

# ESET – MSP-Kunden im PROTECT berechtigen

## Umfang dieser Anleitung

Diese kurze Dokumentation zeigt auf, wie ein MSP-Kunde mit speziellen Rechten eine Rolle im ESET PROTECT übernehmen kann. Dies kann zum Beispiel die Verwaltung der Berichte, oder die Erstellung neuer Installer, sein.

Die Grundberechtigung, damit ein Kunde überhaupt Zugriff auf den ESET PROTECT bekommt, wird im Dokument «**Neuen MSP-Testkunden anlegen**» eingehend erklärt.

Bild-01

Diese Dokumentation ist nicht abschliessend und zeigt ein paar Beispiele mit Zugriffrechten auf den ESET PROTECT. Weitere Informationen dazu finden sie unter dem nachfolgenden Link:

[https://help.eset.com/protect\\_cloud/de-DE/msp\\_users.html?msp\\_features.html](https://help.eset.com/protect_cloud/de-DE/msp_users.html?msp_features.html)

## ESET PROTECT Administrator ausführen

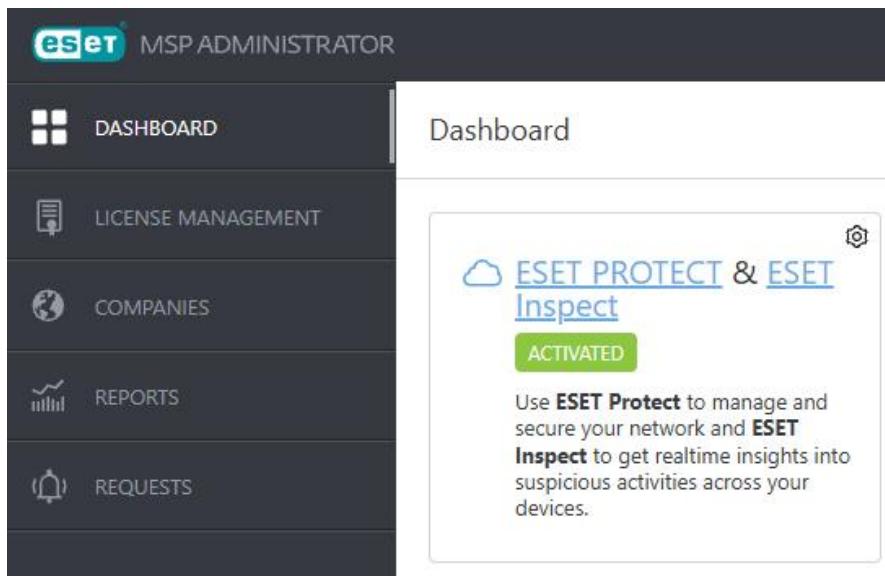


Bild-02

Die ESET PROTECT Konsole wird im MSP-Administrator über den Link im Dashboard aufgerufen. Bei einer Erstinstallation immer warten bis der grüne Button «**ACTIVATED**» erscheint.

Alternativ kann die ESET PROTECT Konsole auch über den nachfolgenden Link ohne sich vorgängig im MSP-Administrator anzumelden, aufgerufen werden:

<https://eu02.protect.eset.com/>

## ESET PROTECT Administrator – Permission Set erstellen

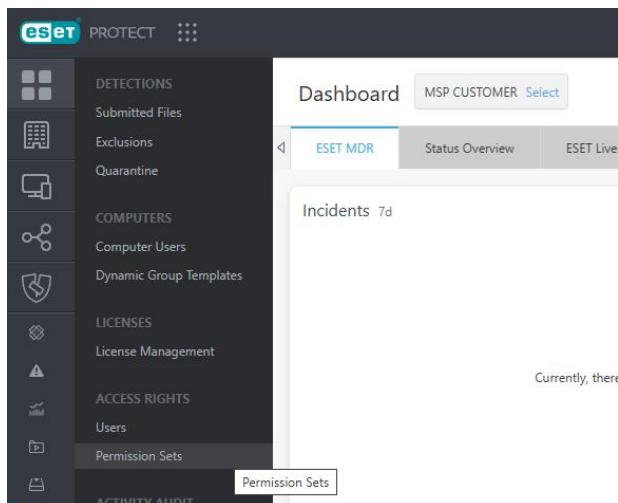


Bild-03

Die Permission Sets befinden sich im Bereich der «**ACCESS RIGHTS**». Wenn sie allerdings den Wizard, bzw. «**Start MSP customer setup**» bei einem neunen Kunden laufen lassen, wird automatisch ein Permission Set erzeugt.

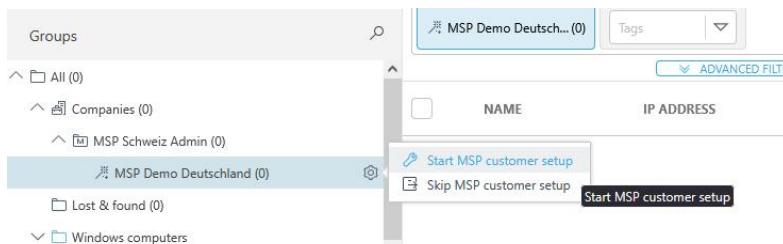


Bild-04

In dieser Anleitung erstellen wir ein Permission Set über das Menü. Klicken sie unten einfach auf den blauen Button «New». Danach geht die Maske auf und wir können das Permission Set konfigurieren.

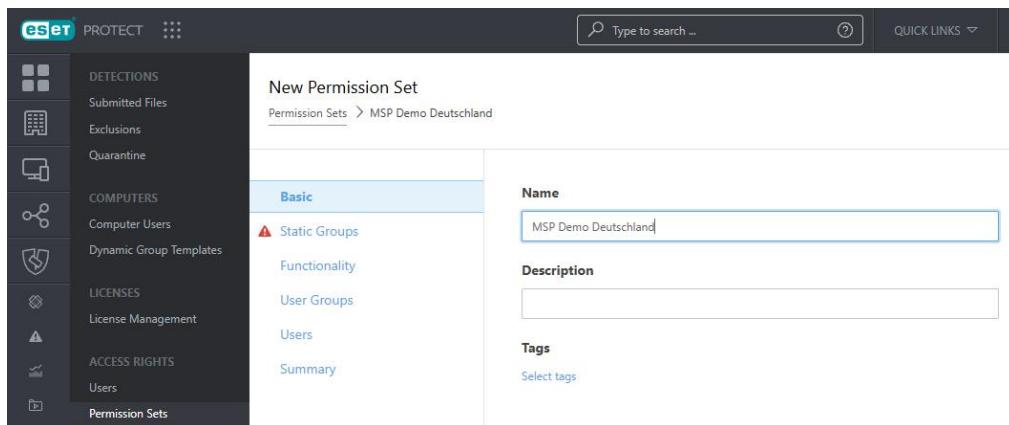


Bild-05

Vergeben sie hier immer einen eindeutigen Namen wie z.B. «**MSP Demo Deutschland**». Das hilft ihnen später den Kunden schneller zu identifizieren. Klicken sie danach auf «**CONTINUE**».

## New Permission Set

Permission Sets > MSP Demo Deutschland

The screenshot shows a user interface for creating a new permission set. On the left, there's a vertical navigation bar with options: Basic, Static Groups (which is highlighted with a blue background), Functionality, and User Groups. The main area has a heading 'Permission sets are applied only to group where you want to apply'. Below it, under 'Static groups', there's a note 'Select or Create new group' with a warning icon. The overall background is white with light gray horizontal lines separating sections.

Bild-06

Wählen sie hier die statische Gruppe des Kunden aus. Also immer die Stammgruppe des Kunden, welche automatisch durch den MSP-Administrator erzeugt wurde und sich im ESET PROTECT wiederspiegelt.

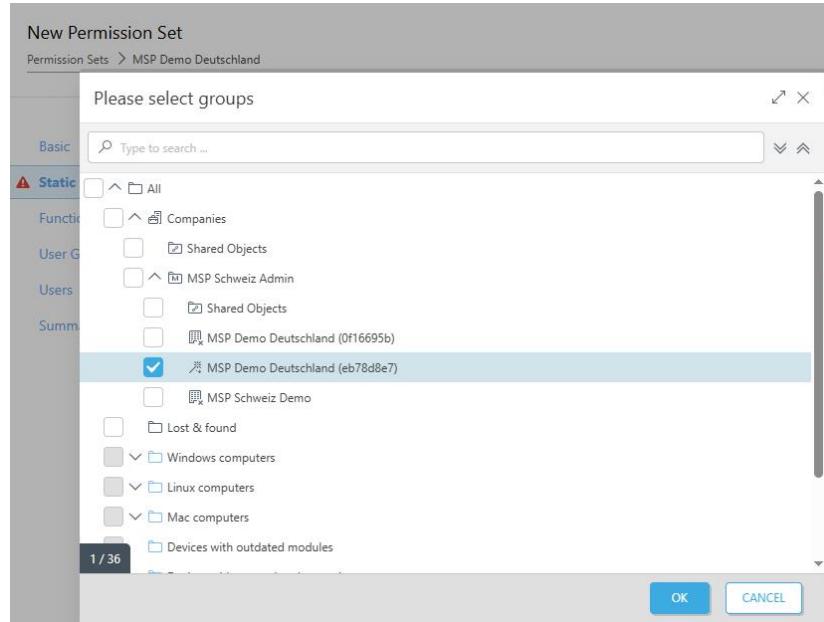


Bild-07

Klicken sie danach auf «CONTINUE». Nun müssen wir die Berechtigungen individuell für den Kunden festlegen.

New Permission Set

Permission Sets > MSP Demo Deutschland

Basic	Functionality Privileges																																																				
Static Groups	<b>All Functionality</b> ⓘ																																																				
User Groups	Clear Access																																																				
Users	Grant All Functionality Read Only																																																				
Summary	Grant All Functionality Use Access																																																				
	Grant All Functionality Full Access																																																				
	<b>Granted Functionality</b> ⓘ																																																				
	<table border="1"> <thead> <tr> <th></th> <th>Read</th> <th>Use</th> <th>Write</th> </tr> </thead> <tbody> <tr> <td>Groups &amp; Computers</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Permission Sets</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Mapped accounts</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Stored Installers</td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>Server Tasks &amp; Triggers</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Client Tasks</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Dynamic Groups Templates</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Encryption recovery</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Reports and Dashboard</td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Policies</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Send Email</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>Licenses</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table>		Read	Use	Write	Groups & Computers	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Permission Sets	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Mapped accounts	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Stored Installers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Server Tasks & Triggers	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Client Tasks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Dynamic Groups Templates	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Encryption recovery	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Reports and Dashboard	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Policies	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Send Email	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Licenses	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Read	Use	Write																																																		
Groups & Computers	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																																																		
Permission Sets	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																																																		
Mapped accounts	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																																																		
Stored Installers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>																																																		
Server Tasks & Triggers	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																																																		
Client Tasks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																																																		
Dynamic Groups Templates	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																																																		
Encryption recovery	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																																																		
Reports and Dashboard	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>																																																		
Policies	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																																																		
Send Email	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																																																		
Licenses	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																																																		
	<input type="button" value="BACK"/> <input type="button" value="CONTINUE"/> <input type="button" value="FINISH"/> <input type="button" value="CANCEL"/>																																																				

Bild-08

In diesem Beispiel erlauben sie dem Kunden «**Gruppen & Computer**» zu sehen. Das bezieht sich natürlich nur auf seine Umgebung!

Sie erlauben ihm auch selbständig neue «**Installer**» zu erstellen. Hierzu müssen sämtliche Berechtigungen wie Read-Use-Write vergeben werden.

Im Bereich «**Reports and Dashboard**» erlauben sie dem Kunden, sie zu lesen und zu benutzen. Sie geben ihm kein «**Write**» Berechtigung, so dass er sie auch nicht verändern kann.

Bei den «**Policies**» vergeben sie nur das «**Read**» Recht. Der Kunden kann den Inhalt der Policies sehen, er darf sie aber keinem Computer zuweisen oder verändern.

Mit «**FINISH**» wird das Permission Set erstellt und der Stammgruppe des Kunden zugewiesen.

Sie als Reseller müssen entscheiden, wie hoch sie einen Kunden berechtigen. Bitte bedenken sie, je höher, desto mehr Konfigurationsfehler können entstehen, was ihnen einem höheren Supportaufwand generiert.

## Kunden Benutzer aus dem MSP-Administrator importieren

The screenshot shows the ESET PROTECT web interface. On the left, there's a sidebar with various navigation options like 'DETECTIONS', 'LICENSES', and 'ACCESS RIGHTS'. The main area is titled 'Users' and shows a list of 'Mapped accounts'. A specific entry, 'Patrik Werren', is selected. A modal window titled 'Tags' is overlaid on the interface, containing a single tag entry: 'MSP Demo Deutschland'. At the bottom right of the modal, there are buttons for 'ACTIONS' and 'ADD NEW...'. A red 'CLOSE' button is located at the bottom left of the modal.

Bild-09

Der Import geschieht im ESET PROTECT über den Bereich «**Users**» / «**Mapped accounts**».

Klicken sie hierzu ganz unten auf «**ADD NEW...**»

New mapped account  
Users > New mapped account

**Basic**

**Account identifier**  
Name  
Home group  
Automatically selected based on assigned permission sets

**Account**  
Enabled

Bild-10

Nun erschein die Maske mit den Mapped account, klicken sie auf «**SELECT**».

Please select item

NAME	COMMENT	REFERENCED DOMAIN
<input checked="" type="checkbox"/> MSP Demo Deutschland	msp-dmo@werren.com	EMA

Bild-11

Hier erscheinen alle Benutzer welche sie im MSP-Administrator angelegt haben. In diesem

Fall wählen wir «**MSP Demo Deutschland**» aus.

Bild-12

Der «**Account identifier**» wird ihnen danach immer kryptisch mit einem HASH-Wert angezeigt. Dadurch ist garantiert, dass kein falscher Benutzer auf ihrer Umgebung berechtigt wird.

Es könnte ja durchaus sein, dass ein anderer Reseller im MSP-Administrator einen Benutzer mit exakt dem gleichen Namen anlegt. Durch den HASH-Wert ist die Zuweisung eindeutig sichergestellt.

Bild-13

Im nächsten Schritt im Bereich «**Permission Sets**» wählen sie das zuvor für den Kunden erstellt Permission Set aus.

Im Anschluss können sie direkt auf «**FINISH**» klicken.

Der Benutzer ist nun im ESET PROTECT importiert und hat seine Berechtigungen erhalten.

## Anmeldung als «Kunde» an der ESET PROTECT Konsole



Bild-14

### Log in

Email

Password

**LOG IN**

[Forgotten password](#)

Or

 [Sign in with Microsoft](#)

Um den Zugang zu testen, kann sich der Kunde nun an dem ESET PROTECT anmelden. Wenn sie alles richtig konfiguriert haben, wird er seine Stammgruppe sehen, aber sonst auf keinerlei Element im ESET PROTECT zugreifen können.

Als zusätzliche Sicherheit könnten sie bei den Kunden auch noch die ESET 2FA aktivieren!

## Elemente in der ESET PROTECT Konsole zuweisen

The screenshot shows the ESET PROTECT console interface. The left sidebar has a dark theme with white icons and text. The main area is titled 'Berichte' (Reports). At the top of the main area, there are tabs for 'Kategorien & Templates' and 'Geplante Berichte'. Below these are filters for 'ZUGRIFFSGRUPPE' (Access Group) with a dropdown menu 'Auswählen' (Select) and 'Tags...' (Tags), and a search bar 'Zu suchender Typ...' (Type to search). The main content area is titled 'Schwachstellen- und Patch-Management' (Weak Point and Patch Management). It contains two cards: 'Übersicht über das Patch-Management' (Overview of Patch Management) and 'Übersicht über Schwachstellensca...' (Overview of Weak Point Scans). Both cards have small descriptions below them.

Bild-15

Durch das importieren des Benutzers aus dem MSP-Administrator, die Erstellung eines Permission Set und der Zuweisung zu der Stammgruppe, ist es dem Benutzer nun möglich sich an der ESET PROTECT Konsole anzumelden.

An dieser Stelle hat er aber noch überhaupt keinen Zugriff auf Elemente wie Berichte, Policies usw.

Diese müssen sie als Reseller zuerst erzeugen und dann dem Kunden zuweisen.

## Elemente in der ESET PROTECT Konsole zuweisen

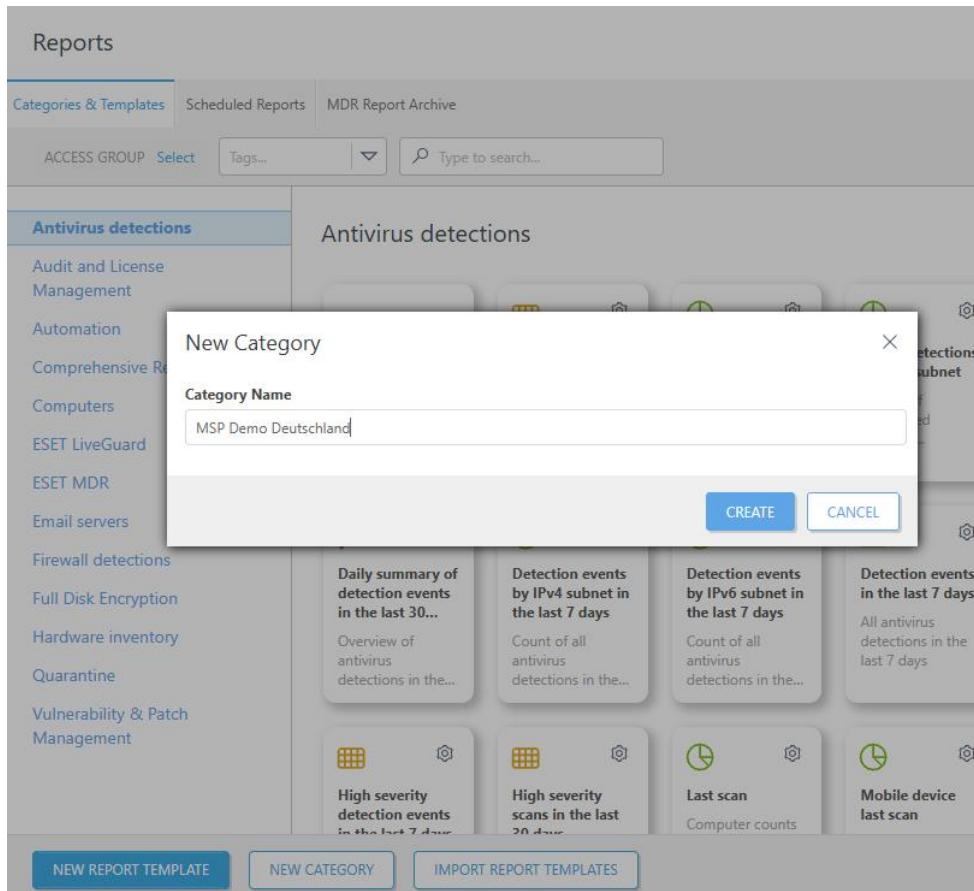


Bild-16

In diesem Beispiel erzeugen wir eine neue Kategorie im Bereich der Berichte. Duplizieren einen bestehenden Bericht und weisen diesen dem Kunden zu.

Klicken sie hierzu im Bereich der Berichte unten auf den Button «**NEW CATEGORY**». Vergeben den Namen und klicken dann auf «**CREATE**».

Vergeben sie einen eindeutigen Namen wie in diesem Beispiel «**MSP Demo Deutschland**». Wenn sie vor den Namen das Sonderzeichen # verwenden, werden die Berichte immer ganz oben in der Struktur angezeigt. >>> **#MSP Demo Deutschland**

## Bericht im ESET PROTECT duplizieren und dem Kunden zuweisen

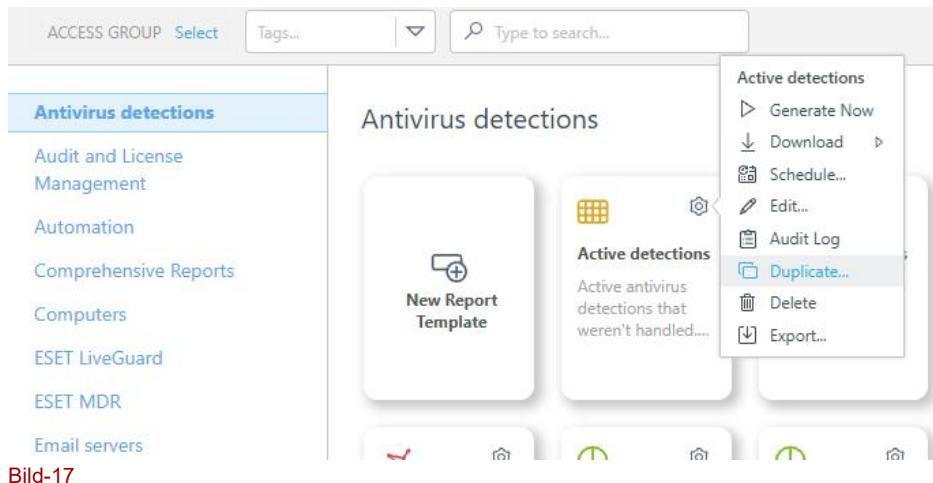


Bild-17

In diesem Beispiel duplizieren wir einen Standard Bericht und weisen ihn dem Kunden zu.

Wählen sie irgendeinen Bericht im ESET PROTECT aus und klicken mit der rechten Maustaste auf das Zahnrad. Wählen sie dann im Kontextmenü «**Duplicate**» aus.

In diesem Beispiel duplizieren wir den Bericht «**Active detections**».

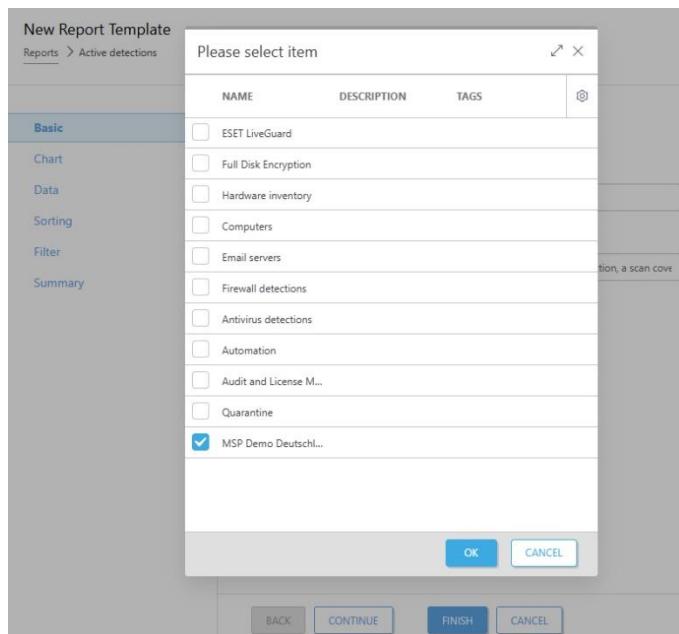


Bild-18

Im nächsten Schritt weisen sie den duplizierten Bericht der vorgängig erzeugten neuen Berichtskategorie «**MSP Demo Deutschland**» zu und klicken auf «**OK**».

New Report Template

Reports > Active detections

**Basic**

Chart

Data

Sorting

Filter

Summary

**Basic**

**Name**  
Active detections

**Description**  
Active antivirus detections that weren't handled. To resolve an active detection, a scan cove...

**Tags**  
Select tags

**Category**  
MSP Demo Deutschland

Bild-19

In der Zusammenfassung sehen sie nun alle Details und dass der duplizierte Bericht der Kategorie «**MSP Demo Deutschland**» zugewiesen wird.

Berichte

Kategorien & Templates Geplante Berichte

ZUGRIFFSGRUPPE Auswählen Tags... Zu suchender Typ...

**MSP Demo Deutschland**

Schwachstellen- und Patch-Management

**MSP Demo Deutschland**

Active detections  
Active antivirus detections that weren't handled. ...

Bild-20

Der duplizierte Bericht erscheint nun im der Kategorie «**MSP Demo Deutschland**».

Damit der Kunde nun auch auf die neue Kategorie «**MSP Demo Deutschland**» zugriff hat, bzw. sie in seiner Umgebung sieht, müssen sie die Kategorie verschieben.

## Bericht Kategorie zum Kunden verschieben

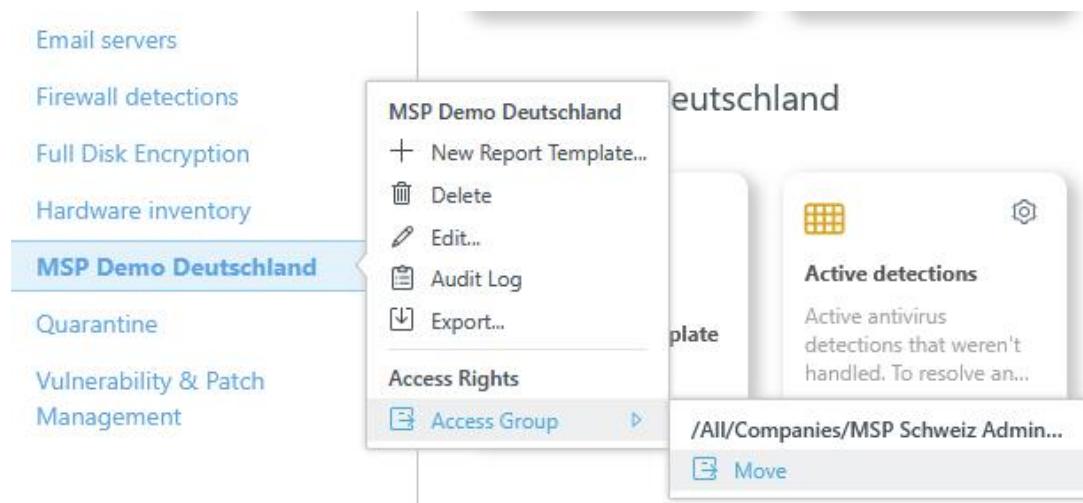


Bild-21

Hierzu klicken sie in der Berichtskategorie auf das Zahnrad mit der Maustaste, danach öffnet sich das Kontextmenü.

Gehen sie ganz runter auf **Access Rights > Access Group >** und wählen «**Move**»

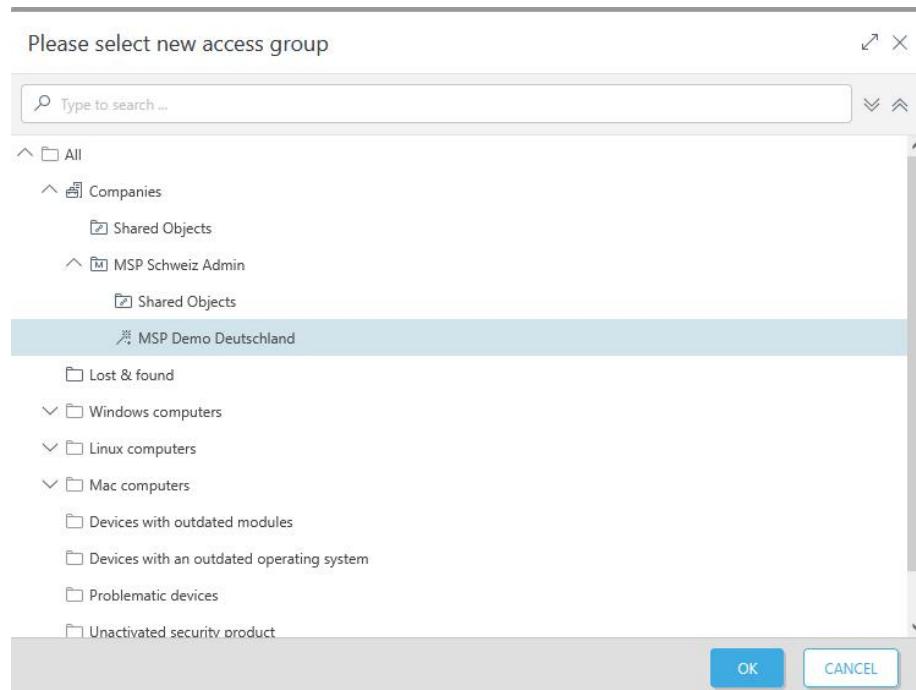


Bild-22

Selektieren sie dann die Stammgruppe des Kunden «**MSP Demo Deutschland**» und klicken auf OK.

Damit wird die Kategorie dem Kunden zugewiesen und er kann sie in seiner ESET PROTECT Umgebung sehen. Sämtliche Berichte die nun dupliziert werden und seiner Kategorie zugewiesen werden, sind dann für den Kunden sichtbar.

## Berichte

Kategorien & Templates Geplante Berichte

ZUGRIFFSGRUPPE Auswählen Tags... Zu suchender Typ...

**MSP Demo Deutschland**  
Schwachstellen- und Patch-Management

**MSP Demo D**

**Active detections**  
Active antivirus detections that weren't handled. ...

Active detections  
Jetzt generieren  
Herunterladen  
Herunterladen als  
Planen...  
Bearbeiten...  
Audit-Log  
Duplizieren...  
Löschen  
Exportieren...

Herunterladen

Herunterladen als

CSV (nur Tabellendaten)

Bild-22

Der Kunde kann nun aufgrund des Permission Set den Bericht als PDF oder CSV herunterladen und Exportieren.

## Fazit

Sämtliche Elemente wie Berichte, Policies, dynamische Gruppentemplates usw. lassen sich auf diesem Weg einem Kunden zuweisen. Das Vorgehen ist immer das gleiche.

Damit können sie eine massgeschneiderte Mandantenumgebung für ihre Kunden erstellen.