G DATA TechPaper

G DATA Managed Endpoint Security Powered by Microsoft Azure – Deployment and Configuration

Contents

Introduction

Partners can deploy and manage G DATA Managed Endpoint Security Powered by Microsoft Azure through the MANAGED SERVICE COCKPIT module of G DATA ActionCenter. The module can be used to deploy and manage server infrastructure with only a few clicks.

1. Accessing the Managed Service Cockpit module

Access to the Cockpit module takes place through G DATA ActionCenter (https://ac.gdata.de). If you do not have an ActionCenter account yet, your G DATA contact will set up an account with the appropriate permissions and provide you with a link to finalize registration. If you already have an ActionCenter account, your G DATA contact will add the appropriate permissions to your account. After logging in, choose the MANAGED SERVICE COCKPIT module on the ActionCenter homepage.
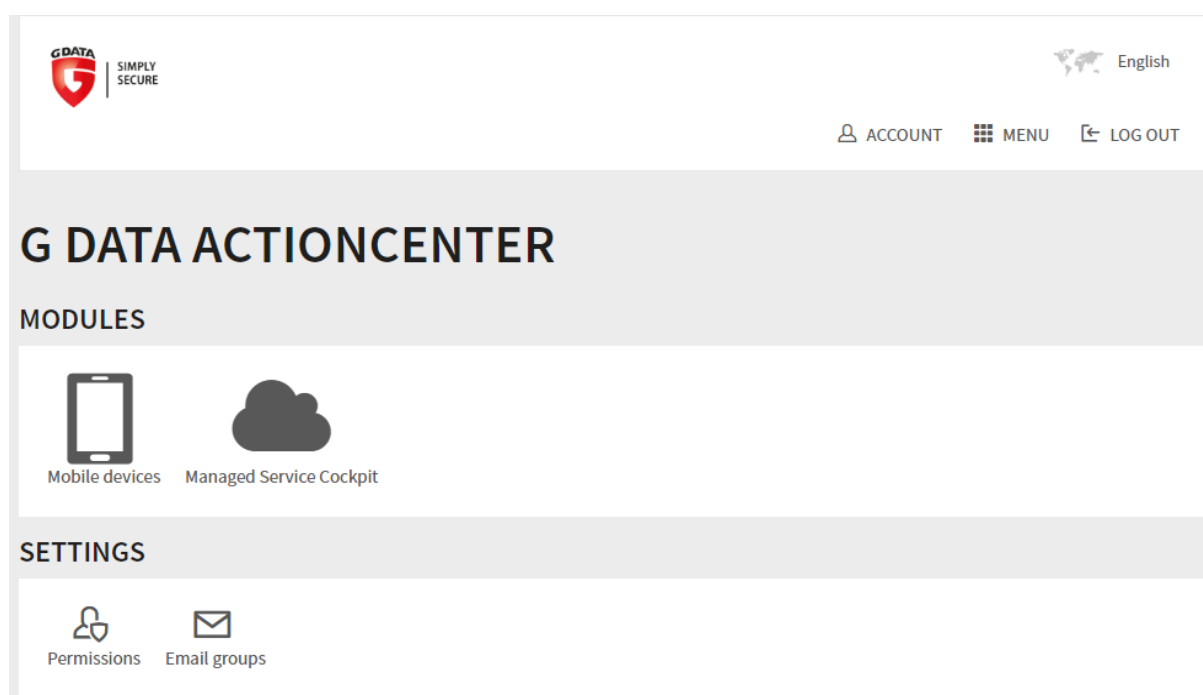

Figure 1: ActionCenter

2. Adding and managing licenses

The MANAGED SERVICE COCKPIT opens on the SERVERS view. Before creating a server, at least one license must be added. Click LICENSE at the top of the page to open the license overview and then ADD LICENSE to enter a new license key.

The license overview lists the following information for each license:

- LICENSE KEY: License key.
- LICENSE VALID UNTIL: License expiry date.
- NUMBER OF SERVERS: Number of servers.
- NUMBER OF CLIENTS: Number of clients that are being managed by the servers.
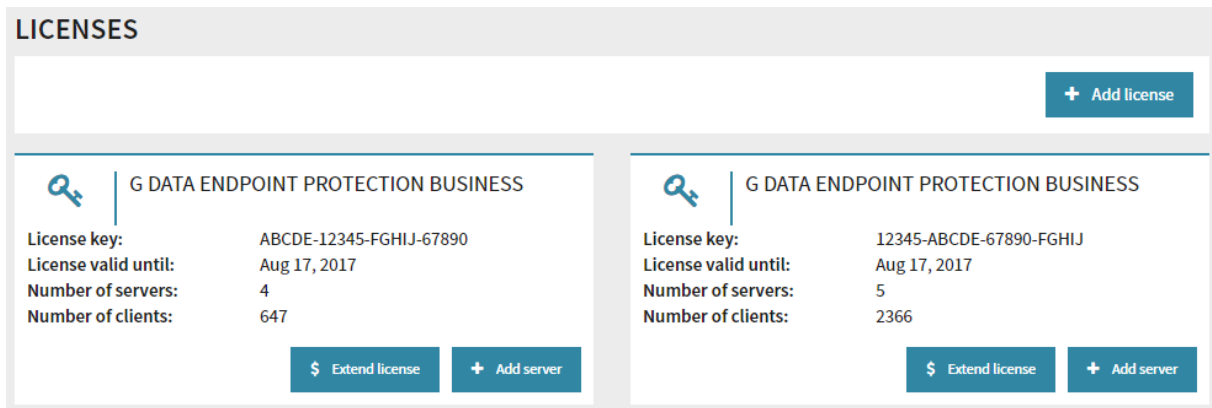
LICENSES

+ Add license

Figure 2: Licenses

Click EXTEND LICENSE to open the renewal center in order to extend an existing license or click ADD SERVER to open the CREATE NEW SERVER form with the selected license preselected.

3.   Creating a new server

The CREATE NEW SERVER form is used to create a new server instance and can be opened through the SERVERS view or by clicking ADD SERVER in the LICENSES view.

Figure 3: Create new server

On the CREATE NEW SERVER form, the following information must be filled out:

- COMPANY: The name of the company for which the server is being deployed.
- NAME: The name of the contact person at the company.
- EMAIL ADDRESS: The email address of the contact person at the company.
- EXPECTED NUMBER OF CLIENTS: The expected number of clients to be served by the server.

- SERVER LOCATION: The Azure cloud region in which the server will be created. Select the region nearest to the clients that will be managed.
- LICENSE: The G DATA license key for which the server will be created.
- HIGH AVAILABILITY: If required, the server can be created in high availability mode, which includes a secondary server.

Click CREATE NEW SERVER to create the new server. All necessary infrastructure will be provisioned automatically, including the operating system, database server, Management Server and all necessary configuration.

4. Managing servers

The SERVERS overview displays all servers. At the top of the screen, the total number of clients across all servers is displayed (updated daily). For each server, the following information is listed:

- NUMBER OF CLIENTS: The number of clients being served by the server.
- PRODUCT: The G DATA product which has been deployed to the server.
- CONTACT: The name of the contact person at the company for which the server was deployed.
- COMPANY: The name of the company for which the server was deployed.

Figure 4: Servers

Click on any server to open its detailed information page and view all available information:

- STATUS: The current status.
- NUMBER OF CLIENTS: The number of clients being served by the server.
- MAIN SERVER: The FQDN for the main server.
- SECONDARY SERVER: The FQDN for the secondary server, if the server was deployed as a high availability server.

- SERVER UNIQUE IDENTIFIER: The unique identifier for the server.
- HIGH AVAILABILITY: Whether the server was deployed as a high availability server (with a secondary server) or not.
- MICROSOFT AZURE RESOURCE GROUP: The Azure resource group to which the virtual machine belongs.
- SERVER LOCATION: The Azure server region which hosts the virtual machine.
- PRODUCT: The G DATA product which has been deployed to the server.
- LICENSE KEY: The license for which the server was created.
- CONTACT: The name of the contact person at the company for which the server was deployed.
- COMPANY: The name of the company for which the server was deployed.
- ADMINISTRATION CREDENTIALS: The user name and password to be used to log in to G DATA Administrator or WebAdministrator.
- ADMINISTRATION URL: A link to G DATA WebAdministrator, which can be used to configure the security settings (see chapter 6).
- INSTALLATION PACKAGE FOR WINDOWS: A link to the client installation package, which can be used to install G DATA Security Client on Windows clients (see chapter 5).

SERVER

Status: STARTED	**Number of clients:** 28
Main server: server2.domain.com	**Secondary server:** server2-secondary.domain.com
Server unique identifier: 1234567890-abcdef	**High availability:** Yes
Microsoft Azure resource group: 1234567890	**Server location:** Europe North
Product: G DATA ENDPOINT PROTECTION BUSINESS	**License key:** ABCDE-12345-FGHIJ-67890
Contact: Contact 2	**Company:** Company 2

Administration credentials:
username / xxxxxxxxxxx 👁

Administration URL:
https://administration.domain.com

Installation package for Windows:
https://server2.domain.com/installationpackage.exe

MANAGEMENT

[Stop server] [Delete server]

Figure 5: Server details

Under MANAGEMENT, click STOP SERVER/START SERVER to stop or start the server instance or DELETE SERVER to completely delete the server instance.

5.   Deploying clients

The installation of G DATA Security Client can be easily automated using the prebuilt client installation package. The package can be downloaded from the INSTALLATION PACKAGE FOR WINDOWS link that is provided on the server details page (see chapter 4). Using GPO or logon scripts or a manual installation, the package can then be deployed to Windows clients in the customer network. Upon installation, G DATA Security Client will automatically connect with the hosted server and can be configured using the administration tools (see chapter 6).

More information about deploying clients for Windows, Mac and Linux and about mobile device management for Android and iOS can be found in the manual as well as the Reference Guide.

6.   Managing and configuring clients

Client management and configuration can be carried out using G DATA Administrator or G DATA WebAdministrator. G DATA WebAdministrator can be started through the ADMINISTRATION URL from the server properties page (see chapter 4). Alternatively, G DATA Administrator can be installed locally from a G DATA installation medium, which can be downloaded from the G DATA website.
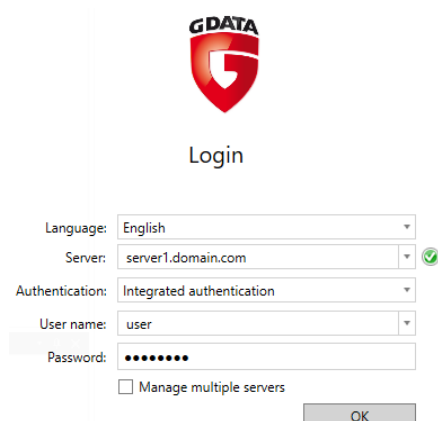

Figure 6: G DATA Administrator login

On the login screen, enter the SERVER (MAIN SERVER from the server details page), select INTEGRATED AUTHENTICATION, enter the USER NAME and PASSWORD (ADMINISTRATION CREDENTIALS from the server details page) and click OK to log in to the server. The use of G DATA Administrator and G DATA WebAdministrator is described in the manual as well as the Reference Guide. Note that because the server is hosted on cloud infrastructure, the administration tools display timestamps in the UTC time zone, which may differ from your local settings.

When configuring multiple servers, G DATA Administrator and G DATA WebAdministrator can be used in MasterAdmin mode. This requires an activation code, which can be requested from your G DATA contact. On the login page of G DATA (Web)Administrator, select MANAGE MULTIPLE SERVERS and set up a MasterAdmin login. After starting G DATA (Web)Administrator in MasterAdmin mode, add the server(s) you want to manage using the MASTERADMIN WIZARD. More information about using MasterAdmin can be found in the Reference Guide.