

Email Security for Microsoft 0365

Deployment and Configuration Guide Directory Integration

Area 1 Horizon Overview

Phishing is the root cause of 95% of security breaches that lead to financial loss and brand damage. Area 1 Horizon is a cloud based service that stops phishing attacks, the #1 cybersecurity threat, across all traffic vectors - email, web and network.

With globally distributed sensors & comprehensive attack analytics, Area 1 Horizon proactively identifies phishing campaigns, attacker infrastructure, and attack delivery mechanisms during the earliest stages of a phishing attack cycle. Using flexible enforcement platforms, Area 1 Horizon allows customers to take preemptive action against these targeted phishing attacks across all vectors - email, web and network; either at the edge or in the cloud.

Purpose

Area 1 Horizon can integrate with Office 365 to retrieve user and group information to enforce the Business Email Compromise configuration to prevent user impersonation.

Configuration Steps

- Step 1: Authorize Area 1 with O365 for access to the directory
- Step 2: Configure the Business Email Compromise List
- Step 3: Configure Secondary Email Address (if required)

Step 1: Authorize Area 1 with O365 for Directory Access

Area 1 Horizon needs to be authorized to make connections into your O365 tenant in order to retrieve your directory details. The account used to authorize will require the **"Privileged authentication admin"** and **"Privileged role admin"** roles.

How does the Authorization work?

The authorization process grants the Horizon Portal access to the Azure environment with the least applicable privileges required to function as shown in the screenshot below. The Enterprise Application that we register is not tied to any administrator account. Inside of the Azure Active Directory admin center you can review the Permissions granted to the application under the Enterprise Application section.

Dashboard > Enterprise application:	s > Area 1 Security - Directory	
Area 1 Security - I	Directory Permissions	×
	≪ Č) Refresh ✓ Review permissions Review perm	
Uverview		
🛄 Deployment Plan	Permissions	
Manage	Applications can be granted permissions to your organization and its data by three methods: an admin consents to the application fo	or all users,
Properties	a user grants consent to the application, or an admin integrating an application and enabling self-service access or assigning users di the application. Learn more.	irectly to
🍰 Owners	As an administrator you can grant consent on behalf of all users in this tenant, ensuring that end users will not be required to consen	it when
Roles and administrators	using the application. Click the button below to grant admin consent.	
Users and groups	Grant admin consent for Area 1 Security	
Single sign-on		
Provisioning	Admin consent User consent	
⊖ Self-service	✓ Search permissions	
Custom security attributes	API Name \uparrow_{\downarrow} Claim value \uparrow_{\downarrow} Permission \uparrow_{\downarrow} Type \uparrow_{\downarrow} Granted for the second se	through 1
(preview)	Microsoft Graph	
Security	Microsoft Graph User.Read Sign in and read user profile Delegated Admin co	onsent
e Conditional Access	Microsoft Graph Group.Read.All Read all groups Application Admin co	onsent
Permissions	Microsoft Graph Directory.Read.All Read directory data Application Admin.co	onsent
Token encryption	Microsoft Graph User.Read.All Read all users' full profiles Application Admin co	onsent
Activity	Microsoft Graph GroupMember.Read.All Read all group memberships Application Admin co	onsent
Sign-in logs		
🛍 Usage & insights		
Audit logs		
Provisioning logs		

When assigning user roles in the O365 console, you will find these roles under the **Identity** admin roles in the Roles configuration section of the user permissions.

1. From the Area 1 Horizon Portal, access the Directories configuration panel in the Settings console

(https://horizon.area1security.com/settings/directories/manage-directories) and click the **+ Add Directory** button to start the authorization process.

AREA 1 HORIZON Home Em	ail Web			Q Search_	0 0 0 0
Email Configuration Web Config	Network Devices Users and Act	ions SSO Dire	tories Subscrip	tions Service Accour	its Delegated Accounts
MANAGE DIRECTORIES	Directories			Q Search_	+ Add Directory
	DIRECTORY NAME	DIRECTORY TYPE	LAST SYNC ATTEMPT	STATUS S	SYNC FREQUENCY
	Area 1 Directory	A1S_DIRECTORY	Not Available	Active N	√ot Available

- 2. Clicking the **+ Add Directory** button will give you access to the configuration panel:
 - In the Directory Type field, use the drop down to change the type to Office 365
 - In the **Directory Name** field, enter a string that represents the directory. This value will be referenced in the Business Email Compromise List configuration section.
 - Update the **Sync Frequency** value to your preference.

AREA 1 HORIZON Home	Email Web		Add Director	y ⁽ⁱ⁾	
		ING ACTIONS	DIRECTORY TYPE	Office 365 *	
MANAGE DIRECTORIES	Directories		DIRECTORY NAME	Office 365	
	DIRECTORY NAME	DIRECT	SYNC FREQUENCY	12h *	
		A1S_D		••• Authorize + Save	

Once you have entered the appropriate values, click the **... Authorize** button to initiate the authorization process.

3. The Area 1 Horizon Portal will redirect you to a Microsoft Login page, select or enter the appropriate account to initiate for the authentication process:



4. Once authenticated, you will receive a dialog explaining the requested permissions, click on the **Accept** button to authorize the change:

directory@comodom		
airectory@someden	locorp.com	
Permissions Review for y	s requeste /our orgai	ed nization
Area 1 Securi unverified	ty - Directory	
This application is your organization.	not published b	y Microsoft or
This app would like t	:0:	
Sign in and read us	ser profile	
Read all users' full	profiles	
Read all groups		
Read directory dat	a	
Read all group me	mberships	
If you accept, this app wil all users in your organizat review these permissions.	l get access to the sp ion. No one else will	ecified resources for be prompted to
Accepting these permission your data as specified in t statement. You can chang https://myapps.microsoft.	ons means that you a heir terms of service these permissions com. Show details	allow this app to use and privacy at
Does this app look suspic	ious? Report it here	
	a 1	Assessed

5. Upon authorization, you will be automatically redirected back to the **Add Directory** configuration panel. You will need to click the **+Save** button to complete the authorization process.

AREA1 HORIZON Home E	imail Web		Add Directory	,0	×	
Email Configuration web Config		nd Actions	DIRECTORY TYPE	Office 365 *		
MANAGE DIRECTORIES	Directories	Directories		Office 365		
Directories		DIDECTORY NAME	DIRECT	SYNC FREQUENCY	12h v	
		A1S_D:		C Revoke		

6. Once saved, the newly configured directory will appear in the configured directories table.

AREA1 HORIZON Home Em	ail Web			Q Search_	0 0 4
Email Configuration Web Config	Network Devices Users and Act	tions SSO Dire	ctories Subscrip	tions Service Accou	nts Delegated Accounts
MANAGE DIRECTORIES Directories	Directories			Q Search_	+ Add Directory
	DIRECTORY NAME	DIRECTORY TYPE	LAST SYNC ATTEMPT	STATUS	SYNC FREQUENCY
	Area 1 Directory	A1S_DIRECTORY	Not Available	Active	Not Available
	Office 365	Office 365	Not Available	Active	12h

Step 2: Configure the Business Email Compromise List

Now that Area 1 has been authorized to access and retrieve directory information. To configure the Business Email Compromise List, access the **Email Configuration** section of the configuration. Under the **Enhanced Detection** option, you will find the **Business Email Compromise** configuration panel.

AREA 1 HORIZON Home Em	ail Web			Q Search_	(000	• •
Email Configuration Web Config	Network Devices Users	and Actions SSO D	Directories	Subscriptions Serv:	ice Accounts	Delegated Account	ts
DOMAINS & ROUTING	Business Email (Compromise Lis	t®	Q Search	+	New Display Name	
EMAIL POLICIES	Attackers often try to order to protect again email addresses for yo) impersonate executi 1st these impostors, Dur key users.	ives within ar add in the na	n organization to t ames and all associa	rigger a malic ated internal	ious action. I and external	n
ALLOW LIST							
BLOCK LIST	Area 1 Directory v						
ENHANCED DETECTIONS	DISPLAY NAME		EMAIL		PI	ROTECTED	
Added Detections		- N	lo results to	display -			
RETRACT SETTINGS							

1. To access the newly configured directory, use the dropdown to change the Directory to the name you used in the previous step:

Configuration Web Conf	ig Network Devices Users and A	Actions SSO Directories	Subscriptions Service A	ccounts Delegated Accounts
DOMAINS & ROUTING	Business Email Com	promise List ⁰	Q Search	+ New Display Name
EMAIL POLICIES	Attackers often try to imp order to protect against t email addresses for your k	personate executives within a these impostors, add in the n cev users	n organization to trigg ames and all associated	er a malicious action. In internal and external
ALLOW LIST	children en e			
BLOCK LIST	Area 1 Directory -			
ENHANCED DETECTIONS	Area 1 Directory Office 365	EMAIL		PROTECTED
Business Email Compromise Added Detections		- No results to	display -	

2. If the initial directory sync has completed, the page will refresh with the groups and users visible.

Note: If you do not see any information, please give it a few minutes as the system is still processing the initial synchronization.

AREA1 HORIZON Home E	Email Web	Q Search_	◎
Email Configuration Web Config	Network Devices Users and Actions	SSO Directories Subscriptions Service	Accounts Delegated Accounts
DOMAINS & ROUTING	Business Email Compromis	e List ⁽⁾ Q Search_	+ New Directory
EMAIL POLICIES	Attackers often try to impersonate order to protect against these impo email addresses for your key users	executives within an organization to trigosors, add in the names and all associate	gger a malicious action. In ed internal and external
ALLOW LIST			
BLOCK LIST	Office 365 $^{\rm v}$ Show All $^{\rm v}$	🖔 Last sync: a few minutes ago	DISABLE AUTO SYNC
ENHANCED DETECTIONS	Groups Unassigned		
Business Email Compromise	GROUP/DISPLAY NAME	EMAIL	PROTECTED
Added Detections	ALL COMPANY		0/0
	LIST		0/0
RETRACT SETTINGS	♣ 0365_GROUP		0/0
	PILOTGROUP		0/0
	> PILOTUSERS		0/1
	> PRIVATEUSERS		0/1
	* RBACDISTRUBUTION		0/0
	RBACMAILENABLESECURITY		0/0
	RBAC0365		0/0
	RBACSECURITY		0/0
	SHARED_GROUP		0/0

3. To see the members of a group, click the > button on the left of the group to expand the group to expose its members.

AREA 1 HORIZON Home	Email Web	Q Search_ 😨 🏚 @ 🌲 😁
Email Configuration Web Config	Network Devices Users and Actions SSO Directories Sub-	scriptions Service Accounts Delegated Accounts
DOMAINS & ROUTING	CO365_GROUP	0/0
	PILOTGROUP	••••
EMAIL POLICIES	> PILOTUSERS	0 /1
ALLOW LIST		
BLOCK LIST	> PRIVATEUSERS	0/1
ENHANCED DETECTIONS	* RBACDISTRUBUTION	0/0
Business Email Compromise	RBACMAILENABLESECURITY	 Ø/Ø
Added Detections	RBAC0365	0/0
RETRACT SETTINGS	RBACSECURITY	0/0
	SHARED_GROUP	0/0
	> 🗱 TEST TEAM SITE	e 8/1
	THE BROWN FAMILY	0/4
	> Brown, Charlie Charlie@some	democorp.com •···
	> Frog, Kermit Kermit@somed	lemocorp.com •···
	> Van Pelt, Linus Linus@somede	mocorp.com •···
	> Van Pelt, Lucy Lucy@somedem	ocorp.com •···
	> THE JOE FAMILY	e /5
	> THE MUPPETS	e 0/4

4. To protect a whole group, select the ... button on the right side of the group you'd like to protect and select the **Protect** option:

AREA1 HORIZON Home E	il Web		Q Search_	00	0 + 0
Email Configuration Web Config	Network Devices Users and Acti	ions SSO Directories	Subscriptions Service Accounts	Delegated	Accounts
DOMAINS & ROUTING	₩ 0365_GROUP			0/0	•••
	PILOTGROUP			0/0	
EMAIL POLICIES	> PILOTUSERS			0/1	
ALLOW LIST					
BLOCK LIST	> PRIVATEUSERS			0/1	
ENHANCED DETECTIONS	RBACDISTRUBUTION			0/0	
Business Email Compromise	RBACMAILENABLESE	CURITY		0/0	•••
Added Detections	RBAC0365			0/0	•••
RETRACT SETTINGS	RBACSECURITY			0/0	•••
	SHARED_GROUP			0/0	
	> TEST TEAM SITE			0/1	
	THE BROWN FAMILY			0/4	
	> Brown, Charlie	Charlie@	somedemocorp.com	Protect	
	> Frog, Kermit	Kermit@s	omedemocorp.com	•	
	> Van Pelt, Linus	s Linus®so	medemocorp.com	•	
	> Van Pelt, Lucy	Lucy@som	edemocorp.com	•	
	> THE JOE FAMILY			0/5	
	> * THE MUPPETS			0/4	

When a whole group is protected, all members of this group will automatically be protected and the protection markers will turn green to indicate that protection is active. 5. You can also protect individual users by clicking on the ... button next to each user:

AREA 1 HORIZON Home E	mail Web		c c	Q Search_	0 0	0 + 0
Email Configuration Web Config	Network D	evices Users and Actions SSO	Directories Subscriptio	ns Service Accounts	Delegated	Accounts
DOMAINS & ROUTING	>	PILOTUSERS		•	0/1	•••
	>	PRIVATEUSERS		e	0/1	
EMAIL POLICIES		RBACDISTRUBUTION		•	0/0	
ALLOW LIST		RBACMAILENABLESECURITY		e	0/0	•••
BLOCK LIST		RBAC0365		e	0/0	
DETECTIONS Business Email		RBACSECURITY		e	0/0	
Compromise Added Detections		SHARED_GROUP		c	0/0	
	>	TEST TEAM SITE		e	0/1	
RETRACT SETTINGS	*	THE BROWN FAMILY		¢	0/4	•••
		> Brown, Charlie	Charlie@somedemoco	rp.com		
		> Frog, Kermit	Kermit@somedemocor;	p.com	Edit	
		> Van Pelt, Linus	Linus@somedemocorp	. com	Protect	
		> Van Pelt, Lucy	Lucy@somedemocorp.	com		•••
	>	THE JOE FAMILY		•	0/5	•••
	>	THE MUPPETS		•	0/4	•••
	>	THE PIG FAMILY		e	0/4	

Step 3: Configure Secondary Email Address (if required)

When the Business Email Compromise List is configured, Area 1 Horizon will enforce the proper match of the sender's Display Name and Email Address. Any deviation from this strict requirement will raise a detection event, with the detection reason of "Protected Name <name> should not appear as <non-configured email address>"

 In some instances, you may want to allow your protected users to send from an alternate email address (i.e. their personal email). In order to configure this alternate address, you an add this to their directory entry by clicking the Edit button next to the user you'd like to configure

AREA 1 HORIZON Home E	mail Web			Q Search_	0 0	0 A O
Email Configuration Web Config	Network D	Devices Users and Actions	SSO Directories	Subscriptions Service Acco	unts Delegate	d Accounts
DOMAINS & ROUTING EMAIL POLICIES ALLOW LIST BLOCK LIST ENMANCED DETECTIONS Business Email Compromise Added Detections RETRACT SETTINGS	•	PILOTUSERS			0/1	
	•	PRIVATEUSERS			0/1	
		RBACDISTRUBUTION			0/0	
		RBACMAILENABLESECURITY			0/0	
		RBAC0365			0/0	
		RBACSECURITY			0/0	
		SHARED_GROUP			0/0	
	>	TEST TEAM STTE			0 /1	
					9 /4	
		- THE DROWN PAMILY				
		> Brown, Charlie	Charlie@:	somedemocorp.com	•	
		> Frog, Kermit	Kermit@s	omedemocorp.com	Protect	
		> Van Pelt, Linus	Linus@sor	medemocorp.com	•	
		> Van Pelt, Lucy	Lucy@som	edemocorp.com	•	•••
	>	THE JOE FAMILY			0/5	
	>	THE MUPPETS			0/4	
	>	HE PIG FAMILY			0/4	

2. Clicking the **Edit** button will give you access to the **Secondary Emails** field where you can add these additional email addresses (place each entry on a new line):

AREA 1 HORIZON Home	Email Web	Business Email Compromise		×
mail Configuration Web Conf: 	g Network Devices Users and Actions	DISPLAY NAME	Brown, Charlie	
DOMAINS & ROUTING	> A PILOTUSERS	EMAIL	Charlie@somedemocorp.com	
EMATE DOLTOTES	PRIVATEUSERS	() SECONDARY EMAILS	charles.brown@isp.com	
ALLOW LIST	* RBACDISTRUBUTION			
BLOCK LIST	RBACMAILENABLESECURITY			
ENHANCED	RBAC0365		Save	
	RBACSECURITY			

Click the **Save** button to update the entry.