

# FileWall<sup>TM</sup> for Microsoft 365 Exchange Online מדריך למשתמש



# תוכן עניינים

3	1 הקדמה
4	2 פתרון הFileWall של SileWall
4	2.1 סקירה כללית
4	2.2 סוגי הקבצים הנתמכים
4	2.3 חווית משתמש
6	3 הפעלת שירות FileWall
8	4 הפעלת משתמשים ראשונית
10	5 ממשק ניהול – סקירה5
11	6 ממשק הניהול- Dashboard
11	6.1 חלונית סקירה כללית
13	
15	6.3 הודעות מערכת
16	7 הגדרות ניהול
16	User Management ניהול משתמשים- 7.1
17	Policy Management ניהול מדיניות- 7.2
18	
23	7.2.2 הוספת מדיניות
24	7.2.3 מחיקת מדיניות
24	7.3 הגדרות כלליות- Settings
24	הרשאת כניסה להודעות דוא"ל מקוריות
25	8 הודעות דוא"ל- Email Messages.
27	8.1 צפייה בפרטי צרופה
27	8.2 שחזור קבצים מקוריים
28	8.3 הסרת קובץ מ- Quarantine



# 1 הקדמה

FileWall הינו תוסף הגנה לתיבות הדואר של מיקרוסופט 365. FileWall מונע חדירת נוזקות לארגון על ידי נטרול הקוד זדוני המסתתר בקבצי צרופות בהודעות הדואר האלקטרוני הנסרקות על ידי השירות.

FileWall מבוסס על טכנולוגיית הלבנת קבצים מבית חברת אודיקס הנקראת ™TrueCDR (Content Disarm and Reconstruction). הטכנולוגיה של odix מוטמעת בארגונים רבים והוכחה כיעילה במניעת מתקפות המועברות באמצעות קבצים זדוניים. טכנולוגיית פטנט זו סורקת, מפרקת ובונה מחדש קבצים הנמצאים בשימוש יומיומי לקבצים בטוחים לשימוש הנקיים מנוזקות.

חברת אזטק בשיתוף עם אודיקס מספקת ללקוחותיה רשיונות OEM הניתנים ללא עלות לשנת 2021.

מדריך משתמש זה מיועד ללקוחות אזטק וכולל הסבר על הפעלת השירות ותפעולו השוטף.

פניות בנושא תמיכה במוצר ניתן להפנות ל: support@aztek.co.il

מסמך זה מנוסח בלשון זכר אך פונה לכלל המינים.



# 2 פתרון הFILEWALL של 2

# 2.1 סקירה כללית

תהליך סריקת הקבצים של odix מסיר ומנטרל את כל הנוזקות, ידועות ובלתי ידועות, המוסתרות בקבצים. תהליך הסריקה מטפל בסוגים שונים של קבצים ומשתמש באלגוריתם מתמטי ייחודי המותאם לכל סוג קובץ. התהליך מתבצע ברקע ללא הפרעה לשימוש השוטף בדואר האלקטרוני.

הקבצים המולבנים שעברו את תהליך הסריקה אינם עוברים המרת פורמטים אלא נשארים זהים לפורמט המקורי (לדוגמא: קובץ אקסל ישאר זהה בפורמט ולא יעבור המרה ל-csv).

תהליך ההלבנה מבצע ניטרול של קודים וכך מבטא את התכונה החזקה ביותר של פתרון ה- odix הוא יכולתו להתמודד עם איומים לא ידועים או איומים עתידיים שבהן פתרונות מדור הקודם נופלים.

לאחר שזוהתה צרופה לדוא"ל, תהליך החיטוי כולל את השלבים הבאים:

- אכיפת מדיניות על כל משתמש חלה מדיניות הקובעת את סוגי הקבצים רשאים/לא
   רשאים להיכנס לתיבת הדואר שלהם. ארגון יכול להחיל מספר מדינויות המגדירות "רשימות שחורות" ו"רשימות לבנות " של סוגי קבצים ואת הפעולות הננקטות על צרופות.
  - הלבנה שלב החלת אלגוריתם ההלבנה (TrueCDR). FileWall מנטרל את הקוד הזדוני
     ומספק עותק מולבן לשימוש בטוח.

. **הערה:** אם FileWall מזהה קובץ פגום, המערכת חוסמת אותו

### 2.2 סוגי הקבצים הנתמכים

FileWall תומך בחיטוי של כל סוגי הקבצים הנפוצים ביותר הכוללים קבצי PDF, קבצי Office, תמונות וארכיב.

**הערה:** בתרחיש בו הודעת דוא"ל מכילה צרופה מסוג קובץ שאינו נתמך, שירות FileWall לא יבצע הלבנה לקובץ ויציג הודעה בגוף ההודעה המציינת כי הקובץ לא עבר הלבנה ויש לפתוח את הקובץ בזהירות.

### 2.3 חווית משתמש

לאחר הפעלת השירות, כל הצרופות המגיעות לתיבות הדואר של מייקרוסופט 365 בארגונך יעובדו ע"י אודיקס, אין זה משנה אם השימוש בתיבת הדוא"ל של אופיס הוא בדפדפן, בשולחן העבודה או בסמארטפון. הזמן הנדרש לעיבוד תלוי במספר הצרופות וגודלן, עם זאת בדרך כלל העיבוד נמשך שניות ספרות פחות מדקה.

לאחר סיום העיבוד, התוצאות יוצגו בבאנר בצבע בהתאם לסטטוס: ירוק (הצלחה), כתום (לא חוטא), אדום (חסום), צהוב (כשל בשירות), אפור (הודעה מקורית שוחררה/ שוחזרה).

קישור More info נמצא בקצה הימני של הבאנר בכדי להציג מידע נוסף.



### צרופות מולבנות

לאחר חיטוי **מוצלח** של צרופות, מוצג באנר ירוק בראש גוף ההודעה:

Attachments were sanitized by FileWall FileWall some elements have been removed

תהליך נטרול הצרופות הושלם בהצלחה.

#### צרופות לא מחוטאות

במקרה שלא ניתן היה לבצע חיטוי של הצרופות, מוצג באנר כתום בראש גוף ההודעה:

Attachments were not sanitized by FileWall

תרחיש זה יכול לקרות אם סוג הקובץ אינו נתמך או אם הוגדרה מדיניות לעקוף נטרול סוג קובץ הזה.

#### צרופות חסומות

במידה וצרופה נחסמת, בראש גוף ההודעה יופיע באנר אדום עם פרטים לסיבת החסימה. לדוגמא, אם הFileWall קבע שהצרופה חשודה, לא מהסוג המורשה לפי המדיניות, או אם מבנה הקובץ אינו תואם את סוג סיומת הקובץ.

3 suspicious attachments were removed by FileWall contact your administrator

#### כשל בשירות

במידה והתרחש כשל בשירות, באנר צהוב יוצג בראש גוף ההודעה:

System error by FileWall

לחץ על הקישור ל**More info** בקצה הימני של הבאנר כדי להציג מידע נוסף. הצרופות לא חוטאו במקרה זה.

### ההודעה המקורית שוחררה/שוחזרה

אם הודעה מקורית (כולל קבצים מצורפים שלה) שוחררה/ שוחזרה, מוצג באנר אפור בראש גוף ההודעה:

Attachments were Restored by FileWall open the attachments with caution

Attachments were Released by FileWall open the attachments with caution



# 3 הפעלת שירות FILEWALL

- 1. לחץ על לינק אתחול ה-FileWall שנשלח אליך במייל ע"י אזטק.
  - ." Accept" דף אישור הרשאות הבא יוצג לפניך, לחץ על.





יופיע, התחבר באמצעות משתמש המייקרוסופט FileWall איסך הכניסה למערכת ניהול 50 אופיע, התחבר באמצעות משתמש המייקרוסופט שלך.



. המתן מספר שניות, והמסך הבא יפתח אוטומטית.



במידה והמסך לא מתקבל תוך מספר דקות, אנא נסו שוב לאחר שעתיים.



# 4 הפעלת משתמשים ראשונית

- 1. הפעלת משתמשים ראשונית מתבצעת דרך ממשק הניהול בפורטל <u>https://app.filewall.com</u>
- 2. הכניסה לממשק הניהול מתבצעת עם שם המשתמש והססמא של Microsoft.
  - המסך הראשי של ממשק הניהול המוצג לאדמניסטרטור הינו המסך הבא.



- 4. להפעלת משתמשים, בחר "User Management" בתפריט הראשי (המופיע באייקון 📩 )
  - 5. הפעל את חשבונות המשתמשים עבורם תרצה להפעיל את שירות ה-FileWall.

	ntormation	25/30							
Q Sear	ch								\$
	Status	Name	Email	Groups	Department	Role	Policy	Admin	
8	•	test	test@odixtests.onmicrosoft	odixtests	R&d	Råd	Default Policy	No	
0	•	test1	test1@odixtests.onmicrosof	NewGroup odixtests			Default Policy	Yes	
	•	test2	test2@odixtests.onmicrosof	odixtests	R&d	Backend Cdr Developer	Default Policy	No	
8	•	test3	test3@odixtests.onmicrosof	NewGroup odixtests			Default Policy	No	
8	•	test4	test4@odixtests.onmicrosof	odixtests	R&d	Developer	Default Policy	No	
0	•	test5	test5@odixtests.onmicrosof	odixtests			Default Policy	Yes	
8	•	test6	test6@odixtests.onmicrosof	NewGroup odixtests	Qa	Qa	Test	Yes	
0	•	test7	test7@odixtests.onmicrosof	NewGroup odixtests		Qa	Default Policy	Yes	
		Q Search	Status         Name           Status         Name           East         test           East         test2           East         test3           East         test5           East6         test6           East6         test7	Status     Name     Email       Status     Name     Email       Status     test     test@adiktests.onmicrosoft       Status     test2     test2@odiktests.onmicrosoft       Status     test3     test3@odiktests.onmicrosoft       Status     test3     test4@odiktests.onmicrosoft       Status     test3     test4@odiktests.onmicrosoft       Status     test4     test4@odiktests.onmicrosoft       Status     test5     test5@odiktests.onmicrosoft       Status     test6     test6@odiktests.onmicrosoft       Status     test6     test6@odiktests.onmicrosoft	Status         Name         Email         Groups           1	Status         Name         Email         Groups         Department           1<	Satur         Nume         Email         Grups         Department         Role           1	Statu       Nume       Email       Orups       Dipatment       Role       Alois       Default Policy         • <t< td=""><td>R sach       Statu       Name       Enal       Grups       Department       Role       Polizy       Admin         I bit       Mark       Edgodistessammicroad:       Galessit       Rad       Rad       Balaco       Default Polizy       Mark       Default Polizy       Rad       Rad       Rad       Default Polizy       Rad       Ra</td></t<>	R sach       Statu       Name       Enal       Grups       Department       Role       Polizy       Admin         I bit       Mark       Edgodistessammicroad:       Galessit       Rad       Rad       Balaco       Default Polizy       Mark       Default Polizy       Rad       Rad       Rad       Default Polizy       Rad       Ra



6. על מנת שתוכל לאמת שהשירות אכן פועל, שלח דוא"ל עם קובץ צרופה לבחירתך אל משתמש שהפעלת בשלב הקודם. כאשר הודעת הדוא"ל מגיעה לתיבת הדואר הנכנס, יוצג באנר של FileWall בחלק העליון של גוף ההודעה (טקסט וצבע הבאנר עשויים להשתנות בהתאם לקובץ המצורף שנשלח). עיבוד ההודעות עשוי להימשך מספר שניות, אם אינך רואה את הבאנר בהודעה לאחר דקה אנא פנה לתמיכה: support@aztek.co.il





# 5 ממשק ניהול - סקירה

פונקציות הניהול של FileWall מאורגנות בתוך הדפים הראשיים:

- לוח בקרה- מספק ייצוג של פעילות המערכת, הכולל בתוכו נתונים סטטיסטיים על הודעות <u>לוח בקרה-</u> מספק ייצוג של פעילות המערכת הכולל בתוכו נתונים סטטיסטיים על הודעות סרוקות וקבצי הצרופה בהם, הודעות מערכת וציון אבטחה.
  - ע"י ה- Quarantine הודעות שעובדו ו/ או הועברו לQuarantine ע"י ה- אודעות דוא"ל- מציג רשומות של ההודעות שעובדו ו/ או הועברו לקטי הצורך. FileWall
- ניהול מדיניות- מאפשר הגדרת כל המאפיינים הנחוצים של המדיניות הקשורים לביצוע תהליך הסריקה והחיטוי, כולל קביעת אילו סוגי קבצים מותרים או חסומים, ואילו פעולות נטרול מוחלות. באפשרותך לצפות במאפייני מדיניות ברירת המחדל וליצור מדיניות חדשה בהתאם לצרכי הארגנך.
- למשתמשים בארגונך. כברירת מחדל, FileWall ניהול משתמשים בארגונך. כברירת מחדל, כלל משתמשים בארגונך מאפשר ניהול מימוש ה-365 בארגונך מופיעים בדף המשתמשים. עליך להפעיל משתמשים על מנת שה-FileWall יוכל לעבד את קבצי הצרופה לדוא"ל שלהם.
  - אפשר קביעת הגדרות מערכת הקשורות לגישת המשתמשים להודעות דוא"ל 🔹 🔹 מקוריות ולקבצי הצרופות בהם. הגדרות נוספות יתווספו בגרסה עתידית.



# 6 ממשק הניהול- DASHBOARD

לוח הבקרה מוצג בכל פעם שאתה מתחבר לFileWall.

JIUIISIUS							This Month
File Turner	Sonitization Parulte		T (( -				
The types	Sumizarion resums		frame			O Message	Attachments
• 2 Other		• 2 Blocked (by Policy)	3				/
• 1 Powerpoint	-	1 Sanitized	2				
5	3	)	1				
			01/01 01/01	1 02/01	03/01	05/01	06/01 0
Top Insights							New
Top Insights			Risky User (2)				New
Top Insights General (15) Taday			Risky User (2)				New
Top Insights General (15) Today High risk files (2) delivered.	07.0	n.2021 10:02 (Dismise)	Risky User (2)				New
<b>Top Insights</b> General (15) Today High risk files (2) delivered.	07.0	1.2021 10:02 (Diamise)	Risky User (2)				New

# 6.1 חלונית סקירה כללית

<b>Overview</b> All time	29	07	୍ୟ <b>17</b>	<b>85%</b> Security score

חלונית הסקירה כללית יציג את הפרטים הבאים:



- מספר צרופות דוא"ל אשר נסרקו 🕛 🔸
- מספר משתמשי תיבות הדואר של מייקרוסופט 365
  - ציון האבטחה המצטבר 🔘 85%

באפשרותך להרחיב את החלונית באמצעות לחיצה על 💴



החלונית תציג כעת את הפרטים הבאים:

- מספר הודעות הדוא"ל אשר נסרקו: 🔛 🛛
  - עם צרופות
  - ללא צרופות
- מספר צרופות דוא"ל אשר נסרקו ותוצאות הסריקה: 🔍 🛛
  - מחוטא (נפתר) 🗹
- (סוג הקובץ אינו נתמך או שלא נוטרל ע"י המדיניות 🕖
  - חשוד (הקובץ צרופה זוהה כחשוד ועל כן נחסם ע"י השירות) 🥹
    - י 🙋 נחסם (הקובץ צרופה נחסם ע"י מדיניות אדמין)
- סה"כ משתמשי תיבות הדואר של מייקרוסופט 365 אשר האימיילים שלהם 🛚 🖉 נסרקו:
  - ממוצע מספר הודעות דוא"ל למשתמש 🔛 🚽
  - ממוצע מספר קבצי צרופה סרוקים למשתמש 🏼 🕛

. מורשים Active Exchange online הערה: הממוצע נקבע ע"י מספר משתמשי תיבות הדואר



.FileWall ציון האבטחה המצטבר נקבע על סמך הלוגיקה והחישובים של ה חישוב ציון האבטחה תלוי במדיניות שנקבעה לארגונך.



# 6.2 סטטיסטיקה

כברירת מחדל, הנתונים בחלק של הסטטיסטיקה בלוח הבקרה מציגים את הפעילות בשבוע



בתפריט נפתח מצד ימין למעלה ניתן לשנות את תקופת הזמן עליו תרצו לראות את הסטטיסטיקה (השבוע הנוכחי, החודש הנוכחי, 30 הימים האחרונים, 7 הימים האחרונים).

החלק הסטטיסטי כולל את רכיבי הנתונים הגרפיים הבאים:

סוג קובץ: מציין את התפלגות הקבצים, לפי סוג, שנסרקו.



**תוצאות ההלבנה:** מציין את מספר הקבצים שהולבנו לפי תוצאות הסריקה.







### **. תעבורה:** מציין את רמת התעבורה של הודעות דוא"ל ושל קבצי צרופה.

באפשרותך להציג את הנתונים של הודעות דואר ו/ או קבצי צרופה יחד או בבידוד על ידי בחירה או ניקוי האפשרויות מיד מעל לתרשים. העבר את העכבר מעל נקודה בגרף

25/01 Messages 5 Attachments 7



# 6.3 הודעות מערכת

אזור ה- Top Insights מכיל הודעות מערכת אודות פעילות בדבר קבצים חשודים, וקטורי תקיפה שזוהו וכל תרחיש שזוהה כחריג ומצריך אזהרה מטעם המערכת.

כברירת מחדל, הרשימות כוללות את כלל ההודעות. באפשרותך לסנן את הרשימות ע"י בחירה; חדש (**New**) או נפתר (**Resolved**), בתפריט נפתח הנמצא למעלה מימין בחלק זה. ניתן גם לפסול או לפתור הודעות ע"י העברת העכבר על התובנה ובחירה באפשרות הרצויה. לאחר שההודעה נפתרה, יופיע סימן ⊘ .

Top Insights			All	•
General (4)		Risky User (2)		
Older		Older		
4 encrypted files delivered.		einav@prodemail.onmicrosoft.com received more than 5 threat vectors during the last 24h.		
8 encrypted files delivered.	02.08.2020 23:48 Resolve Dismiss	einav@prodemail.onmicrosoft.com received more than 5 blocked files during the last 24h.		
High number of blocked files (85) in last 24 hours.				
8 encrypted files delivered.				

החלק של התובנות העליונות מחולק ל2 רשימות:

- כללי: הערכים ברשימת ההודעות הכלליות מספקים תובנות ופרטים חשובים לגבי הודעות הדוא"ל וקבצי הצרופה בארגונך. לדוגמא: מספר הקבצים שנחסמו, מספר הקבצים המוצפנים אשר נשלחו, או התראות בנוגע מספר רב של קבצים שנחסמו בפרק זמן נתון.
- <u>מסוכן:</u> הערכים ברשימת המשתמשים המסוכנים ממקדים את תשומת ליבך למשתמשים המקבלים מספר יוצא דופן של קבצי צרופה חשודים או לא תקינים בדוא"ל. באמצעות מידע זה תוכל לבצע מעקב עם המשתמש בכדי לקבוע את הבעיה ולטפל בה.

פתירת או פסילת הודעות:

- <u>פתירת הודעות:</u> מקל על מיקוד תשומת הלב על הבעיות הפתוחות שנותרו. פתרון הודעה אינו מסיר אותה מן הרשימה. (ניתן לבחור צפיה בהודעות הפתורות לפי הסינון שנבחר).
  - פסילת הודעות: כאשר אתה פוסל הודעה, היא מוסרת מן הרשימה. 🔹



# 7 הגדרות ניהול

כאדמיניסטרטור המערכת הינך מורשה לנהל הגדרות מדיניות הFileWall , הפעלת/ ניתוק משתמשים ועוד.

# User Management -ניהול משתמשים 7.1

הFileWall שולף את נתוני משתמשי המייקרוסופט 365 בארגונך מן הAzure Active Directory ומציג אותם ברשימה בדף משתמשים. כברירת מחדל, חלה על כלל המשתמשים מדיניות ברירת מחדל עם סטטוס לא פעיל. עליך להפעיל את חשבונות המשתמשים על מנת שהFileWall יוכל לעבד את קבצי הצרופה להודעות הדוא"ל.

. **הערה:** אין באפשרותך ליצור משתמש או לערוך פרטי משתמש.

ניהול משתמשי FileWall מתבצע בחלון User Management, למעבר אליו לחץ על Å בתפריט הראשי.

<b>FileWall</b>	User Management								
	Act Licenses i	<b>ive Use</b> nformation	ers (2/18) 2/17						٥
55		Status	Name	Email	Groups	Department	Role	Policy	
Dashboard		•	Adele Vance	AdeleV@alongolan.onmicrosoft.c	alongolan	Retail	Retail Manager		
Email		•	Alex Wilber	AlexW@alongolan.onmicrosoft.c	alongolan	Marketing	Marketing Assistant		
Messiges		•	Alon Golan	along@alongolan.onmicrosoft.com	alongolan			Default Policy	
Policies		•	Candance Salem	Candy@alongolan.onmicrosoft.c	alongolan			Default Policy	
Management		•	Diego Siciliani	DiegoS@alongolan.onmicrosoft.c	alongolan	Hr	Hr Manager		
Users Management		٠	Grady Archie	GradyA@alongolan.onmicrosoft.c	alongolan	Råd	Designer		

מעל לרשימת הפעלת משתמשים, נמצא מונה המציין את מספר המשתמשים **המופעלים** ומספר סך כל תיבות הדואר בארגונך. בנוסף, מצוין מספר הרישיונות בשימוש.

🛆 Active Users (2/18)	
Licenses information	2/17

רשימת המשתמשים הפעילים כוללת את פרטי המשתמש המיובאים מ- Azure Active Directory. המדיניות שהוגדרה לכל משתמש מופיעה בעמודת המדיניות. (משתמשים שלא הופעלו לא חלה עליהם מדיניות)



# Policy Management -ניהול מדיניות 7.2

FileWall מגיע עם מדיניות ברירת מחדל המוגדרת במערכת. באפשרותך להחיל מדיניות זו עבור כל המשתמשים הפעילים, או להגדיר מדיניות ספציפית בהתאם לצרכי ארגונך. הגדרת מדיניות קשיחה המצמצמת אפשרויות קבלת קבצים בעלי סיכון משפיעה על קביעת ציון האבטחה של ארגונך במערכת.

הגדרה והקצאת מדיניות מתבצעת בחלון Policy Management, למעבר אליו לחץ על 屋 בתפריט הראשי.

<b>FileWall</b>	Policy Ma	inagement									
	Policies(1	l) + Create new poli	icy								
	Hide Inactiv	ve Policies								Search	\$
	Active	Name	Description	CDR	Type Validation	Type Filter	Last Used	Owner	Date Modified	Users	
Dashboard		Default Policy		Yes	No	Yes		Default Policy		All Unassigned	
Email						× 1 ×					
Policies Management											
Users Management											
Settings											

בכל מדיניות מפורט המידע הבא:

הסבר	פרמטר
מציין את סטטוס המדיניות (מופעל).	Active
סטטוס מדיניות ברירת המחדל הוא פעיל ולא ניתן לשינוי.	
ניתן לשנות סטטוס מדיניות ספציפית ע"י לחיצה על המתג	
(ס = לא פעיל, 🗢 = פעיל) = 🔾	
שם המדיניות.	Name
הסבר קצר על המדיניות.	Description
מציין האם ההלבנה מוחלת כחלק מהמדיניות(כן/ לא).	CDR
מציין האם אימות סוג הקובץ מוחל כחלק מהמדיניות (בו/ לא)	Type Validation
מציין האם סינון סוגי קובץ מוחל כחלק מהמדיניות(כן/ לא).	Type Filter
התאריך בו המדיניות הוחלה לאחרונה.	Last Used
שם משתמש האדמין אשר יצר את המדיניות.	Owner
התאריך בו המדיניות נערכה לאחרונה.	Date Modified
מספר המשתמשים עליהם המדיניות מוחלת.	Users



# 7.2.1 צפייה/ עריכת הגדרות מדיניות

## לצפייה בהגדרת המדיניות:

בדף המדינויות, בתפריט אפשרויות נוספות (፤) הנמצא בשורה של המדיניות, בחר ב**Edit** או לחץ קליק כפול על שורת המדיניות.

Policy Name My Policy 1	Description My Policy for demo	Users 0 Users	Policy Status
> Content Disarm Control (3	55/35) ① SANITIZING: Documents, Images		<b>~</b>
> File Type Filter ①	BLACK LIST Allowing all files except:		<b>Con</b>
> File Structure Validation (	D		O off
			Save
	Policy Status		

באפשרותך להפעיל ולכבות את המדיניות במתג הבא 🤇 👓 🚺 .

בכדי להרחיב חלק או תת חלק, לחץ 🔇

בכדי לצמצם את החלק או תת חלק, לחץ 💛.

**הערה:** בין חלק לתת-חלק מתקיים קשר היררכי. הגדרות המוחלות על חלק מוחלות על תת-חלק שלו. לדוגמא; אם תכבה את File Type Filter ברמה ההיררכית הגבוהה, הסנן יהיה כבוי לכלל סוגי הקבצים.

# (Content Disarm Control) הגדרות הלבנה (7.2.1.1

הגדרות ההלבנה קובעות את הפעולות המבוצעות על קבצי הצרופה בדואר הנכנס. מספר סוגי הקובץ שהוגדרו לסריקה מסומן בסוגרים בכחול, עם מספר המקסימלי של הסוגים הזמינים (בשחור) () (13/35) Content Disarm Control </



✓ Content Disarm Control (35/35) ①	<u>•</u> •
✓ Documents (22)	
> 🔼 Adobe (1)	
> 🖪 Excel (6)	🏚 Configure
> Sever Point (9)	🏚 Configure
> 🝓 Word (6)	💠 Configure
V 図 Images (13)	
bmp	
eps	
gif	
	Save

קבוצת המסמכים כוללת בתוכה תתי- חלקים. באפשרותך להציג את סוגי סיומת הקבצים המשויכים לתת- חלק ע"י הרחבת חלק זה. לדוגמא:

V 🧃 Word (6)	🕸 Configure
doc	🌣 <u>Configure</u>
docm	🕸 <u>Configure</u>
docx	🕸 Configure
dot	🗘 Configure
dotm	🌣 Configure
dotx	🕸 Configure

קבוצת התמונות לא כוללת בתוכה תתי- חלקים.

# 7.2.1.1.1 ביטול הסרת רכיבי קובץ מוטמעים

רמה נוספת של הבחנה הנוגעת בביטול הסרת רכיבי קובץ מוטעמים (אלמנטים שמצורפים) בתוך מסמכים. רכיבים מוטעמים הם אובייקטים, תוכן פעיל ופונקציות היכולים להתקיים במסמך אופיס. יכולת זו לעיתים מנוצלת ע"י תוקפים מפני שבאפשרותם להטמיע קוד זדוני הנראה סטנדרטי. תהליך ההלבנה מאפשר הסרת רכיבים אלו. משמעות ביטול הסרת רכיבי קובץ מוטמעים היא אי הסרה של רכיבי הקובץ במקרה של הימצאותם בסריקה.

בכדי לבטל הסרת רכיבי קובץ מוטמעים לכלל סיומות הקבצים הקשורים לקבוצה (מסמכים או תמונות) לחץ על **Configure** בשורה של הקבוצה. באפשרותך לאפשר או לבטל סוגים ספציפיים של רכיבים.

בכדי לבטל הסרת רכיב קובץ מוטבע עבור סוג סיומת קובץ ספציפי, לחץ על 🌣 בשורה. באפשרותך לאפשר או לבטל סוגי רכיבים ספציפיים ולחץ Save.





# (File Type Filters) הגדרות סינון סוג קובץ 7.2.1.1

בהגדרת File Type Filters באפשרותך לחסום או לאפשר קבלת צרופה בדוא"ל מסוג ספציפי. הגדרות אלו מוגדרות בשימוש במנגנון **White List** "רשימה לבנה" או **Black List** "רשימה שחורה".

**הרשימה השחורה** מגדירה את סוגי הקבצים שאין להם הרשאה להתקבל כצרופה בדוא"ל. הגישה לסוגי קבצים שהוגדרו ברשימה השחורה נדחית. (קבצי צרופה מסוגי קבצים שלא מוגדרים תחת הרשימה השחורה יוכלו להתקבל).

k List All	files will be	allowed exe	cept for typ	es mention	ed below														Blac	<b>k List</b> Whi	ite L
ade ×	adp x	app x	asp x	aspx x	asx ×	bas x	bat ×	cer x	chm >	cm	d x	cnt x	com x	cpl ×	crt x	csh x	der x	diagcab ×	exe x	fxp x	
gadget x	grp x	hlp x	hpj x	hta x	htc x	inf x	ins x	isp x	its x	jar 🗙	jnlp	x js x	jse x	ksh x	lnk x	mad x	maf x	mag x	mam y	maq x	b.
mar x	mas ×	mat x	mau ×	mav x	maw ×	mcf ×	mda	x md	b x r	nde ×	mdt x	mdw	× md	z x m	sc x r	nsh x m	sh1 x	msh2 x	mshxml ×	msh1xml	l ×
msh2xml	x msi	x mst :	x msu	x ops	x osd	x pcd	x pif	x pl	x plg	x	orf x	prg x	printerexp	port x	ps1 x	ps1xml x	ps2 x	ps2xml x	psc1 x	psc2 x	
psd1 x	psdm1 ×	pst ×	ру ж	рус ж	руо х	pyw ×	pyz x	pyzw	× reg	x x	scf x	scr ×	sct ×	shb x	shs ×	theme x	tmp x	url x	vb ×	vbe x v	bp
vbs x	vhd x	vhdx x	vsmacros	x vsw	× web	pnp x	website	x ws	x ws	c x	wsf x	wsh x	xbap x	xll x	xnk x	java 🗙	settingo	content-ms	x xsl x	xslt x	
nsert File	Type																				

**הרשימה הלבנה** מגדירה את סוגי הקבצים בעלי ההרשאה להתקבל כצרופה להודעת דוא"ל, כלומר, הפרטים ברשימה מורשים ועובר את תהליך החיטוי.

$\vee$ File Type Filter $\oplus$	On O
White List All files will be blocked except for types mentioned below	Black List White List
jpg x gff x Insert File Type	

. **הערה:** באפשרותך לבחור להגדיר רשימה שחורה **או** רשימה לבנה- לא את שתיהן



### הגדרת מסנן סוג קובץ

בכדי להוסיף סוג קובץ ספציפי:

. הזן את סוג סיומת קובץ או חלק ממנו בחלונית Insert File Type. השלמה אוטומטית מפרטת את סוגי קבצים/ קטגוריות התואמים להקלדה.

p	
Categories:	1
File Extensions:	
<b>p</b>	
p10	
p7b	
<b>p</b> 7c	
<b>p</b> 7m	
p/r p7s	
Z	5

2. בחר את סוג הקובץ או הקטגוריה בכדי להוספה לרשימה. הערה: במידה ותזין מחרוזת שלא מופיעה בתוצאות ההשלמה האוטומטית ותלחץ על Enter, המחרוזת תתווסף לרשימה עם התווית "unknown" והתג עצמו יסומן בצהוב עם סמל זהירות ברשימת סוגי הקבצים.

wbmp 🗴 🔹 Executable (7) 🔹 🔥 jibbersi x 🛛 Insert File Type
---



בכדי להוסיף את כל סוגי סיומות קובץ בקטגוריה מסוימת:

. הזן רווח בשדה **Insert File Type**. סוגי קטגוריות קבצים מופיעים בראש התפריט נפתח. מספר סוגי הקבצים בכל קטגוריה מצוין בסוגריים.



בחר קטגוריה בכדי להוסיף אותה לרשימה.
 תג הקטגוריה מופיע בכחול וכולל את סמל הקטגוריה.



בכדי להסיר סוג קובץ או קטגוריה:

לחץ על × הנמצא בימין התג של סוג קובץ/ קטגוריה ברשימה.

### (File Structure Validation) הגדרות אימות מבנה קבצים 7.2.1.2

File Structure Validation מאמת שתוכן הקובץ והמבנה תואמים את סיומת הקובץ. דבר זה יכול להועיל בזיהוי/ חסימה של ניסיונות זיוף קבצים (לדוגמא, קובץ הפעלה עם סיומת txt.).





# 7.2.2 הוספת מדיניות

באפשרותך ליצור מדיניות מותאמת אישית על בסיס צרכי ארגונך. **הערה:** מדיניות מותאמת אישית מוחלת על משתמשים שהוקצו אליה. שאר המשתמשים יישארו תחת מדיניות ברירת המחדל.

### בכדי להוסיף מדיניות:

**1**. בחלון ניהול מדינויות, לחץ על Create new policy + Create new policy + create new policy
במידה ותרצה ליצור מדיניות חדשה בהתבסס על מדיניות ברירת המחדל, לחץ על תפריט בימין השורה של מדיניות ברירת המחדל (1) על Duplicate

Create New Policy			
Dlicy Name De Add Policy Name	scription Add Description	Users 😌	Policy Status
> Content Disarm Control (35/35) ①	SANTIZING: Documents, images		<b>0</b>
> File Type Filter ①	BLACK LIST Allowing all files except:		<b>On ●</b>
> File Structure Validation ①			0 0#
			Create Policy

- **ב.** הזן את שם המדיניות ופירוט קצר על המדיניות בשדות המתאימים.
  - **.3** הגדר את הגדרות המדיניות. לפירוט על השדות:
    - <u>הגדרות הלבנה</u>
    - הגדרות סינון סוג קובץ
    - הגדרות אימות מבנה קבצים 🔹
- 4. אם ברצונך ליישם את המדיניות, שנה את סטטוס המדיניות 💶
  - **5.** בכדי להקצות משתמשים למדיניות זו:
  - לחץ על 😁 <sup>users</sup> בקדמת המסך.
- באפשרותך להוסיף משתמשים ספציפיים או את כלל המשתמשים בתפריט
   הנפתח הבא:



**הערה:** ניתן להקצות משתמש למדיניות אחת בלבד בכל זמן. במידה והנך מחיל



Policy Status

מדיניות חדשה על משתמש, הקצאתו למדיניות הקודמת תוסר. במידה ותסיר משתמש מהמדיניות, המשתמש יוקצה מחדש אוטומטית למדיניות ברירת המחדל.

## לחץ על **Save**.

## 7.2.3 מחיקת מדיניות

באפשרותך למחוק מדיניות מותאמת אישית שאינה רלוונטית יותר עבור ארגונך. במידה ותמחק מדיניות, המשתמשים אשר הוקצו לה יוקצו אוטומטית למדיניות ברירת מחדל. **הערה:** אין באפשרותך למחוק את מדיניות ברירת מחדל.

### בכדי למחוק מדיניות:

בחלון המדינויות, בתפריט הנפתח (፤) הנמצא בשורה של המדיניות ולחץ על

👕 Delete

# Settings - הגדרות כלליות 7.3

ההגדרות הכלליות חלות על כל המשתמשים וכל המדינויות.

# 7.3.1 הרשאת כניסה להודעות דוא"ל מקוריות

באפשרותך לאפשר לכל המשתמשים, גישה ישירה להודעות הדוא"ל החסומות והמקוריות בתיקיה ייעודית (odix-backup) שתתווסף אוטומטית לתיבת הדוא"ל. תייקת odix-backup מכילה העתק מקורי של כל הודעת דוא"ל נכנסת עם קבצי צרופה המקוריים שלהם (טרום חיטוי).

**הערה:** במידה והרשאה אינה מופעלת, משתמש חייב לפנות לאדמיניסטרטור במקרה שנדרשת גישה להודעת הדוא"ל המקורי.

# בכדי לתת/ לבטל הרשאה להודעות הדוא"ל המקוריות:

. Settings בתפריט הראשי לחץ על 🔅 בכדי להיכנס לחלון ה





# EMAIL MESSAGES -הודעות דוא"ל 8

חלון ה Email Messages מציג פרטים על ההודעות שעברו את התהליך או הוכנסו לQuarantine ע"י הFileWall בשבועיים האחרונים.

בתפריט הראשי לחץ על 🔀 בכדי להיכנס לחלון הודעות הדוא"ל. חלון הודעות דוא"ל שהוכנסו לQuarantine (הודעות דוא"ל שנחסמו) יופיע כברירת מחדל.

FileWall	Email	Messag	es								
	-O <sup>Qua</sup>	rantine (S	) A	ll (46)							
	Q w									×	٥
		Result	Action taken	Subject	Sender	Recipient	Date & Time	Attachments	Summary	Policy	
		0	None	9 layers	inbal@prodemail.onmicrosof	inbal@prodernalLonmicrosof	02.08.2020 15:00	(9.2ip)		Default Policy	
22						1 🖬 1					
*											
R											
\$											
ф ©											

. **AII** בכדי לצפות בכלל ההודעות, לחץ על חלונית

<b>FileWall</b>	Emai	il Me	essages								
	Qu	arant	cine (0)	All (6)	_						
	Q Se	earch b	y Recipient / S	ender / Subject / Stat	e / Mail ID						•
22			Result	Action taken	Subject	Sender	Recipient	Date & Time	AttachmentsSummary	Policy	
Dashboard		>	0	None	Test b	UriaW	along	24.09.2020 18:25	s +1	Default Policy	
Email		>	0	None	One u	UriaW	along	24.09.2020 18:24	Н	Default Policy	
Messages		>	0	None	test 5	UriaW	along	24.09.2020 18:23	t	Default Policy	
Policy		>	$\odot$	None	zip tes	UriaW	along	24.09.2020 18:23	s	Default Policy	
management		>	0	None	Test 3	UriaW	along	24.09.2020 18:23	B +1	Default Policy	:
User Management		>	0	None	Your	micro	along	10.09.2020 10:22	G	Default Policy	
							« 1 »				
Settings											



הפרטים הבאים מוצגים לכל הודעת דוא"ל:

הסבר	פרמטר
מציין את התוצאה של עיבוד קבצי דוא"ל:	Result
אייקון ירוק 🥺 מציין כי ההודעה חוטאה בהצלחה.	
אייקון כתום 🕖 מציין כי קבצי הצרופה לא עברו חיטוי. 🔹 🔹	
אייקון צהוב 🧭 מציין על כשל בשירות. 🔹	
אייקון אדום 🔗 מציין כי הודעת הדוא"ל נחסמה. 🔹	
אייקון אפור 🕅 מציין כי מצרופות מספר צרופות להודעת דוא"ל 🔹 🔹	
בעלות תוצאות עיבוד שונות.	
הפעולות שננקטו על הודעת הדוא"ל.	Action Taken
שורת הנושא של הודעת הדוא"ל המקורית.	Subject
שולח ההודעה.	Sender
רשימת התפוצה.	Recipient
התאריך והשעה בהם נשלחה הודעת הדוא"ל.	Date & Time
קבצי הצרופה להודעת הדוא"ל. אם ההודעה כללה יותר מצרופה אחת,	Attachments
מספר הצרופות מופיע כפלוס ליד שם הקובץ. לחיצה כפולה על השורה עם	
פרטי ההודעה תפתח מידע נוסף על כל צרופה להודעת הדוא"ל הזו. למידע	
נוסף- <u>צפייה בפרטי צרופה</u> .	
המספר מזהה המלא של הודעת מייקרוסופט. העבר את העכבר מעל שדה בפן בכדי לבעיים עם בסי בבליגים	Mail ID
הטו בכדי כהציג את הטו בחכונית. קבועה בעת בעת	<b>C</b>
ונקציר, האם קיים.	Summary
המדיניות המוחלת על המשתמש.	Policy

**הערה-** במידה והמוען שולח הודעת דוא"ל עם צרופה למספר נמנעים, המערכת מתייחסת אליהם במספר שורות (לכל נמען שורה נפרדת ברשימות הודעות הדוא"ל).

באפשרותך לחפש הודעת דואר אלקטרוני ספציפית על ידי הזנת מחרוזת מלאה או חלקית בשדה החיפוש. הטבלה מסוננת באופן אוטומטי כדי לכלול רק את הערכים המכילים את המחרוזת הספציפית.



## 8.1 צפייה בפרטי צרופה

באפשרותך להציג מידע מפורט על כל אחד מקבצי הצרופה להודעת דוא"ל ע"י לחיצה כפולה על שורת הודעת הדוא"ל זו.

~	0	None	test 5	UriaWa@odi	along@alon	24.09.2020 18:23	testBlo		Default Policy
0	Status	Name	Ту	be	Size	Original Hash	New Hash	Block Reason	CDR Summary
	Ø	testBlock.jj.rtf	ap	plication/rtf	567.0	B b98dc15ace7	28624701892		Success

#### הפרטים הבאים מוצגים לכל צרופה להודעת דוא"ל:

הסבר	פרמטר
מציין את תוצאת תהליך סריקת הקבצים:	Status
אייקון ירוק 🧭מציין כי ההודעה עברה את תהליך החיטוי בהצלחה. 🔹	
אייקון כתום 🕖 מציין כי קבצי הצרופה לא עברו חיטוי. 🔹	
אייקון צהוב 🔗 מציין על כשל בשירות. 🔹	
אייקון אדום 🔗 מציין כי הצרופה להודעת הדוא"ל נחסמה. 🔹	
שם הקובץ.	Name
סוג הקובץ.	Туре
גודל הקובץ.	Size
הhash המקורי של הצרופה.	<b>Original Hash</b>
הhash המוקצה לעותק המחוטא של הצרופה. (לא רלוונטי לקבצים	New Hash
חסומים.)	
סיבת חסימת הקובץ (לדוגמא; הלבנה או מדיניות).	Block Reason
הסבר קצר המשקף את ממצאי תהליך ההלבנה (לדוגמא; קובץ לא מאושר	CDR Summary
ע"י המדיניות, קישורים זוהו בקובץ, אובייקטים פעילים הוסרו, צלח, וכו').	

### 8.2 שחזור קבצים מקוריים

במידה ומשתמש זקוק להודעת דוא"ל טרם ההלבנה והצרופות לה, יש באפשרותך לשחזר את הקבצים המקוריים, ולהפוך אותם לזמינים למשתמש.

### בכדי לשחזר קבצים מקוריים:

Restore original files בחר בהודעת דוא"ל אחת או יותר ולחץ על All בחר בהודעת דוא"ל אחת או יותר ולחץ ל

Yes

**2**. כאשר תתבקש לאשר, לחץ

הודעת הדוא"ל המקורית והצרופות המקוריות ישוחררו מהQuarantine וישלחו לתיבת



#### הדואר הנכנס של המשתמש (ללא נטרול). באנר אפור יופיע בתחילת ההודעה.

Attachments were Released by FileWall open the attachments with caution

# Quarantine -הסרת קובץ מ- 8.3

במידה והינך בטוח כי קובץ הצרופה לא מהווה איום לארגונך, באפשרותך לשחרר אותו מQuarantine.

Yes

#### בכדי לשחרר קובץ:

- בחר הודעת דוא"ל אחת או כמה ולחץ .1 .1 בחלונית בהQuarantine בחר הודעת דוא"ל אחת או כמה ולחץ .1
  - **2**. כאשר תתבקש לאשר, לחץ

הודעת הדוא"ל המקורית והצרופות המקוריות ישוחררו מהQuarantine וישלחו לתיבת הדואר הנכנס של המשתמש (ללא נטרול). באנר אפור יופיע בתחילת ההודעה.

Attachments were Released by FileWall open the attachments with caution

