your patience and hard work on this demo. We hope you liked this session and exercise!

For any feedback, please address your trainer, or product management:

SAP-ETD@sap.com