



# Microsoft Azure Cloud (direct) getting started guide

Version 2.1

December 9, 2020



## What's in this guide?

Howdy! In this guide, you'll find instructions on how to:

1. Enable and configure console access for the Expel SOC;
2. Enable Application Programming Interface (API) access for Expel;
  - Enable Access for 'Expel Azure Integration' Enterprise Application
  - Create Azure Application with minimal permissions footprint
3. Select subscription(s) for Expel to monitor;
4. Enable Azure resource logs;
5. Register Azure in Expel Workbench™.

## Overview

This document will provide prerequisites and onboarding steps for Microsoft Azure Cloud (direct).

## Prerequisites

1. Before getting started, make sure you have an **Azure Active Directory (AD) admin** on hand to grant permissions.
2. Enabling Azure Defender is highly recommended by Expel to monitor Azure infrastructure. Azure Defender can be enabled on a per resource basis, or for resource groups. The following Azure Defender services are currently supported by Expel:
  - a. Azure Storage
  - b. Azure KeyVault
  - c. Azure Resource Manager
  - d. Azure App Service
  - e. Azure SQL Service
  - f. Azure Cosmos DB Service

## Step 1 — Enable console access

Having read-only access to the interface of your technology allows Expel to dig deeper when performing incident investigations. Our device health team uses this access to investigate potential health issues with your tech.

- A. Sign into the [Azure portal](#) as a user who is assigned a limited administrator directory role or the Guest Inviter role
- B. In the navigation pane, select **Azure Active Directory**
- C. Under **Manage**, select **Users**
- D. Select **New guest user**
- E. On the **New user** page, select **Invite user**, fill out the email address (**expel\_analyst@expel.io**), and optionally include a message
- F. Under roles, add the role **Global Reader** role
- G. Select **Invite** to automatically send the invitation to the guest user
- H. After you send the invitation, the user account is automatically added to the directory as a guest

## Step 2 — Enable Azure Enterprise Application

In order to integrate the technology with Expel, we need to create secure credentials to the API. There are two options presented below for enabling API access:

- Option 1 — Enable the **Expel Azure Integration Enterprise Application** within Azure
- Option 2 — Create a custom **Azure Active Directory (AD) Application**

In most cases, enabling the Enterprise Application is the recommended approach. However, because Enterprise Application supports access for multiple Microsoft integrations (Sentinel, Log Analytics, etc.), it may be the case that the permissions granted to the Enterprise Application are more than the minimum required for the Azure integration specifically. The second option is offered for cases where the absolute minimum permissions are required. In either case, the table below presents the required items that should be obtained during this step:

Item we need	Description
Directory (tenant) ID	This is a unique identifier for your Azure AD instance. Expel needs this information to route our API requests to the right place.
Application (client) ID (Option 2 only)	This is a unique identifier for the application you will create that grants Expel the access it needs to your Azure instance.
Application (client) Secret (Option 2 only)	This is the API secret that allows Expel to authenticate as the created application to your Azure instance.

Figure 1

## Option 1 — Enable Azure Enterprise Application

- A. As an Administrator, navigate to [Expel's Admin Consent Page](#)
- B. Review and accept requested permissions
- C. The 'Expel Azure Integration' app should now show up under **Enterprise Applications** — review properties and ensure that all permissions were properly granted

## Option 2 — Create Custom Azure AD Application

- A. As an Azure administrator, log in to the [Azure Portal](#)
- B. Navigate to **Azure Active Directory > App registrations** and click **+New registration**
- C. Fill in the application details. You can technically fill these in however you want, but we recommend the following:

**Name:** Expel Cloud Service

**Supported account types:** Accounts in this organizational directory only (first option)

Microsoft Azure Search resources, services, and docs (G+)

Home > Expel | App registrations >

### Register an application

\* Name

The user-facing display name for this application (this can be changed later).

Expel Cloud Service ✓

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (Expel only - Single tenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web e.g. https://myapp.com/auth

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

Figure 2

- D. Once you've filled out the fields, click **Register** to create the new application
- E. You should be navigated automatically to the settings page for the **Expel Cloud Service** app you just created. If not, navigate to **Azure Active Directory > App Registrations > View all applications** (if you don't see the new app) > **Expel Cloud Service**
- F. Make a note of the **Application (client) ID** and the **Directory (tenant) ID** for use in later steps

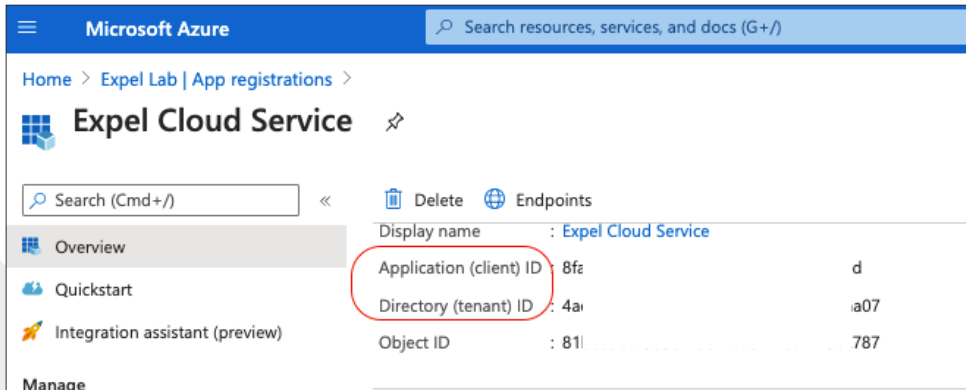


Figure 3

- G. Open **API permissions**. Click **+Add a permission**

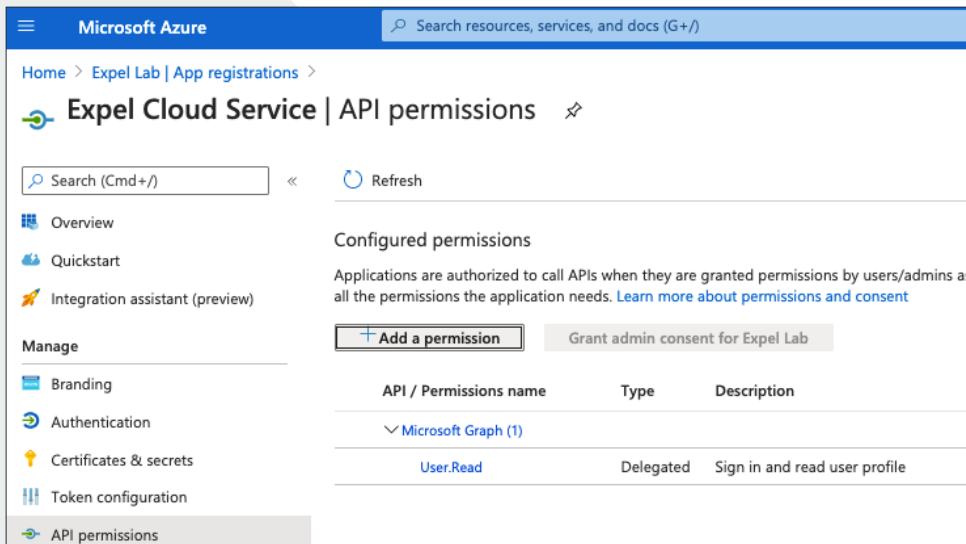


Figure 4

- H. Click on **APIs my organization uses**, type **Log Analytics** and select **Log Analytics API > Application Permissions**

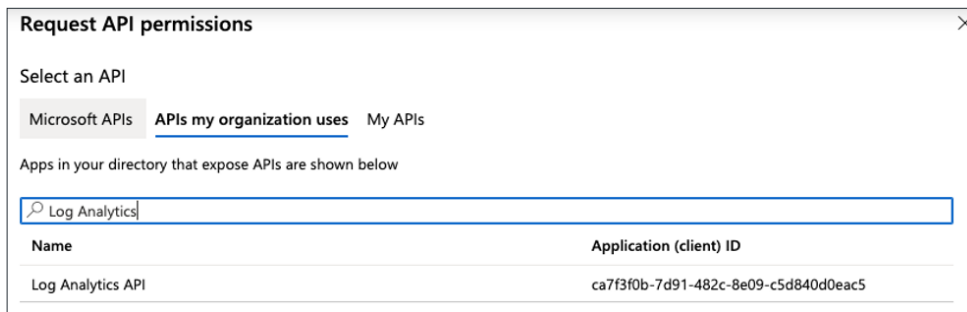


Figure 5

- I. Search for **Data.Read**, select the permission and click **Add permissions**
- J. You should be returned to the API permissions page for the application. Click **+Add a permission**
- K. Click on **APIs my organization uses**, type **Microsoft Graph** and select **Microsoft Graph > Application Permissions**
- L. Search for **SecurityEvents.Read.All**, select the permission and click **Add permissions**
- M. Once permissions have been assigned, click **Grant admin consent** and **Yes** on the confirmation popup:

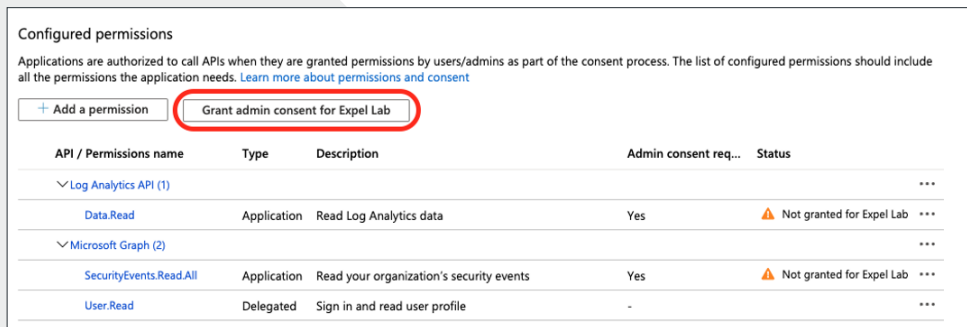


Figure 6

- N. Navigate to **Expel Cloud Service > Certificates & secrets** to begin creating an API key (aka client secret). To create a new key, click on **+New client secret**
- O. Add a description for the secret (like **ExpelAPI**) and select **Never** for expiration. Click **Add** to create the secret.

P. You will see a new secret (API Key) appear under **Client secrets**. Copy the value and save it for later. It will disappear when you navigate away from this screen:



Figure 7

### Step 3 – Enable roles within Azure subscriptions

Some event sources within Azure require **Role Based Access (RBAC) roles** to be granted to the Azure AD Application within each Azure subscription. These same **RBAC** roles granted to our Azure AD Application should also be granted to the Expel user created in *Step 1* to allow Expel to investigate further into any alerts. This section will walk through granting the Log Analytics Reader and Storage Blob Data Reader roles to both the Azure AD Application from *Step 2* and the Expel user from *Step 1*. For more information on these roles see the following:

- [Storage Blob Data Reader](#)
- [Log Analytics Reader](#)

A. Navigate to **Subscriptions** in the main Azure service menu by searching “**Subscriptions**”

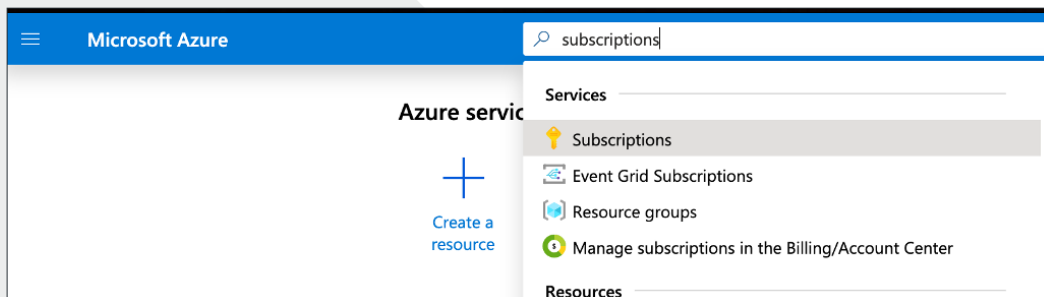


Figure 8

B. Select the subscription(s) Expel will monitor. This step is a requirement or Expel will not be able to poll any logs. Repeat steps below for each subscription

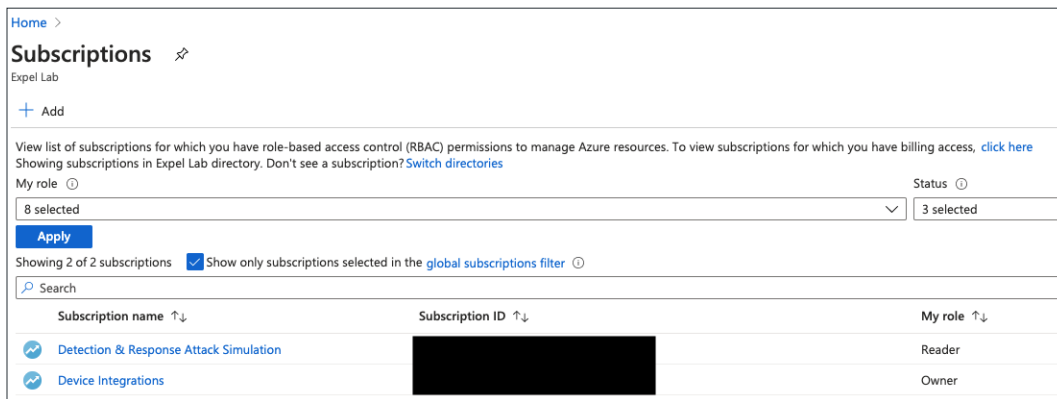


Figure 9

C. Add the below roles by clicking **Access Control (IAM) > +Add > Add role assignment**, assigning access to **Azure AD user, group or application**, and selecting the **Expel Cloud Service** or **Expel Azure Integration** app created earlier and **expel\_analyst@expel.io**. **Required roles:**

- a. Log Analytics Reader
- b. Storage Blob Data Reader

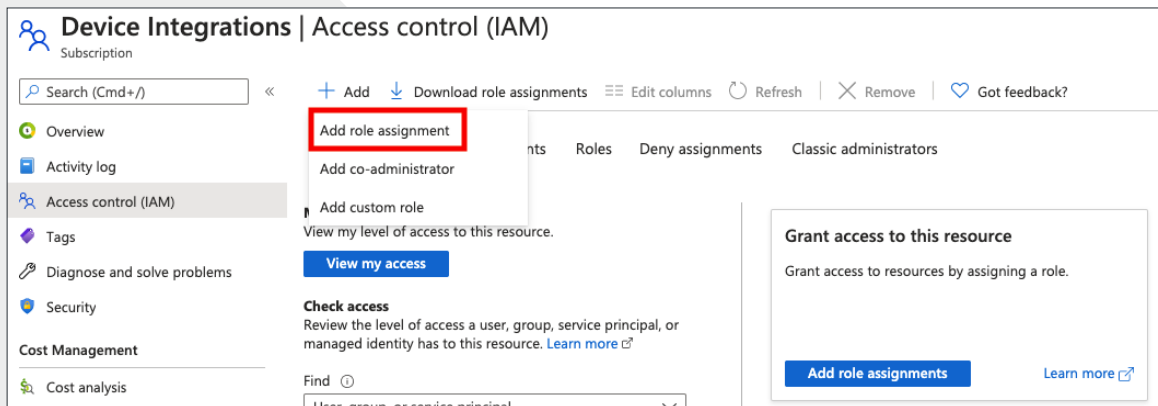


Figure 10

## Step 4 — Enable Azure Resource Logs

The Expel Azure Integration monitors alerts and logs across a variety of Azure resources. Some of these alerts and logs are accessible by default but some must be enabled in order for Expel to monitor that particular resource. The following Azure resources require user configuration in order to be monitored. Note that not all Azure deployments will utilize these resources and enabling logging within the resources will only widen Expel's default monitoring capabilities for Azure.



## Step 4 — Part 1: Enable Azure Storage Logs

Azure Storage logs give Expel context around Azure user activity to help us to determine whether that activity is malicious. Access to each storage account helps Expel provide better service but is not required. If you're unsure of whether to enable logging for storage accounts, work with your Expel Engagement Manager to help determine what approach is best for you.

- A. Navigate to the [Storage Account view within the Azure portal](#). The following steps will need to be done for each Storage Account:
- B. Select **Diagnostics settings (classic)** menu

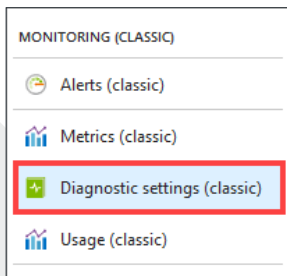


Figure 11

- C. Turn Status to **On** if not already set. Ensure each operation is checked under **Logging** section for each tab: **Blob, File, Queue, and Table properties**

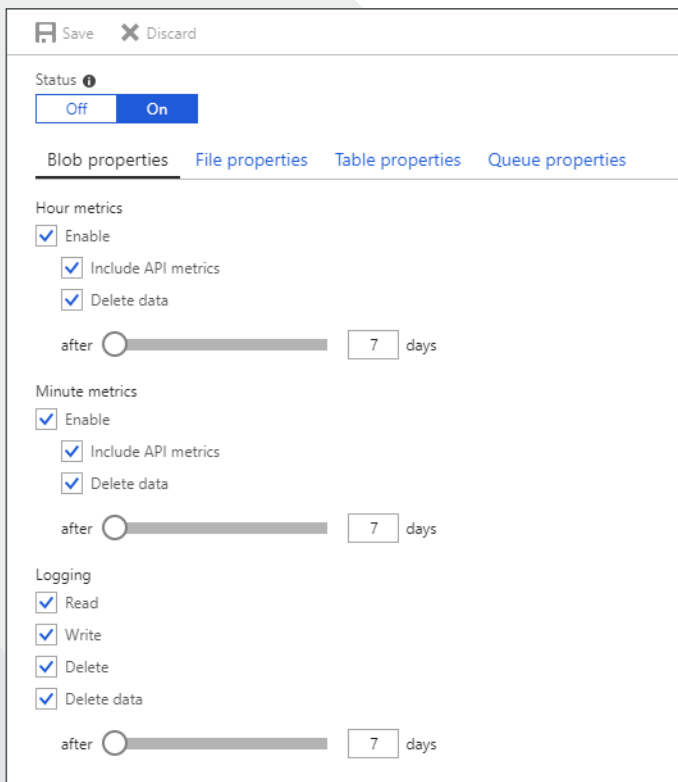


Figure 12

D. Click **Save**

E. Some storage accounts may have Network Access Control Lists (ACLs) set that limit what IP addresses may access those accounts. Azure provides a way to allow for logs to be read from these types of accounts without having to enable access or modify existing Network ACLs. Click **Firewalls and virtual networks** from the menu

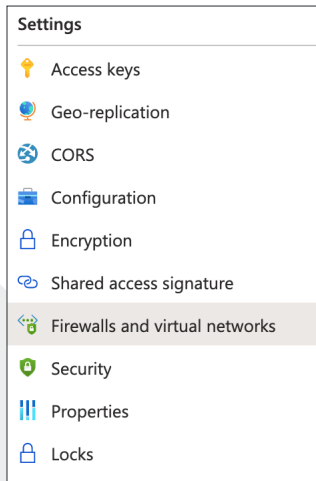


Figure 13

F. If **Allow access from** is set to **Selected networks**, check the **Allow read access to storage logging from any network** to allow access to logs (Note: the access to these logs is still managed via **RBAC** roles)

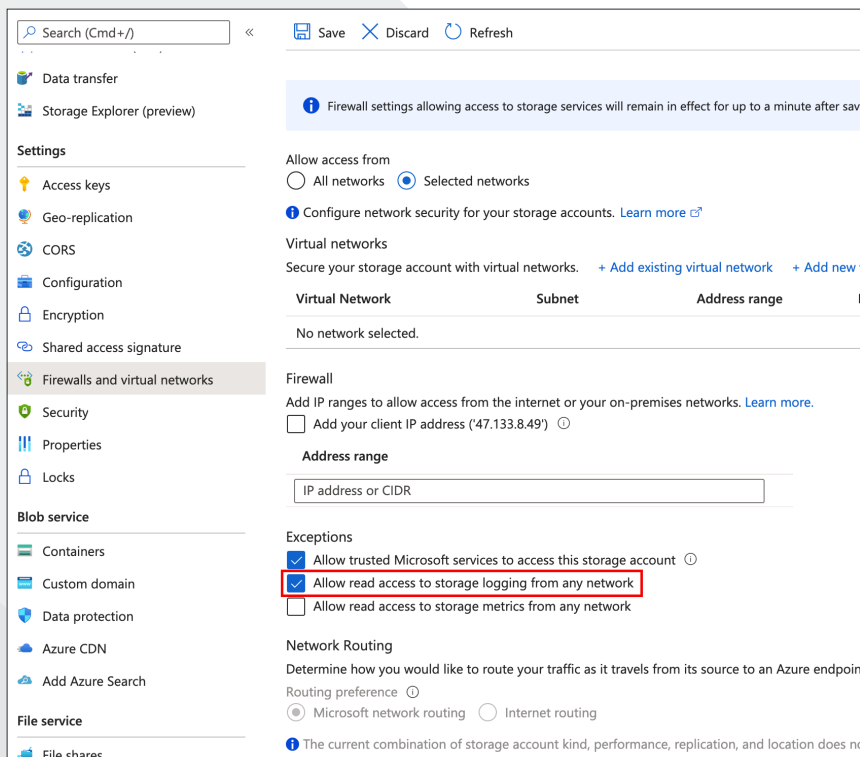


Figure 14

G. Repeat Steps B - F for every storage account

## Step 5 – Configure Azure in Workbench

Now that we have all the correct access configured and have noted the credentials, we can integrate Azure with Expel.

- A. In a new browser tab, log into <https://workbench.expel.io>
- B. On the console page, navigate to **Settings > Security Devices**
- C. At the top right of the page, select **+Add Security Device**
- D. Search for and select **Azure (direct)**
- D. Complete all fields using the credentials and information you collected in *Step 2A* or *Step 2B*

The screenshot shows the 'Add Security Device' interface. At the top, there is a search bar containing 'azure' and a dropdown menu set to 'All vendors'. Below this, a list of search results is shown, with 'Azure (direct)' selected. The main form area is titled 'Azure (direct)' and includes a link to 'View Azure (direct) setup guide'. The form is divided into several sections:
 

- SIEM:** A dropdown menu with 'Expel Cloud Service' selected.
- Name and Location:** Two text input fields.
- CONNECTION SETTINGS:**
  - Directory (tenant) ID:** Text input field.
  - Application (client) ID:** Text input field.
  - Application (client) secret:** Text input field with a 'Show' link.
  - Use storage account contributor role (y/N):** Text input field.
- CONSOLE LOGIN (OPTIONAL):**
  - Console URL:** Text input field.
  - Username and Password:** Two text input fields with a 'Show' link next to the password field.

 At the bottom right of the form, there are 'Cancel' and 'Save' buttons.

Figure 15

Field Name	What to put in it
SIEM	Select the name of a previously onboarded Expel Cloud device from the dropdown
Name	What you want to name the security device
Location	Microsoft Cloud
Directory (tenant) ID	Azure AD Directory/Tenant ID
Application (client) ID (Option 2 only)	The Azure <b>Application (Client) ID</b> that we saved in <i>Step 2, Option 2, letter F</i>
Application (client) Secret (Option 2 only)	The <b>Client Secret</b> that we saved in <i>Step 2, Option 2, letter P</i>
Use storage account contributor role (y/N)	Leave this blank or enter “N” if you provided the <b>Log Analytics Reader</b> and <b>Storage Blob Data Reader</b> roles in <i>Step 3, letter C</i>

Figure 16

- E. Select **Finish**
- F. After a few minutes, refresh the **Security Devices** page and you should see your device status reporting as *Healthy*, or if there is an issue, it will provide more details of what the issue may be


Azure Test	Cloud	 The Azure AD application has not been assigned RBAC roles within any subscriptions. Unhealthy since 2020-12-09T17:37:46Z (1 sec ago)
------------	-------	---

Figure 17

- G. To check and see if alerts are coming through, navigate to **Alerts** on the console page; click the icon in the upper right to switch to grid view, then check the list for Azure alerts

**That's it! Give yourself a pat on the back — you're done!**

If you have any issues, concerns, questions or feedback, please don't hesitate to contact Expel at [devicehealth@expel.io](mailto:devicehealth@expel.io).