CLOUDFLARE
AREA 1 SECURITY

Email Security for Microsoft O365

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

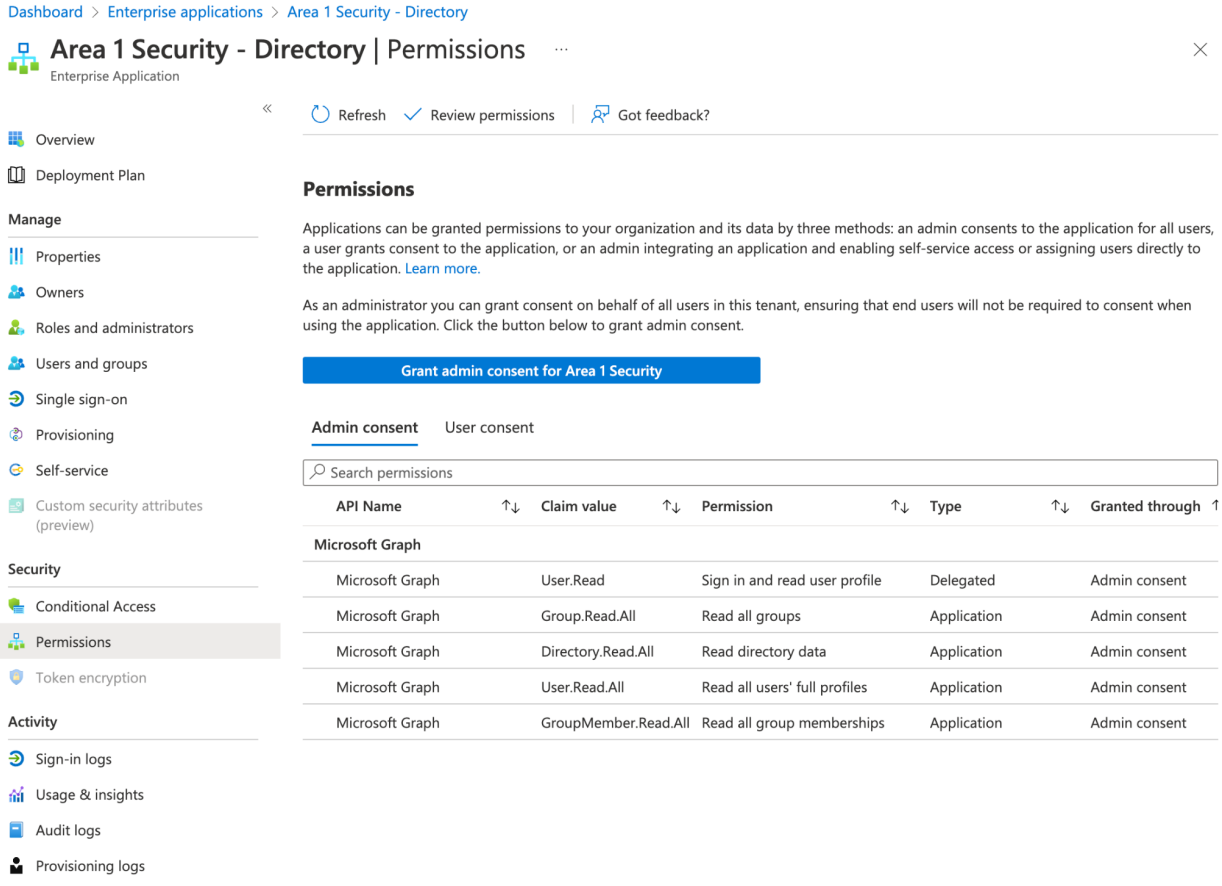
- Step 1: Authorize Area 1 with O365 for access to the directory
- Step 2: Configure the Business Email Compromise List
- Step 3: Configure Secondary Email Address (if required)

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.

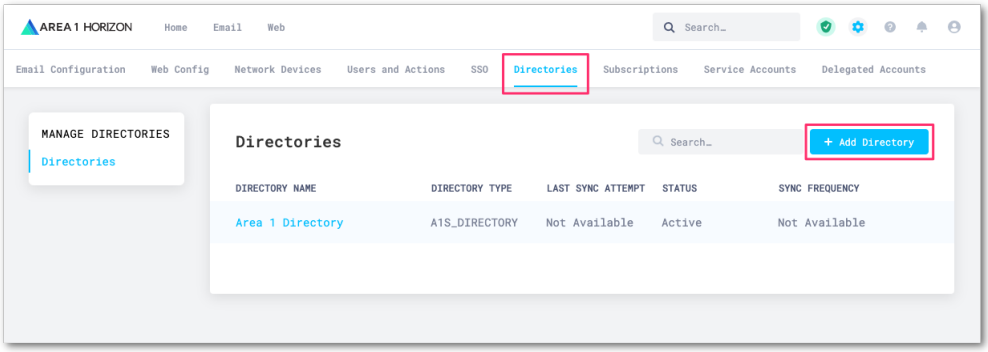
How does the Authorization work?

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.

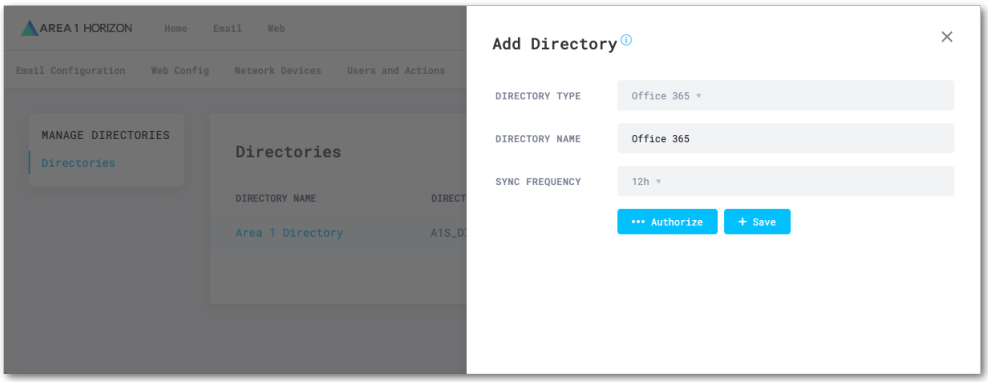


When assigning user roles in the O365 console, you will find these roles under the **Identity** admin roles in the Roles configuration section of the user permissions.

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.

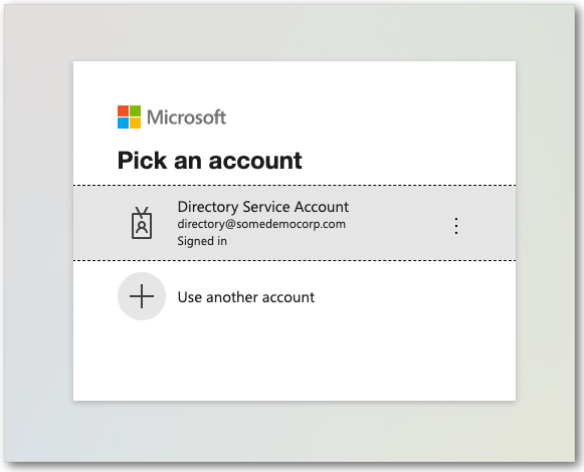


2. Clicking the **+ Add Directory** button will give you access to the configuration panel:
    - In the **Directory Type** field, use the drop down to change the type to **Office 365**
    - In the **Directory Name** field, enter a string that represents the directory. This value will be referenced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

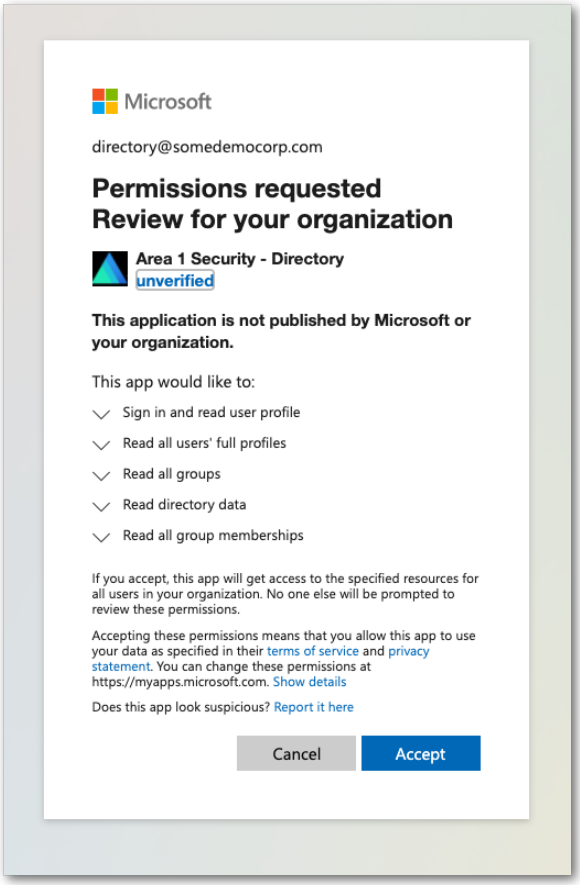


Once you have entered the appropriate values, click the **... Authorize** button to initiate the authorization process.

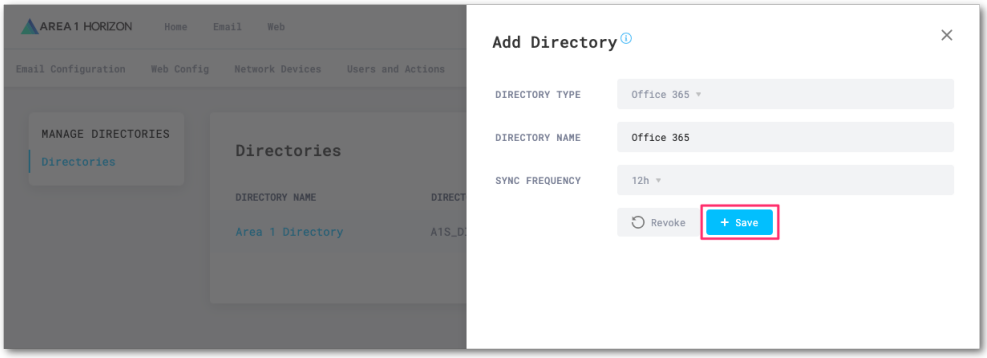
3. The Area 1 Horizon Portal will redirect you to a Microsoft Login page, select or enter the appropriate account to initiate for the authentication process:



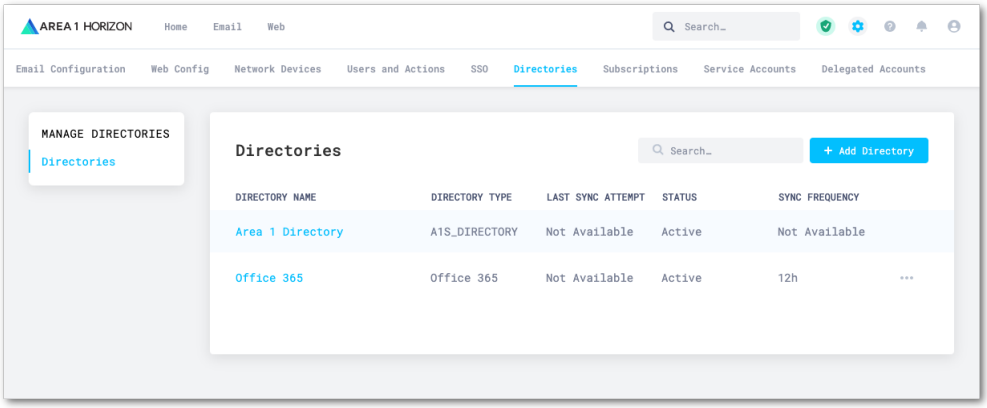
4. Once authenticated, you will receive a dialog explaining the requested permissions, click on the **Accept** button to authorize the change:



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.

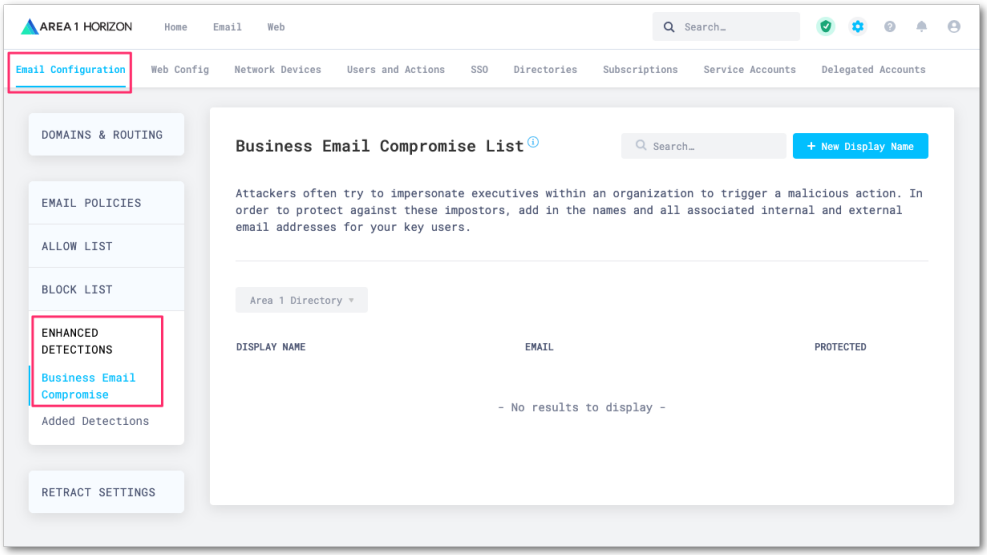


6. Once saved, the newly configured directory will appear in the configured directories table.

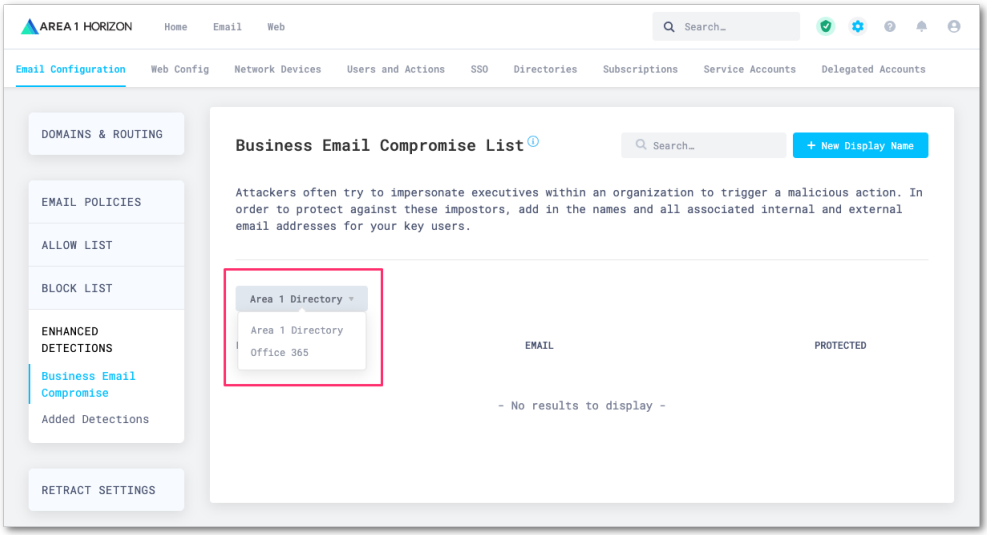


Step 2: Configure the Business Email Compromise List

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.

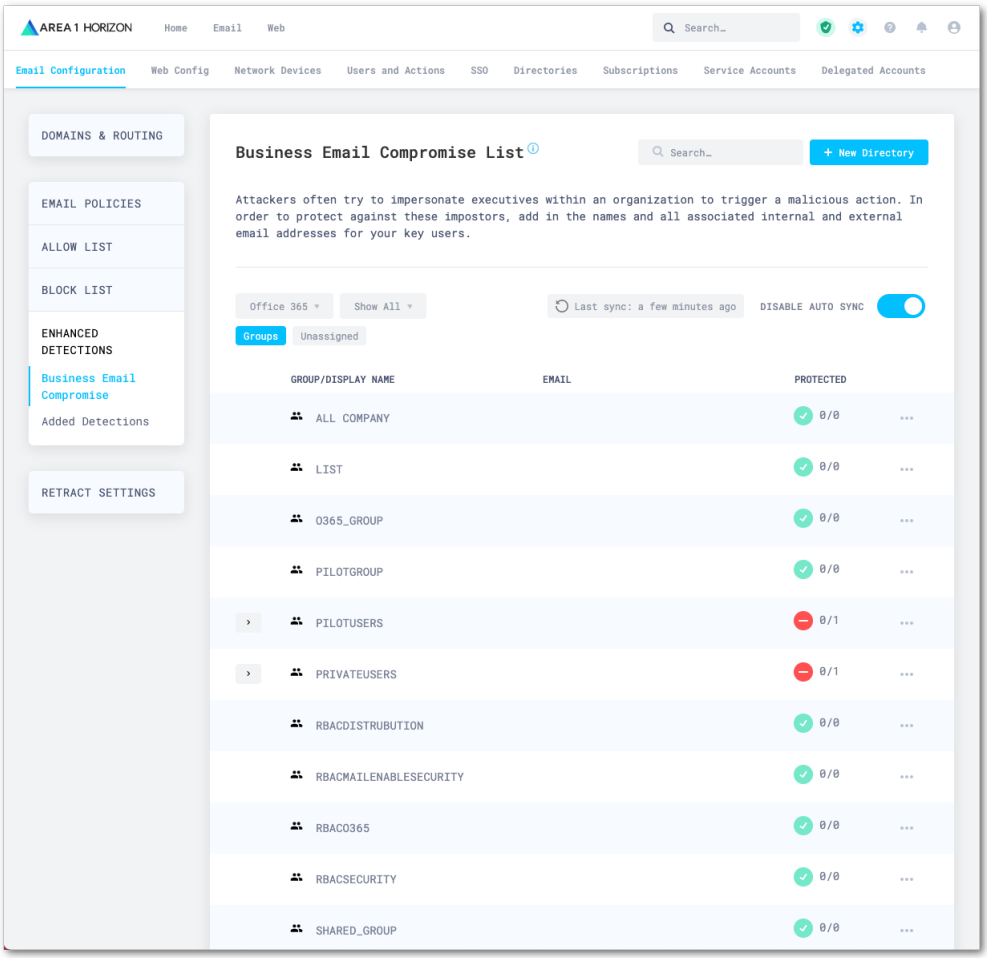


1. To access the newly configured directory, use the dropdown to change the Directory to the name you used in the previous step:

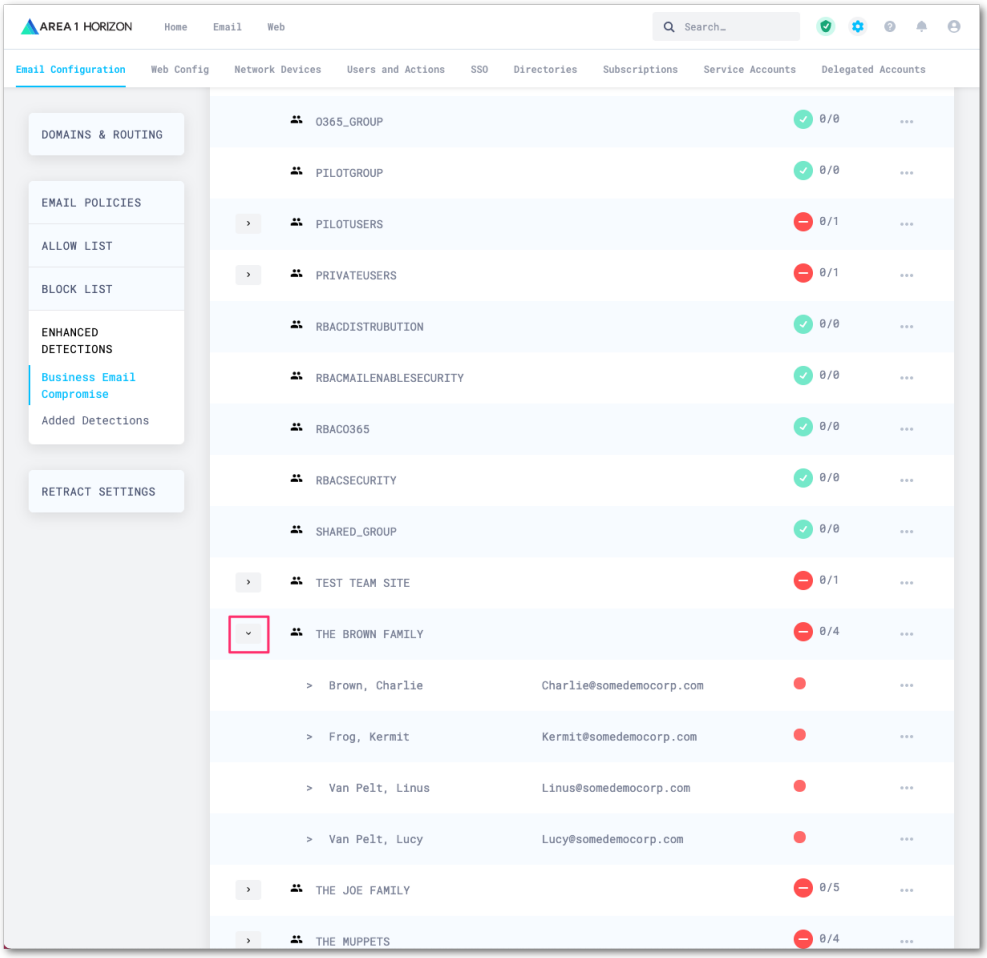


2. If the initial directory sync has completed, the page will refresh with the groups and users visible.

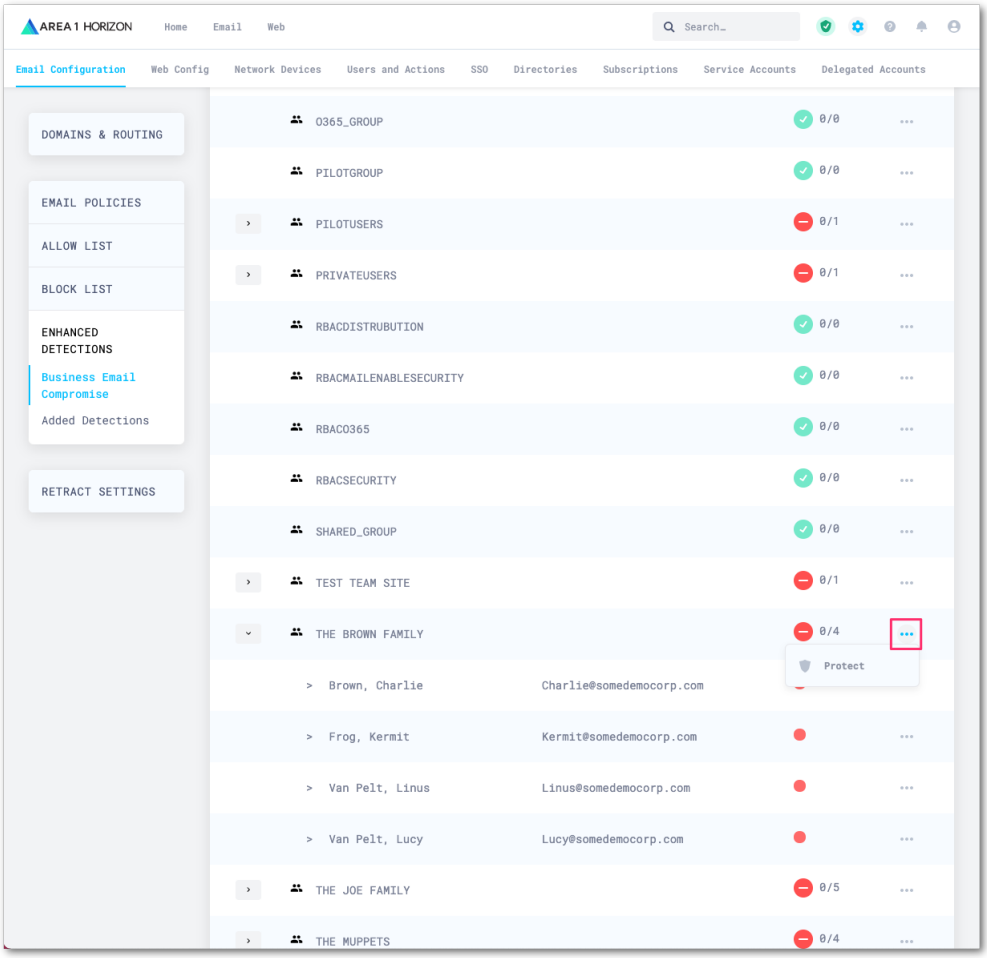
   Note: If you do not see any information, please give it a few minutes as the system is still processing the initial synchronization.



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.

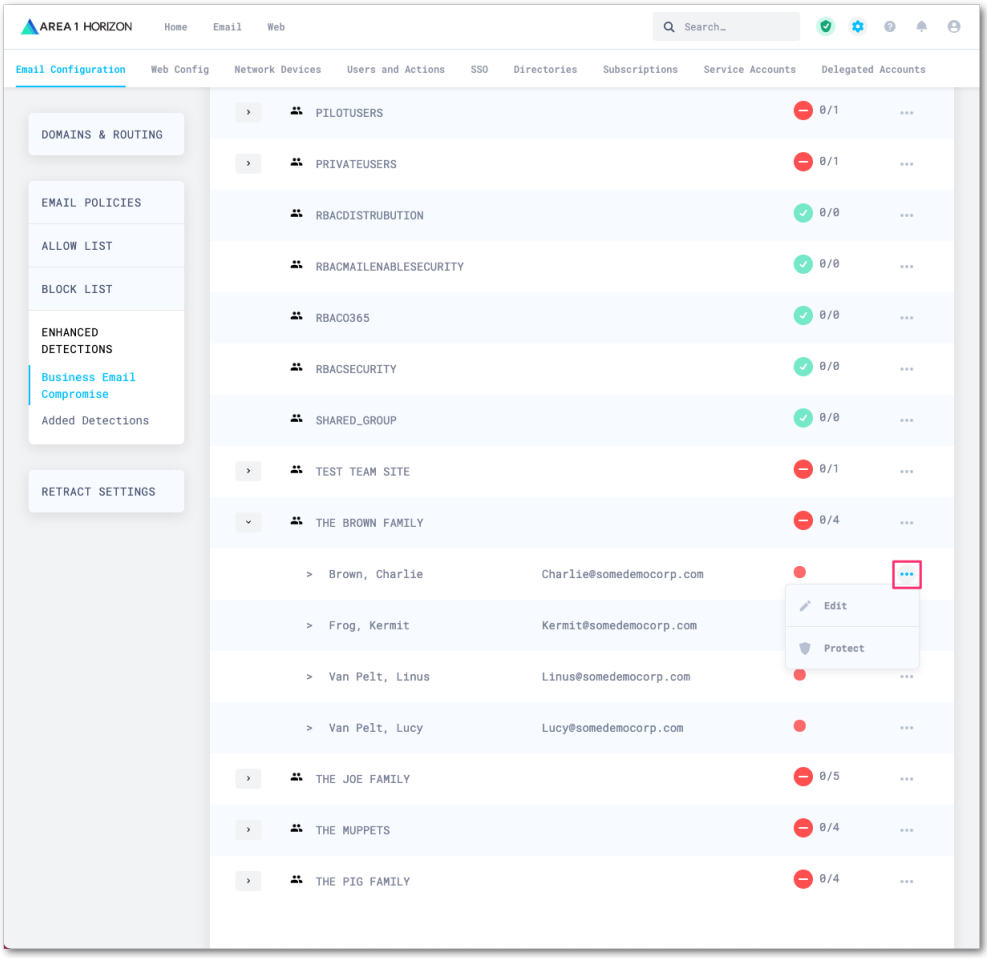


4. To protect a whole group, select the **...** button on the right side of the group you'd like to protect and select the **Protect** option:



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.

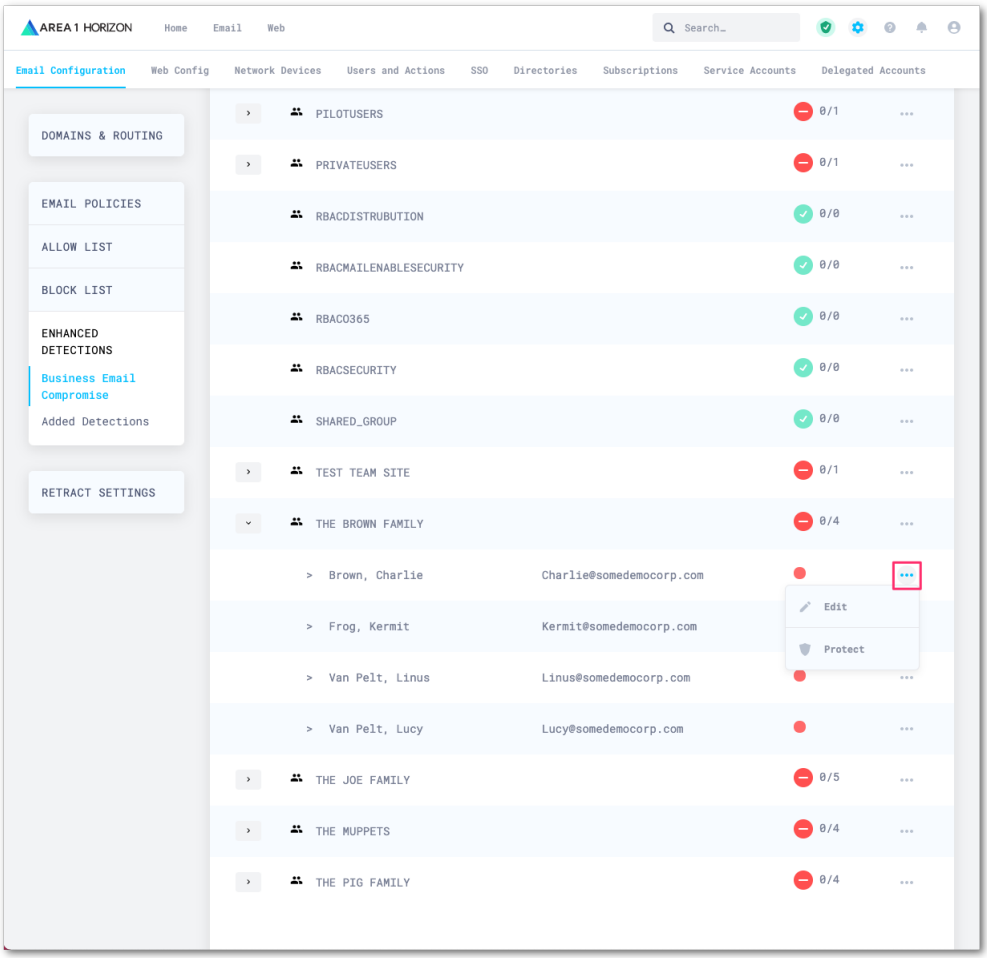
5. You can also protect individual users by clicking on the **...** button next to each user:



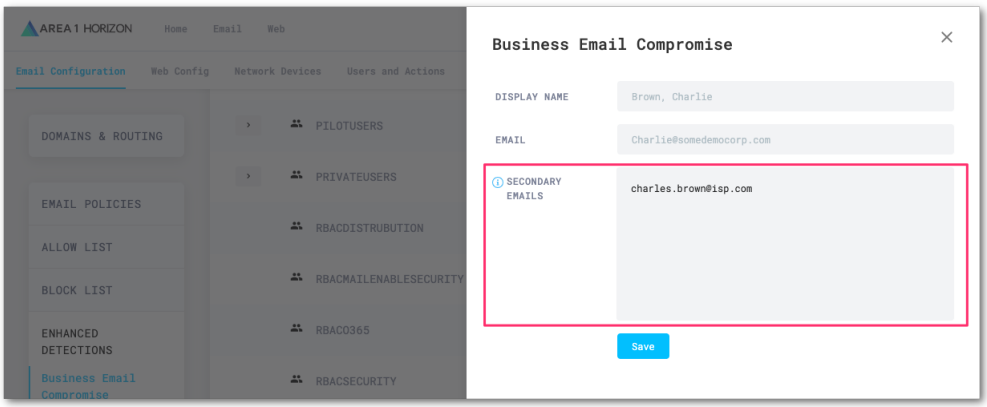
Step 3: Configure Secondary Email Address (if required)

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>"

1. 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



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):



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