



# **iQ.Suite – Azure Edition**

## **Processing Microsoft 365 Emails by iQ.Suite**

**Document Version 2.2**

**iQ.Suite for SMTP**

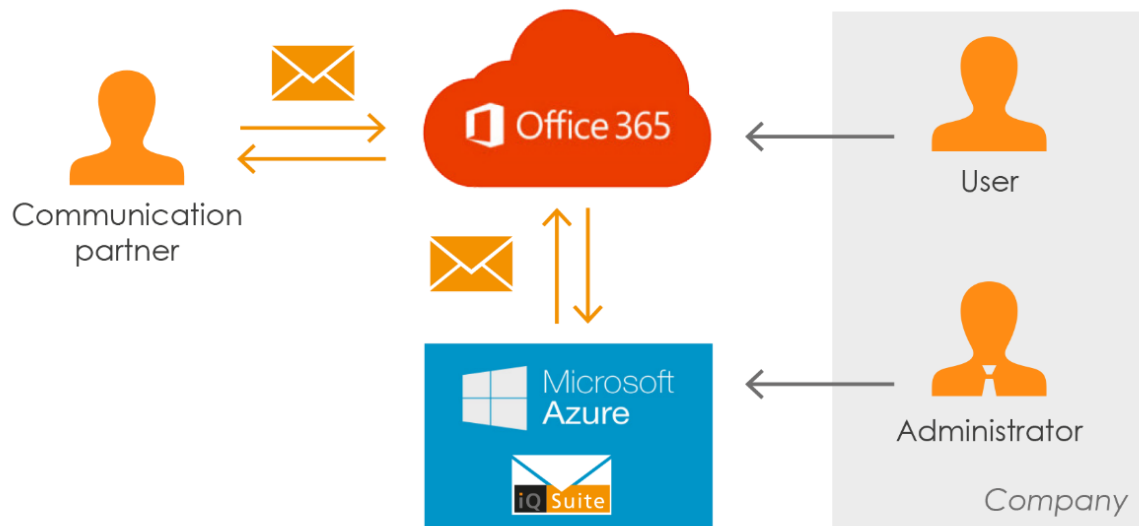
## Contents

<b>1</b>	<b>Overview .....</b>	<b>4</b>
<b>2</b>	<b>Configuration in Azure Portal .....</b>	<b>6</b>
2.1	Configuring the Network Security Group.....	6
2.2	Creating and Configuring iQ.Suite Azure VM.....	7
2.2.1	Setting the VM Basic Settings .....	7
2.2.2	Defining a Fixed DNS Name for the VM .....	10
<b>3</b>	<b>Setting up the Azure VM Environment .....</b>	<b>12</b>
3.1	General Configuration .....	12
3.2	SMTP Server Configuration .....	12
3.3	iQ.Suite Configuration .....	14
3.4	Additional Information and Configuration .....	16
3.5	Monitoring the Mail Flow Status .....	16
<b>4</b>	<b>Setting up the Microsoft 365 Environment.....</b>	<b>18</b>
4.1	Guid for Message Header .....	18
4.2	Requirements for Microsoft 365 SMTP Relay .....	19
4.3	Limitations for Microsoft 365 SMTP Relay .....	19
4.4	Creating Connectors.....	19
4.4.1	Azure VM to M365.....	19
4.4.2	M365 to Azure VM.....	20
4.5	Creating Exchange Mail Rules .....	22
4.5.1	Rule for mail forwarding .....	22
4.5.2	Rule for mail approval .....	24
4.6	Optional: Adding SPF Record to the Domain.....	25
4.7	Adding Public IP to the Exchange Filter .....	26
4.8	Delisting Blocked Public IP (Microsoft).....	26
4.9	Delisting Blocked Public IP (Spamhaus) .....	27
<b>5</b>	<b>Configuring WebClient Authentication with Azure AD .....</b>	<b>28</b>

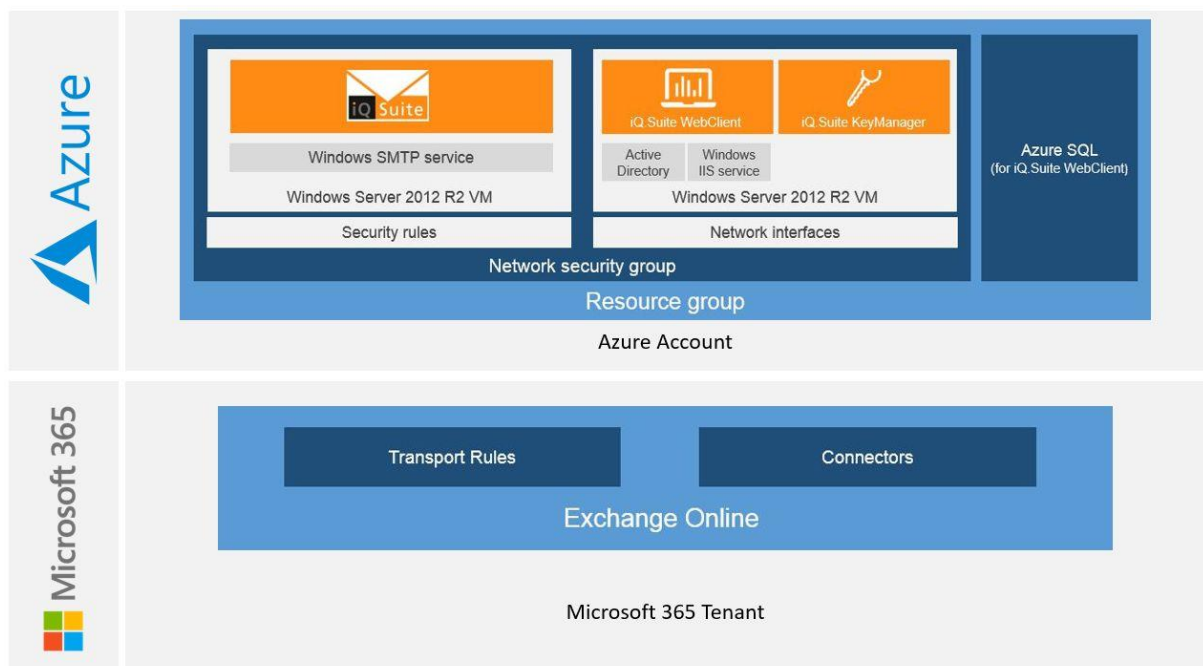
5.1	Setting up the Azure Active Directory.....	28
5.1.1	Creating Azure App for WebClient.....	29
5.1.2	Configuration of the WebClient Azure App .....	31
5.1.3	Permissions of Azure App WebClient .....	32
5.1.4	Creating Azure App for iQ.Suite PowerShell .....	35
5.2	Settings in the 'dynamic_configuration.xml' .....	37
5.2.1	Authorization and Group Resolution in Azure AD .....	37
5.2.2	Authorization in Azure AD and Group Resolution in LDIF File .....	37
5.3	Resetting the SecurityContext.....	38
5.4	LDIF Sync of Exchange Online directory .....	38
<b>6</b>	<b>For using EWS – Use OAuth and set permission.....</b>	<b>42</b>
6.1	Enable OAuth in the Registry .....	42
6.2	Setting permission for using EWS.....	43
<b>7</b>	<b>High Availability (optional).....</b>	<b>46</b>
7.1	Creating a Load Balancer.....	47
7.2	Configuring the Load Balancer.....	48
<b>8</b>	<b>About GBS.....</b>	<b>54</b>

## 1 Overview

With iQ.Suite hosted in Microsoft Azure, you can operate your complete email environment in the Cloud. Emails from your Microsoft 365 mailboxes can be transported by email routing to your iQ.Suite for SMTP. In iQ.Suite, they can be processed in a rule-based manner and then be transported back to Microsoft 365. This is possible for incoming and outgoing emails as well as for internal emails.



Overview of the relevant components in Microsoft 365 and Azure:



This documentation describes the required configurations and adjustments for using our solution in Microsoft 365 and in Microsoft Azure.

## 2 Configuration in Azure Portal

With the creation of iQ.Suite in Azure Marketplace Offer, the following scenario is created:

A new virtual machine based on an iQ.Suite image is created. During this creation, a **Resource Group** is also created. With a Resource Group, different resources can be combined to a virtual network. This way, all VM(s) are in the same subnet. The Network Security Group of a Resource Group allows to establish general network rules. A Network Security Group is connected to the Network Interfaces of the VM(s). For the VMs, static public IPs and DNS names must be assigned in the Azure Portal to be able to access the VM outside of the subnet, e.g. when using iQ.Suite WebClient. Every VM on which an SMTP server will run later on has to be added to the same Availability Set during the creation. An Availability Set is needed for the later usage of a Load Balancer. An already existing VM cannot be added to an Availability Set.

If you want to use additional products such as iQ.Suite KeyManager, we recommend to create another VM in the Resource Group in order to distribute the load to several VMs.

Additionally, you can set up a connection to Azure SQL databases for iQ.Suite and WebClient to allow a complete Cloud operation.

Before you start with the configuration in the Azure Portal (<https://portal.azure.com>), note that it is not possible to rename any resources created in the Azure Portal afterwards.

### Sizing recommendation:

We recommend to use one of the following sizes for the Azure VM:

- Standard A4\_v2
- Standard A3
- Your VM size should have at least 4 CPUs and 7GB RAM

## 2.1 Configuring the Network Security Group

Configure your Network Security Group (NSG):

1. Open your NSG and click on **Inbound security rules**.
2. Create your required security rules according to the following table:

## Inbound security rules

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
100	RDP	3389	TCP	Any	Any	✓ Allow
110	SMTP	25	TCP	Any	Any	✓ Allow
120	WebClient	8099	TCP	Any	Any	✓ Allow
121	KeyManager	8080	Any	Any	Any	✓ Allow
123	iQ.Suite	8008	TCP	Any	Any	✓ Allow
124	HTTP	80	TCP	Any	Any	✓ Allow
134	HTTPS	443	TCP	Any	Any	✓ Allow

The specified ports must also be released in the Windows firewall on the Azure VM. Otherwise, they cannot be reached from outside of the Azure subnet, e.g. for using iQ.Suite KeyManager.

**Important:** Only add rules for services, which you actually use. For a default environment with just iQ.Suite, only SMTP and RDP are necessary. If you also want to access the WebClient from outside the Azure VM, then you will also need to add rules for either HTTP or HTTPS.

For the RDP rule in particular, for security reasons, you should also use your own static company IP as the 'Source IP address' and not use 'Any' as source.

## 2.2 Creating and Configuring iQ.Suite Azure VM

### 2.2.1 Setting the VM Basic Settings

1. Select the size and the pricing tier of the VM.  
*Recommendation: A4\_V2 Standard.*
2. Assign the VM to the previously created Availability Set:

The assignment to an Availability Set cannot be changed after the creation of a VM.

Dashboard > New > Marketplace > iQ.Suite (preview) > Create a virtual machine

## Create a virtual machine

customization.  
Looking for classic VMs? [Create VM from Azure Marketplace](#)

### Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* ⓘ

Resource group \* ⓘ  [Create new](#)

### Instance details

Virtual machine name \* ⓘ  ✓

Region \* ⓘ  ✓

Availability options ⓘ  ✓

Availability set \* ⓘ  ✓ [Create new](#)

Image \* ⓘ  ✓ [Browse all public and private images](#)

Size \* ⓘ **Standard A4 v2**  
4 vcpus, 8 GiB memory  
[Change size](#)

### Administrator account

Username \* ⓘ  ✓

Password \* ⓘ  ✓

Confirm password \* ⓘ  ✓

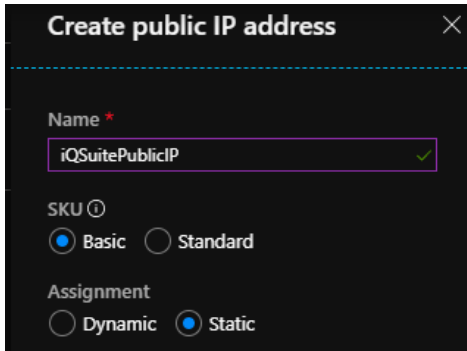
- You can choose either HDD or SSD as disk type.
- Under 'Advanced', you can also choose to use the 'Managed Disks' option which is enabled by default. The 'Managed Disk' option means, that Microsoft will manage the hard disk of your VM and it will not be saved in your own storage account.
- If you choose not to use the 'Managed Disk' option, then either create a new Storage Account for the VM or assign the VM to an already existing Storage Account. The region must be identical for both the VM and the storage.

For highest security and availability, each VM should have an own storage and the replication should be set to **Geo-Redundant Storage** (GRS). This way, your data would be replicated to another Azure region.

Please note that this would result in higher costs.



6. In Networking, make sure that your VM has been assigned to the virtual net of the Resource Group.
7. Select that a new public IP is created for the VM. This IP must be static. So, select 'Static' and confirm with **OK**.



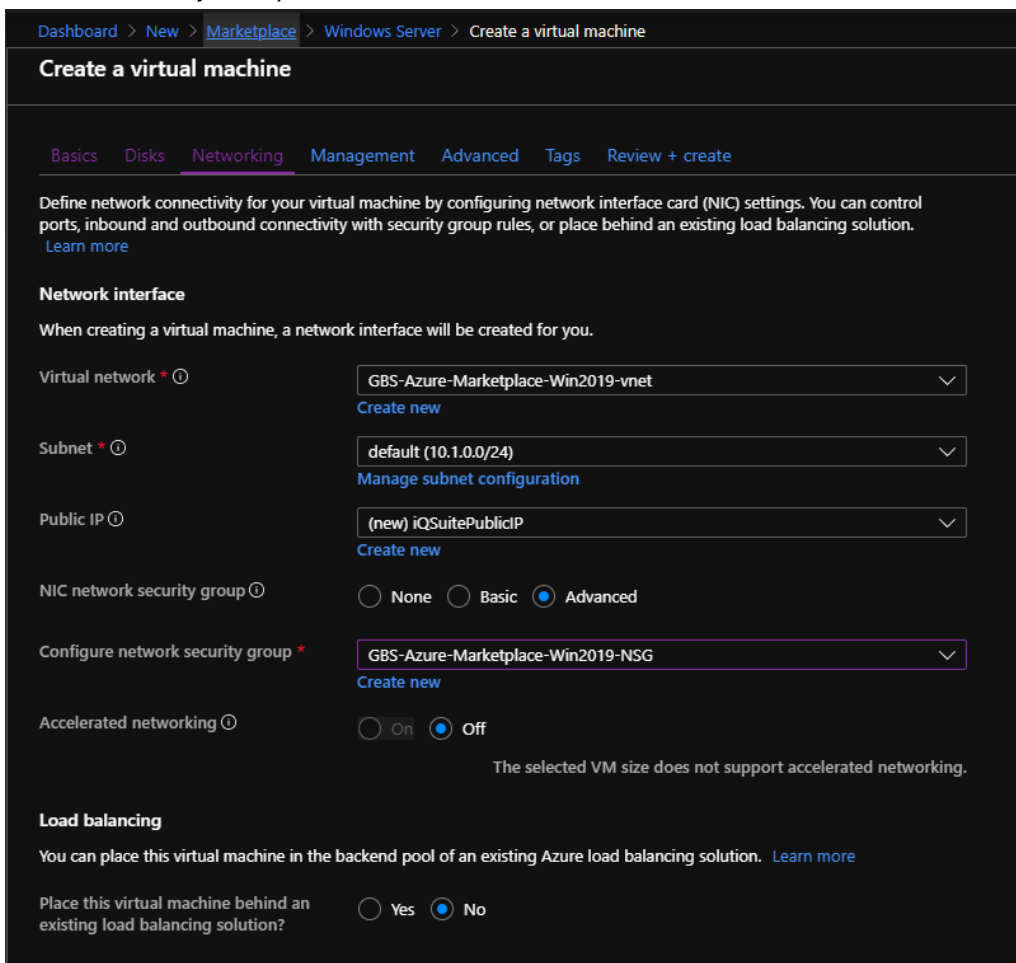
**Create public IP address**

Name \*  
iQSuitePublicIP ✓

SKU ⓘ  
☒ Basic ☐ Standard

Assignment  
☐ Dynamic ☒ Static

8. Under the 'NIC network security group' setting, choose the advanced option and then select the Network Security Group, that was created before and has all firewall rules.



Dashboard > New > Marketplace > Windows Server > Create a virtual machine

### Create a virtual machine

Basics Disks **Networking** Management Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. [Learn more](#)

#### Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network \* ⓘ GBS-Azure-Marketplace-Win2019-vnet  
[Create new](#)

Subnet \* ⓘ default (10.1.0.0/24)  
[Manage subnet configuration](#)

Public IP ⓘ (new) iQSuitePublicIP  
[Create new](#)

NIC network security group ⓘ ☐ None ☐ Basic ☒ Advanced

Configure network security group \* GBS-Azure-Marketplace-Win2019-NSG  
[Create new](#)

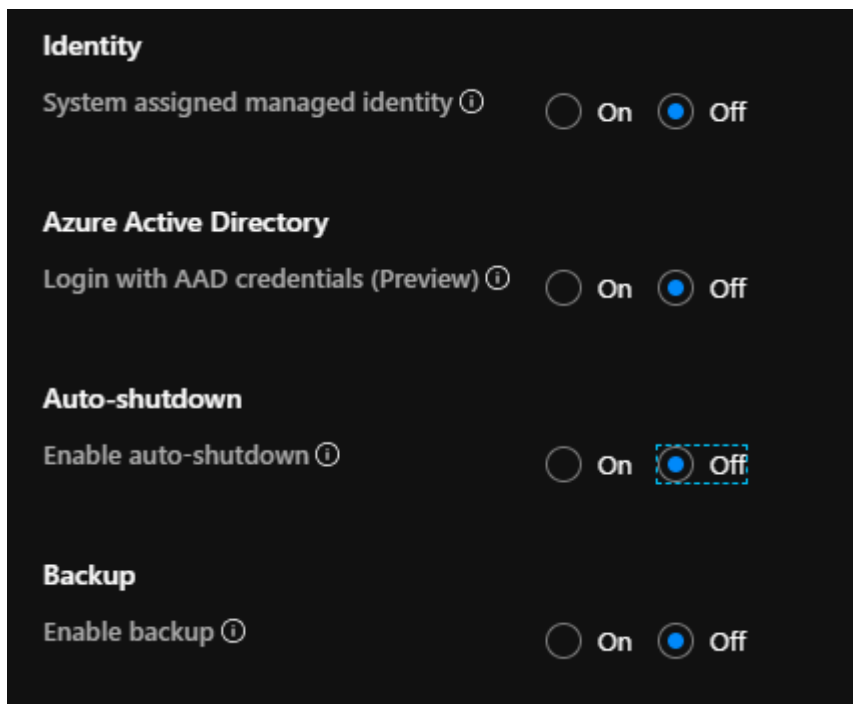
Accelerated networking ⓘ ☐ On ☒ Off  
The selected VM size does not support accelerated networking.

#### Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more](#)

Place this virtual machine behind an existing load balancing solution? ☐ Yes ☒ No

9. Under Management, activate the 'OS guest diagnostics' setting.
10. Deactivate the 'Auto-Shutdown' option.  
For the other settings, you can leave the default options.

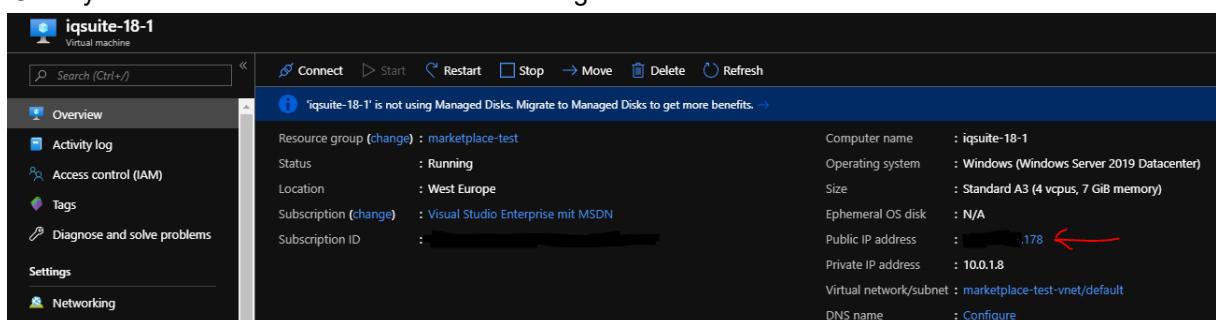


11. Under 'Advanced' and 'Tags', you do not need to change anything else.
12. Finally, review and check all settings of the VM, before starting the creation.

## 2.2.2 Defining a Fixed DNS Name for the VM

After the VM creation, you should also define a fixed DNS name for the VM in addition to the fixed IP. You can do this via the configuration menu of the assigned IP address.

1. Go to your Virtual machine and click on the assigned 'Public IP address':



2. Make sure that the IP assignment is set to 'Static' and enter a label in the field 'DNS name label'. With this you will set a global FQDN for your Azure VM. Here you can also note your static IP for your Azure VM.

Dashboard > iqsuite-18-1 > iqsuite-18-1-ip - Configuration

### iqsuite-18-1-ip - Configuration

Public IP address

Search (Ctrl+/) <<

Save Discard

Assignment  
☐ Dynamic ☒ Static

IP address ⓘ  
[REDACTED].178

Idle timeout (minutes) ⓘ  
 4

DNS name label (optional) ⓘ  
iqsuite-18-1 ✓  
.westeurope.cloudapp.azure.com

Alias record sets  
Want to closely track this Public IP address? Create an alias record in Azure DNS. [Learn more.](#)  
[+ Create alias record](#)

Subscription	DNS zone	Name	Type	TTL
No results.				

- Click on SAVE to finish the VM configuration.  
No other VM settings need to be changed.

## 3 Setting up the Azure VM Environment

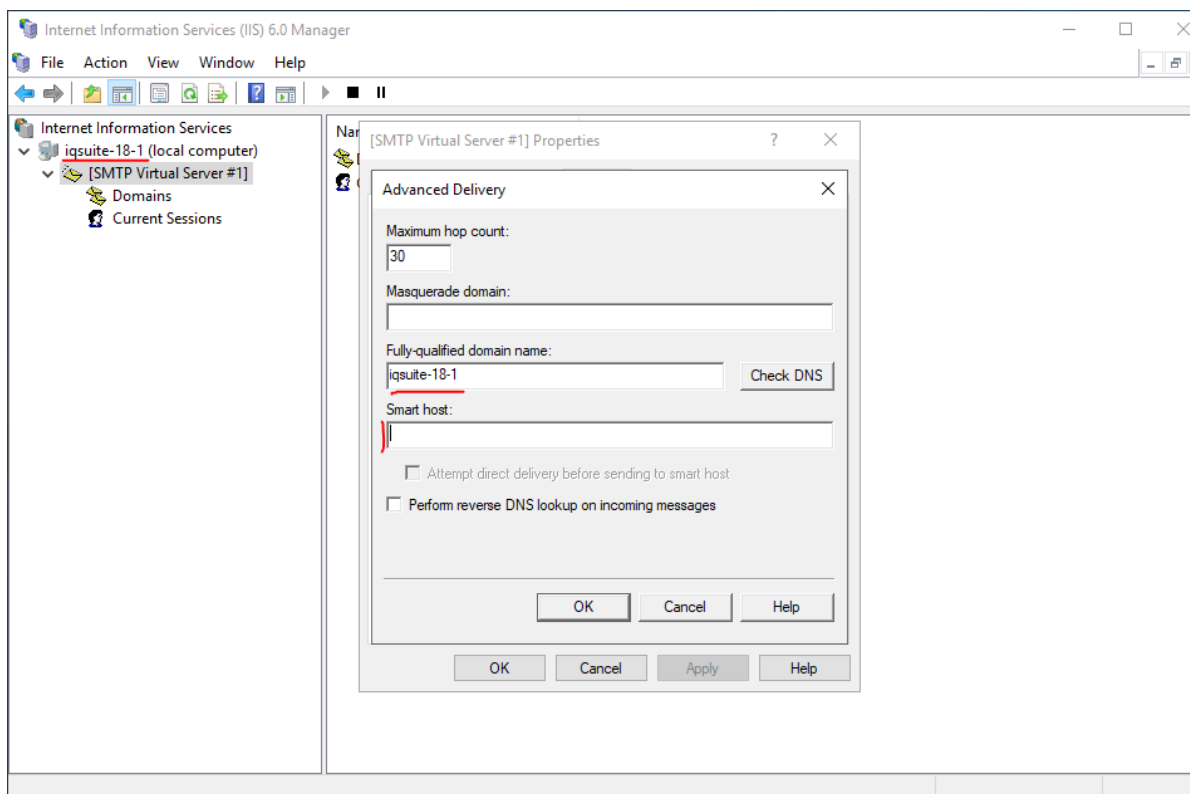
### 3.1 General Configuration

If a virus/malware scanner (e.g. Windows Defender) is active on the VM, set exceptions for the following directories to avoid on-access errors:

**C:\inetpub** and **C:\Program Files\GBS\iQ.Suite\GrpData**

### 3.2 SMTP Server Configuration

1. Open the **Advanced Delivery** dialog (SMTP PROPERTIES -> 'DELIVERY' TAB -> 'ADVANCED' BUTTON) and set the FQDN of the SMTP server. By default, the name of the VM image is specified.
2. To verify whether the specified FQDN is valid, click on the **CHECK DNS** button:

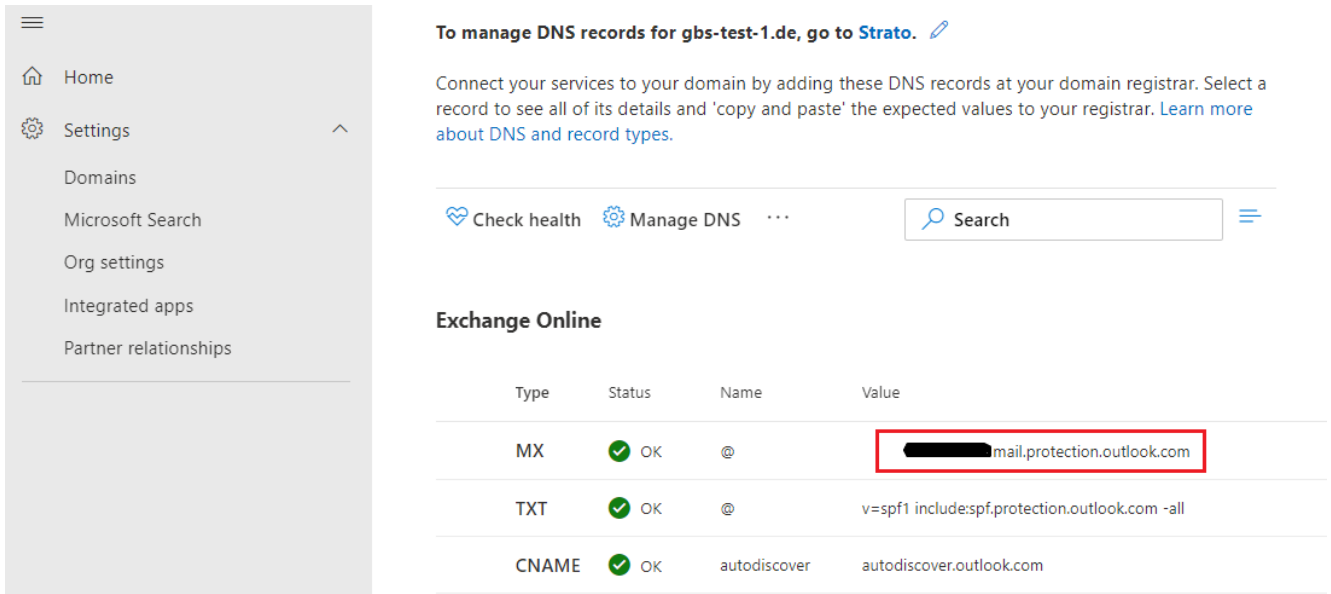


3. Enter the smart host which should be used. For Microsoft 365, the smart host is the MX Record of your used domain.

In order to re-integrate the emails into the M365 mail flow, a smart host must be used. This is only possible for external domains and not for internal Microsoft domains. Without this smart host setting, the emails are directly sent from the Azure VM and not from the actual M365 mail server.

The smart host is identical to your MX Record of your used domain in Microsoft 365. You can find this Record in the Admin Center.

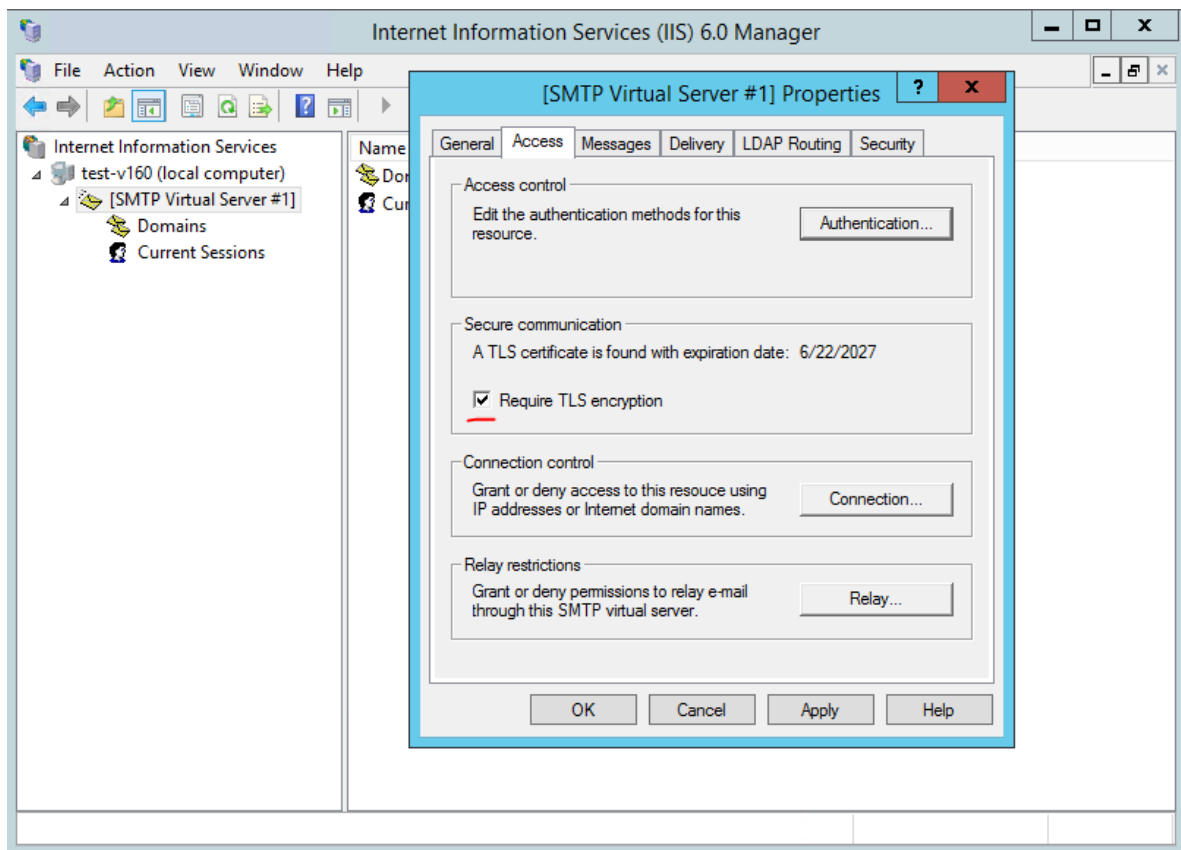
4. In the Microsoft 365 Admin Center, select your domain under SETTINGS -> DOMAINS:



The screenshot shows the Microsoft 365 Admin Center interface. On the left is a navigation pane with options: Home, Settings (selected), Domains, Microsoft Search, Org settings, Integrated apps, and Partner relationships. The main content area is titled 'To manage DNS records for gbs-test-1.de, go to Strato.' and includes a link to 'Learn more about DNS and record types.' Below this, there are buttons for 'Check health' and 'Manage DNS'. A search bar is also present. The 'Exchange Online' section displays a table of DNS records:

Type	Status	Name	Value
MX	✓ OK	@	mail.protection.outlook.com
TXT	✓ OK	@	v=spf1 include:spf.protection.outlook.com -all
CNAME	✓ OK	autodiscover	autodiscover.outlook.com

5. After having added your smart host, close the window with OK and click APPLY to save the configuration. Then, close the **Properties** dialog with OK as well.
6. Open the **Properties** dialog again and, in the **Access** tab, activate the TLS encryption:

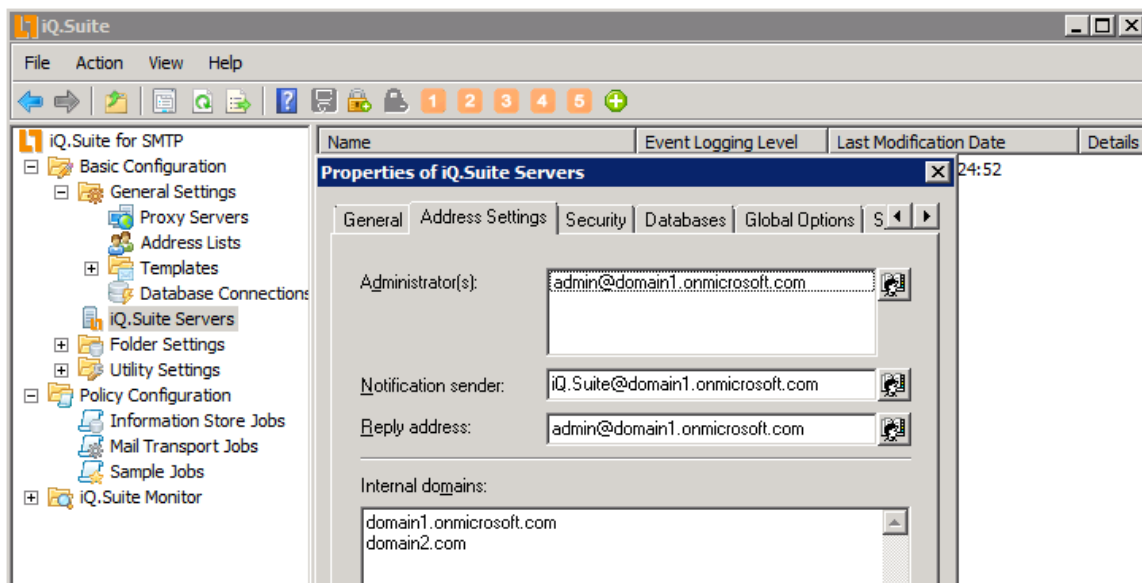


The Properties window only updates after closing and opening again. Only after re-opening the window, the TLS can be activated.

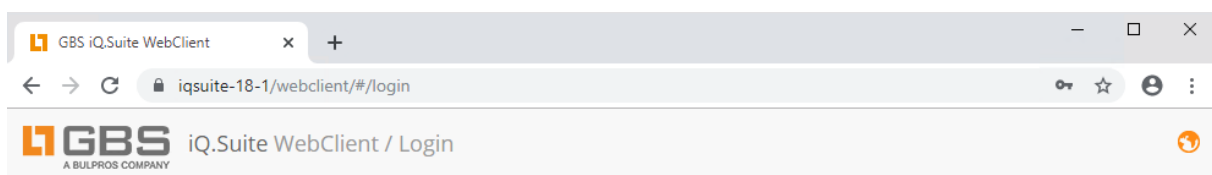
7. Save with APPLY and exit with OK.
8. Restart the SMTP server.

### 3.3 iQ.Suite Configuration

1. Open iQ.Suite and add your Microsoft 365 domains as internal domains in the properties of iQ.Suite Servers (to access the properties, right-click on IQ.SUITE SERVERS):



2. Now, you can configure some jobs. To start, we recommend just a Trailer job.
3. You should be able to log in to the already opened iQ.Suite WebClient with your local administrator account and the corresponding password.  
 Url of the local WebClient: **`https://<vm-hostname>/webclient`**



**iQ.Suite WebClient**

Administration of email management environment via iQ.Suite WebClient.

© GBS Europa GmbH 2019 | UI: 18.1.0.5516

## 3.4 Additional Information and Configuration

The passwords for the SQL SA user, iQ.Suite Remoting (Global password), the self-signed certificate for the SMTP, and the iQSuite SQL user are auto-generated as random, complex passwords and encrypted to be saved in a configuration file to be used during the automated setup. For this PowerShell uses the Windows Data Protection API (DPAPI) to encrypt/decrypt your passwords. This means that it will only work for the same user on the same machine.

If you are going to use the environment in a productive way, you should change all generated passwords and use your own certificate for the SMTP TLS communication. The generated passwords are saved as Strings initially during the automated setup in the transcript (C:\iQSuite-Azure-Automation\GBS-PowerShell-Management\Initialize-iQSuiteAzure.log), so after saving the passwords you should delete them from the transcript as a security measure.

## 3.5 Monitoring the Mail Flow Status

Through the automated PowerShell setup of the Azure VM, an internal iQ.Suite monitoring task will also be activated. This task by default will run every 10 minutes to monitor the mail flow. This includes the monitoring of the following directories:

- C:\inetpub\mailroot\Badmail
- C:\inetpub\mailroot\Queue

Each time the task is executed, Event log entries are created by default. These entries can be used to verify the current status of the mail flow. Each monitored directory has its own Event log entry and Event ID.

The default threshold settings for the creation of Event log entries for the Queue are as follows:

- Less than 25 items in a directory => Event log entry with **Information** level
- More than 25 items, but less than 50 items in a directory => Event log entry with **Warning** level
- More than 50 items in a directory => Event log entry with **Error** level

The default threshold settings for the creation of Event log entries for the Badmail are as follows:

- Less than 10 items in a directory => Event log entry with **Information** level
- More than 10 items, but less than 20 items in a directory => Event log entry with **Warning** level
- More than 20 items in a directory => Event log entry with **Error** level

If you want to change those thresholds, you can do so within the registry under the following key:

HKEY\_LOCAL\_MACHINE\SOFTWARE\GBS\iQ.Suite\ControlService\SMTPMonitoring



You can also change the time interval, in which the monitoring checks the directories. For this you have to change the decimal value of the 'CheckTimeout' registry key to another value. Per default it is set to 600, which means 600 seconds / 10 minutes.

**Notification emails** can be sent in case a monitored threshold for a directory is met. By default, no notification is sent. To enable the sending of notifications, adjust the registry under the following key:

HKEY\_LOCAL\_MACHINE\SOFTWARE\GBS\iQ.Suite\ControlService\MailReporting

- Add the data of an email account, e.g. a Microsoft 365 or Google account
- Set the 'Enabled' registry key to 1 to activate the sending of notification emails.

This way, notification emails can be sent in case the error threshold is met.

In some cases, the SMTP queue might have some stuck emails which are left without actually being sent. To resolve such a situation, the SMTP service has to be restarted. The restart action is activated by default in the monitoring task. So, if you encounter an increasing amount of stuck mails in the SMTP queue directory, the SMTP service will be restarted automatically. The restart action will only be executed in case the error threshold of the Queue is met.

You can disable the automatic restart of the SMTP service by setting the value of the `AutoRestartSMTPSvcEnabled` Registry key to **0**.

## 4 Setting up the Microsoft 365 Environment

If you are already using your Microsoft 365 tenant in a productive way, you should configure the transport rule to be valid not for all emails but, to begin with, just for one specific email address (refer to [4.5 Creating Exchange Mail Rules](#)). This way, your regular mail flow will not be disturbed, but you can still use your Microsoft 365 tenant with the iQ.Suite environment.

### 4.1 Guid for Message Header

Before creating the Microsoft 365 environment, you will need to get the Guid, which was created during the automated setup. To do so, open the following XML file and copy the value of the Guid node under “userData” inside of:

"C:\iQSuite-Azure-Automation\GBS-PowerShell-Management\configuration.xml"

Example: <Guid>your-created-guid</Guid>

**This Guid is tenant-specific and will also need to be added to the Exchange Online transport rules.** Therefore, in case you use multiple Azure VMs (e.g. for High availability), you will need to use the same Guid for all machines. This Guid is automatically added to a iQ.Suite registry key during the setup. It is used to tag your processed emails to ensure that no loop exists in the mailflow.

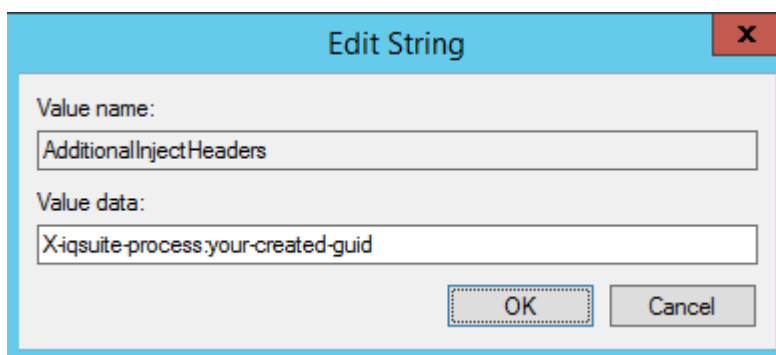
The used registry key “**AdditionalInjectHeaders**” can be found under:

HKEY\_LOCAL\_MACHINE\SOFTWARE\GBS\iQ.Suite\Inject

The value of this key has to be the same for all used Azure VMs. This Guid also has to be added to the transport rules, which will be created in the next steps.

Example value with a Guid:

X-iqsuite-process:657a43d3-f52a-4969-93aa-60cfc012e1d6



## 4.2 Requirements for Microsoft 365 SMTP Relay

- **Static IP address or address range:** Most devices or applications are unable to use a certificate for authentication. To authenticate your device or application, use one or more static IP addresses that are not shared with another organization.
- **Connector:** You must set up a connector in Exchange Online for email sent from your device or application.
- **Port:** Port 25 is required and must not be blocked on your network or by your Internet Service Provider.
- **Licensing:** SMTP relay doesn't use a specific Microsoft 365 mailbox to send email. Therefore, it is important that only licensed users send emails from devices or applications configured for SMTP relay.

## 4.3 Limitations for Microsoft 365 SMTP Relay

- Sent mails can be disrupted if your IP addresses are blocked by a spam list.
- Reasonable limits are imposed for sending.
- Requires static unshared IP addresses.

For information on the requirements and limitations of Microsoft 365 SMTP Relay, please refer to [https://technet.microsoft.com/en-us/library/dn554323\(v=exchg.150\).aspx?f=255&mspperror=-2147217396#option3](https://technet.microsoft.com/en-us/library/dn554323(v=exchg.150).aspx?f=255&mspperror=-2147217396#option3)

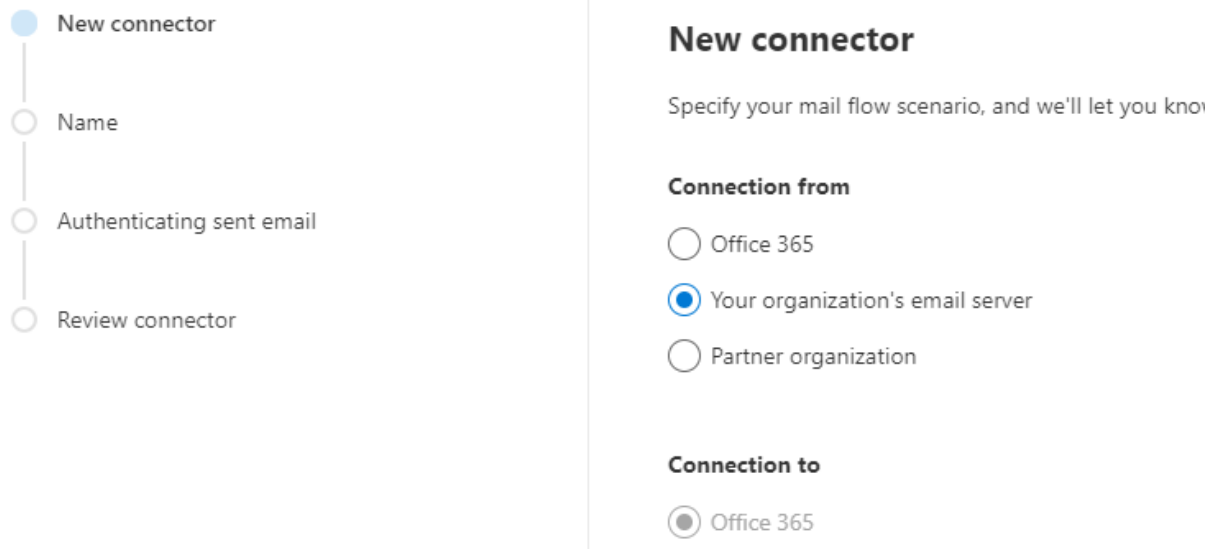
## 4.4 Creating Connectors

In the Microsoft 365 Admin Portal, click on the **Administrator** menu to open the Exchange Online Configuration Portal. There, select MAIL FLOW. In the newly opened menu, create the connectors **Azure VM to M365** and **M365 to Azure VM**:

### 4.4.1 Azure VM to M365

From: 'Your organization's email server' (SMTP on Azure VM) -> To: Office 365 (Microsoft 365)

1. In the Exchange Admin Center, click on CONNECTORS -> MAIL FLOW -> + (NEW):

**Add a connector**

**New connector**

Specify your mail flow scenario, and we'll let you know what to do next.

**Connection from**

☐ Office 365

☒ Your organization's email server

☐ Partner organization

**Connection to**


☒ Office 365

2. Click NEXT and specify a name for the connector, e.g. 'FROM Azure VM to M365'.
3. Click NEXT and configure the connector:

## Authenticating sent email

How should Office 365 identify email from your email server?

Choose how Office 365 will authenticate and accept email sent from your email server.

- ☐ By verifying that the subject name on the certificate that the sending server uses to authenticate with Office 365 matches the domain entered in the text box below (recommended)
- Example: contoso.com or \*.contoso.com
- ☒ By verifying that the IP address of the sending server matches one of the following IP addresses, which belong exclusively to your organization
- 192.168.0.1 

4. Here, add the static public IP of the Azure-VM on which the SMTP server is installed.

### 4.4.2 M365 to Azure VM

From: Microsoft 365 -> To: 'Your organization's email server' (SMTP on Azure VM)

1. In the Exchange Admin Center, click on CONNECTORS -> MAIL FLOW -> + (NEW):
2. Specify the use of a transport rule to redirect all incoming and outgoing emails to your Azure VM with iQ.Suite:

## Use of connector

Specify when you want to use this connector.


- ☐ For email messages sent to all accepted domains in your organization
- ☒ Only when I have a transport rule set up that redirects messages to this connector
- ☐ Only when email messages are sent to these domains

3. Enter the FQDN or the static IP of your Azure VM with the SMTP server:

## Routing

How do you want to route email messages?

Specify one or more smart hosts to which Office 365 will deliver email messages. A smart host is an alternative server and can be identified by using a fully qualified domain name (FQDN) or an IP address.

Example: myhost.contoso.com or 192.168.3.2	+
azuresmtpab12r2.cloudapp.net	

4. For the email traffic between your mail server and M365, you must activate the encryption protocol 'TLS' in the connector and use a valid certificate:

## Security restrictions

How should Office 365 connect to your email server?

☒ Always use Transport Layer Security (TLS) to secure the connection (recommended)

Connect only if the recipient's email server certificate matches this criteria

☒ Any digital certificate, including self-signed certificates

☐ Issued by a trusted certificate authority (CA)

☐ And the subject name or subject alternative name (SAN) matches this domain name:

Example: contoso.com or \*.contoso.com

## 4.5 Creating Exchange Mail Rules

### 4.5.1 Rule for mail forwarding

1. In the Exchange Admin Center, click on MAIL FLOW -> RULES -> + (NEW):
2. Choose **More Options** to configure the rule.

## Route all Mails to own Azure VM

Name:

\*Apply this rule if...

\*Do the following...  
 [FROM O365 to Azure VM](#)

Except if...  
☒  ['x-igsuite-process' header includes 'processed'](#)

Properties of this rule:

Priority:

☒ Audit this rule with severity level:



Choose a mode for this rule:


☒ Enforce  
☐ Test with Policy Tips  
☐ Test without Policy Tips

### Important:

Instead of the message header value “processed”, add your Guid here, the same Guid that is described in chapter [4.1 Guid for Message Header](#).

specify words or phrases



**657a43d3-f52a-4969-93aa-60cfc012e1d6**

☐ Activate this rule on the following date:  
Tue 12/13/2016 8:00 AM

☐ Deactivate this rule on the following date:  
Tue 12/13/2016 8:00 AM

☐ Stop processing more rules

☐ Defer the message if rule processing doesn't complete

Match sender address in message:  
Envelope

## 4.5.2 Rule for mail approval

1. In the Exchange Admin Center, click on MAIL FLOW -> RULES -> + (NEW).
2. Choose **More Options** to configure the rule. The IP is the Public IP of the Azure VM.

Approve all Mails from own SMTP Server on Azure VM

Name:  
Approve all Mails from own SMTP Server on Azure VM

\*Apply this rule if...

× A message header includes... ['x-iqsuite-process'](#) header includes ['processed'](#)

and

× Sender's IP address is in the range... ['50.51.52.53'](#)

add condition

\*Do the following...

Set the spam confidence level (SCL) to... [Bypass spam filtering](#)

You don't need to create a transport rule to bypass spam filtering or mark email as spam for a sender or domain. Click here to use an [allow or block list in the spam filter](#).

add action

Except if...

add exception

### Important:

Instead of the message header value “processed”, add your Guid here. The same Guid that is described in chapter [4.1 Guid for Message Header](#).



Properties of this rule:

Priority:

4

☒ Audit this rule with severity level:

Not specified ▼

Choose a mode for this rule:

☒ Enforce

☐ Test with Policy Tips

☐ Test without Policy Tips

☐ Activate this rule on the following date:

Wed 9/7/2016 ▼

8:30 AM ▼

☐ Deactivate this rule on the following date:

Wed 9/7/2016 ▼

8:30 AM ▼

☐ Stop processing more rules

☐ Defer the message if rule processing doesn't complete

Match sender address in message:

Header ▼

## 4.6 Optional: Adding SPF Record to the Domain

If you want that your emails which are processed by iQ.Suite on the Azure VM and then forwarded by SMTP are not declared as SPAM, set an SPF Record in your domain configuration. If you use a Microsoft 365 smart host, this is optional.

As an IP address, specify the static public IP of your Azure VM on which the SMTP server is installed. The SPF Record must have the following scheme:

DNS entry	Value
SPF	v=spf1 ip4:<Static IP Address> include:spf.protection.outlook.com ~all

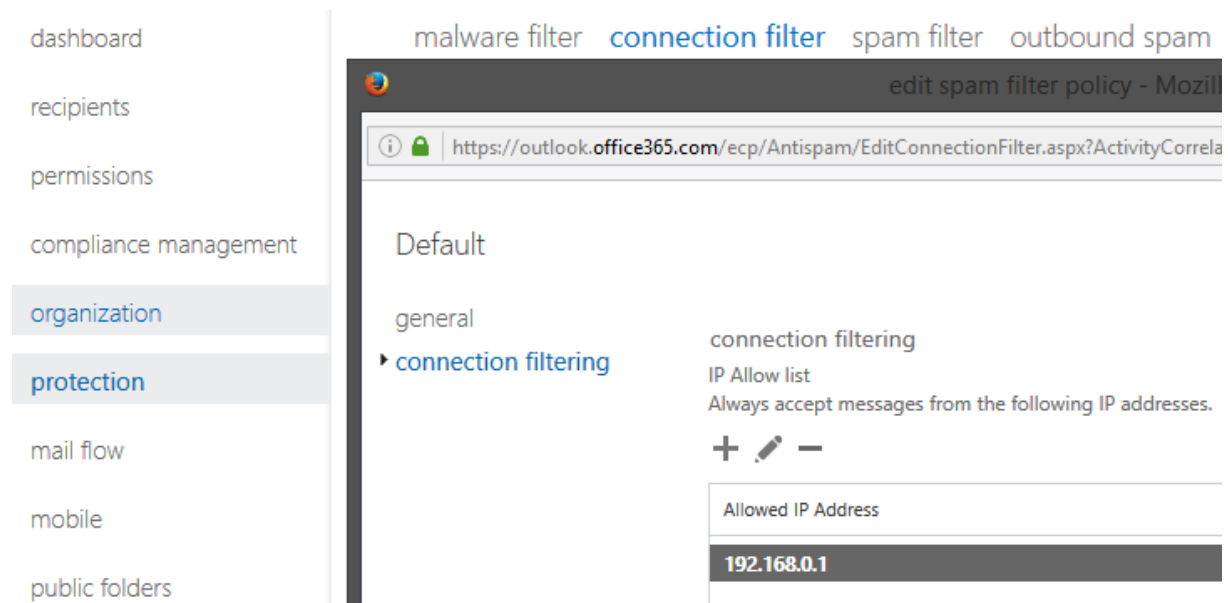
Example of a new entry:

```
v=spf1 ip4:192.168.0.1 include:spf.protection.outlook.com ~all
```

## 4.7 Adding Public IP to the Exchange Filter

In the Exchange Admin Center under PROTECTION -> CONNECTION FILTER, add the static public IP of the Azure VM on which the SMTP is used to the list of the allowed IP addresses:

### Exchange admin center



Save your settings.

## 4.8 Delisting Blocked Public IP (Microsoft)

If the public IP address assigned to your Azure VM is initially blocked (check in SMTP log), delist your IP by using the Microsoft page <https://sender.office.com/Delist>.

Here, you have to specify the IP and a valid email address. After approx. 30 minutes, the IP will be unblocked.



## 4.9 Delisting Blocked Public IP (Spamhaus)

The Public IP assigned to your Azure VM may be inside an IP range which is blocked by Spamhaus. This can happen initially or at a later time. In theory, this can happen once to all Azure IPs because it is not a specific blacklisting, but rather a blocking of IPs which were known as dynamically assigned before but not specified as mail servers.

Check the SMTP log to determine whether your IP is blocked. To delist your IP, proceed as described under <https://www.spamhaus.org/pbl/removal/>.



### PBL Self-Service IP Removal

#### Automatic removal mechanism for single Static IP addresses

This function allows mail server operators with Static IP addresses listed on the PBL (such as IPs within a range previously identified as Dynamic but which has been recently reassigned as Static) to automatically remove their Static IP addresses from the PBL database.

## 5 Configuring WebClient Authentication with Azure AD

For initial testing, this step is not necessary but can still be done.

Users should be able to authenticate to iQ.Suite WebClient via Azure Active Directory (AAD).

Additionally, it should be possible to resolve the group membership via LDIF file (through export from the AAD). The resolution of groups via an LDIF file makes sense in an AAD environment for the following reasons:

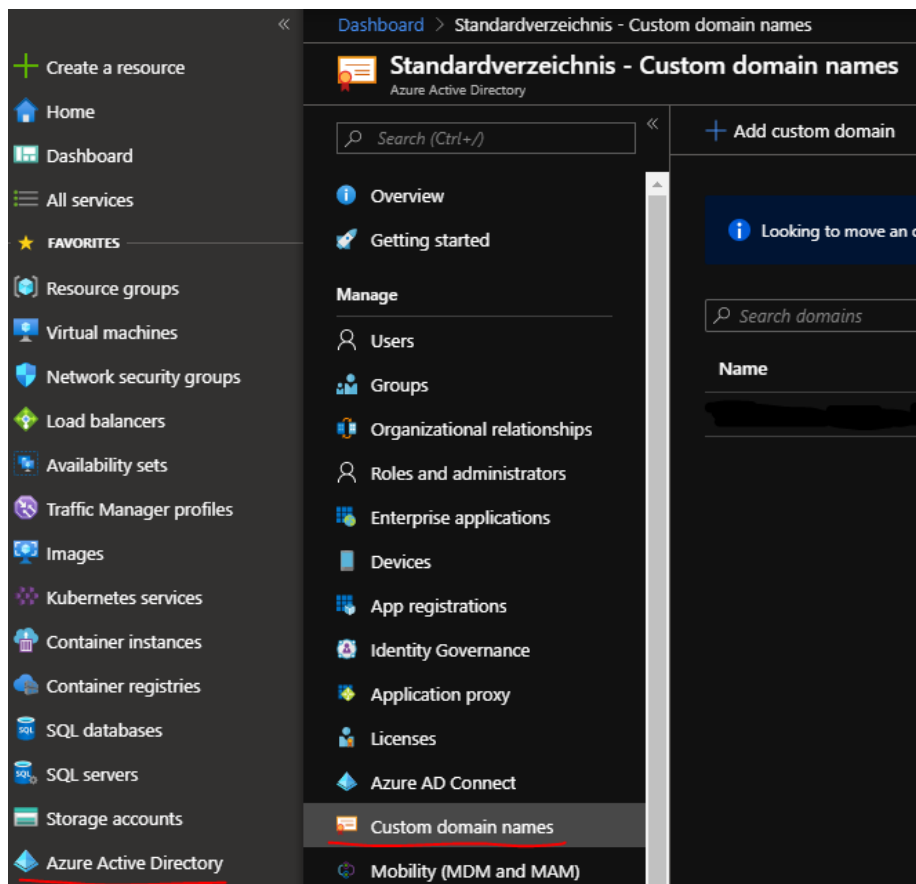
- Accessing the AAD is expensive; with an LDIF file, an access is made only at login time. Additional accesses to the AAD until log-out are only necessary in order to get a **list of users** for the **assignment to roles**. If the **role assignment is based on groups**, no AAD access is required either.
- The same LDIF file can be used by the iQ.Suite backend and frontend as well, so that here **consistent group memberships** are available for all sections.

The following sections describe the requirements for authentication to the WebClient via Azure Active Directory.

### 5.1 Setting up the Azure Active Directory

Before you run the setup to install iQ.Suite WebClient, proceed as follows:

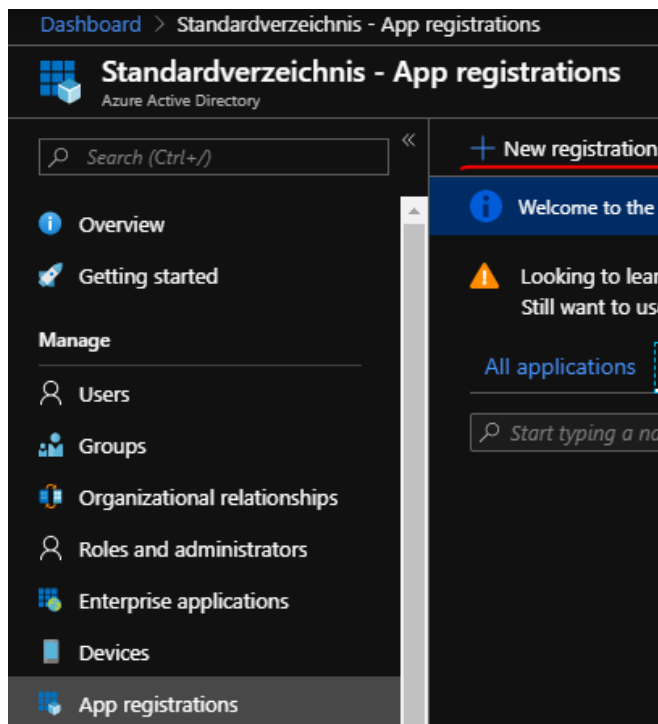
1. Log on to the new Azure Portal: <https://portal.azure.com/>
2. Select in your **user settings** (at the top right) an Azure Active Directory.
3. From the menu (on the left), select AZURE ACTIVE DIRECTORY -> CUSTOM DOMAIN NAMES:



Please note the **domain name**. This name is required in the settings in *dynamic\_configuration.xml*.

### 5.1.1 Creating Azure App for WebClient

1. Select **App registrations** and click on NEW REGISTRATION:



Dashboard > Standardverzeichnis - App registrations > Register an application

## Register an application

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

iQ.Suite - WebClient ✓

**Supported account types**  
Who can use this application or access this API?

☒ Accounts in this organizational directory only (Standardverzeichnis 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 ▼  ✓

2. **Name:** Enter any name.  
Example: iQ.Suite WebClient
3. **Account type:** Select 'Single tenant'.

4. **Sign-on URL:** Specify the URL under which you want the WebClient to be accessible or under which it was installed. The default entry should be the url of the locally installed WebClient, which includes the vm-hostname.

If it should be accessible under different URLs, you can add them later (refer to **Reply URLs** below).

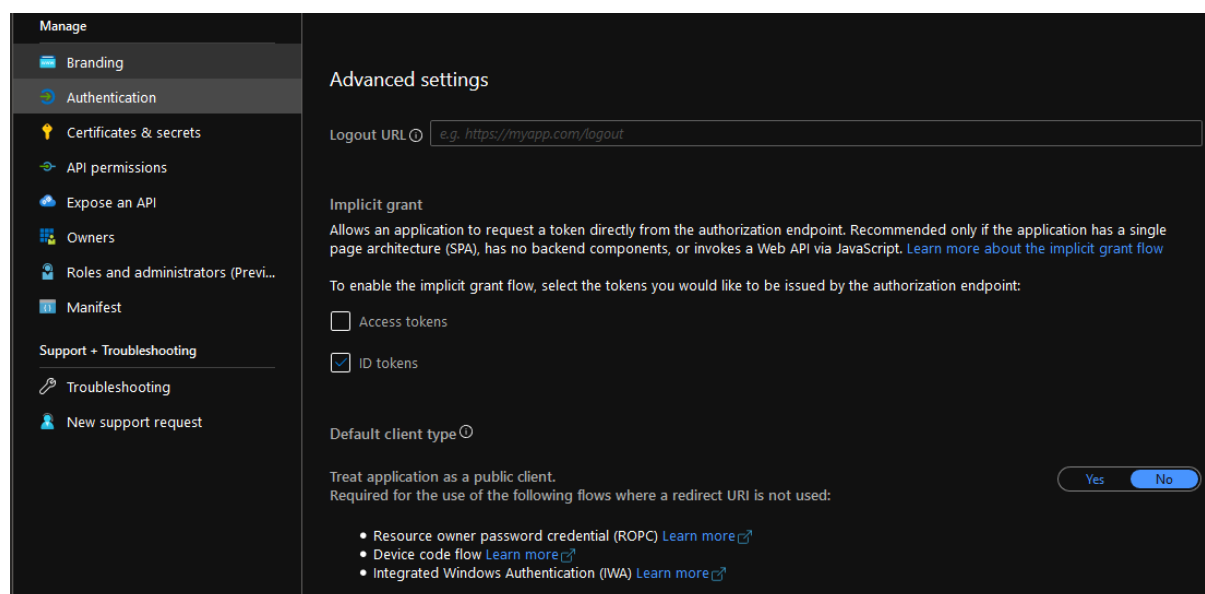
**Important:** All URLs need to have a trailing slash at the end.

The creation of a new application may take a few seconds.

5. Once the app is created, you should be redirected to the new app configuration page.

### 5.1.2 Configuration of the WebClient Azure App

1. Note the **Application ID** which you can see at the top of the page.  
This ID is required in the settings of the *dynamic\_configuration.xml*.
2. Go to **Authentication**. Under **Reply URLs**, enter all URLs under which the WebClient should be available, e.g. custom domains or dns urls.
3. Under Advanced settings, enable the option 'ID tokens'



The screenshot shows the 'Advanced settings' page for an Azure application. On the left, a navigation menu includes 'Manage', 'Branding', 'Authentication' (selected), 'Certificates & secrets', 'API permissions', 'Expose an API', 'Owners', 'Roles and administrators (Previous)', 'Manifest', 'Support + Troubleshooting', 'Troubleshooting', and 'New support request'. The main content area is titled 'Advanced settings' and contains a 'Logout URL' field with a placeholder 'e.g. https://myapp.com/logout'. Below this, the 'Implicit grant' section explains that it allows an application to request a token directly from the authorization endpoint and is recommended for SPAs. It lists three token types: 'Access tokens' (unchecked), 'ID tokens' (checked), and 'Refresh tokens' (unchecked). At the bottom, there is a toggle for 'Treat application as a public client' set to 'No'. Below the toggle, it states 'Required for the use of the following flows where a redirect URI is not used:' and lists three flows: 'Resource owner password credential (ROPC)', 'Device code flow', and 'Integrated Windows Authentication (IWA)', each with a 'Learn more' link.

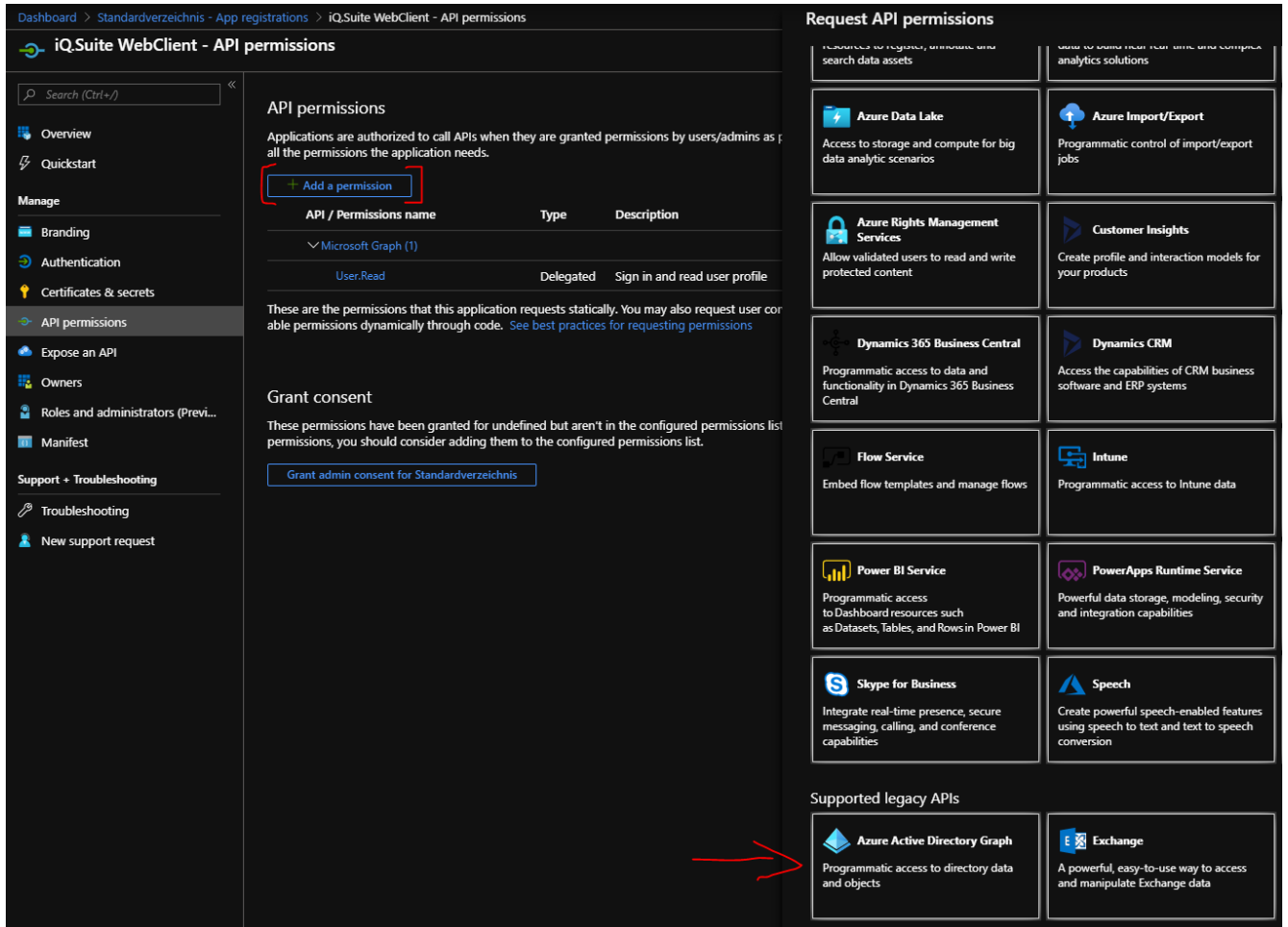
4. Save your changes.
5. Go to **Certificates & secrets**.
6. Under **Client secrets**, create the secret access key to the Azure Active Directory for your application. Please note the secret access key after saving.

**Caution:** You can no longer display the key after leaving this view. Otherwise, a new key would have to be created.

### 5.1.3 Permissions of Azure App WebClient

Under **API permissions**, permissions for a successful access to the Azure Active Directory through the WebClient backend (search for users and groups, resolution of group memberships) must be set:

1. Click on 'Add a permission' and scroll down to choose the 'Azure Active Directory Graph'.



Dashboard > Standardverzeichnis - App registrations > iQ.Suite WebClient - API permissions

#### iQ.Suite WebClient - API permissions

Search (Ctrl+/)

- Overview
- Quickstart
- Manage
  - Branding
  - Authentication
  - Certificates & secrets
  - API permissions**
  - Expose an API
  - Owners
  - Roles and administrators (Previ...
  - Manifest
- Support + Troubleshooting
  - Troubleshooting
  - New support request

#### API permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as all the permissions the application needs.

[+ Add a permission](#)

API / Permissions name	Type	Description
Microsoft Graph (1)		
User.Read	Delegated	Sign in and read user profile

These are the permissions that this application requests statically. You may also request user configurable permissions dynamically through code. [See best practices for requesting permissions](#)

#### Grant consent

These permissions have been granted for undefined but aren't in the configured permissions list. You should consider adding them to the configured permissions list.

[Grant admin consent for Standardverzeichnis](#)

#### Request API permissions

**Azure Data Lake**  
Access to storage and compute for big data analytic scenarios

**Azure Import/Export**  
Programmatic control of import/export jobs

**Azure Rights Management Services**  
Allow validated users to read and write protected content

**Customer Insights**  
Create profile and interaction models for your products

**Dynamics 365 Business Central**  
Programmatic access to data and functionality in Dynamics 365 Business Central

**Dynamics CRM**  
Access the capabilities of CRM business software and ERP systems

**Flow Service**  
Embed flow templates and manage flows

**Intune**  
Programmatic access to Intune data

**Power BI Service**  
Programmatic access to Dashboard resources such as Datasets, Tables, and Rows in Power BI

**PowerApps Runtime Service**  
Powerful data storage, modeling, security and integration capabilities

**Skype for Business**  
Integrate real-time presence, secure messaging, calling, and conference capabilities

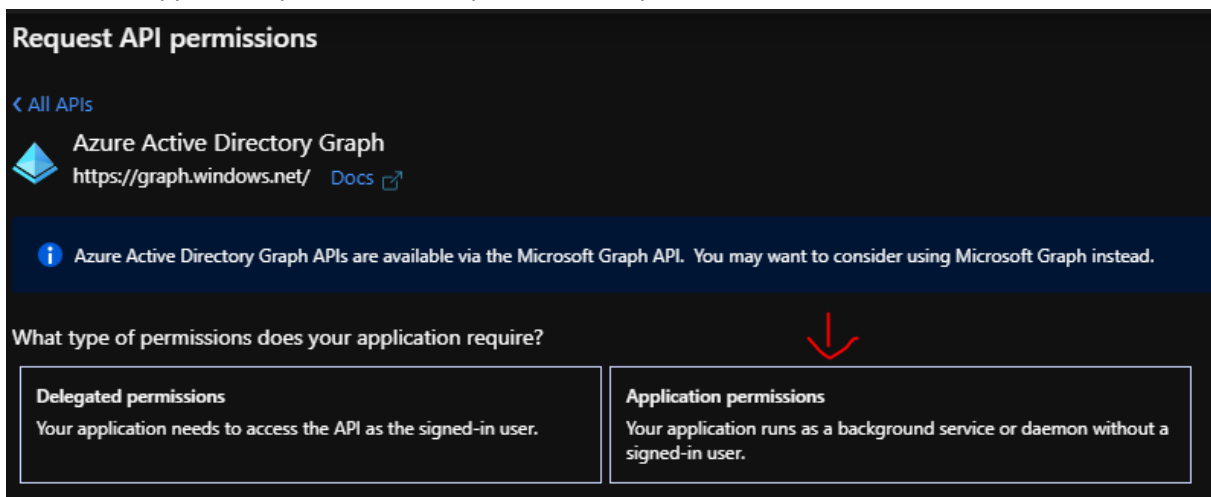
**Speech**  
Create powerful speech-enabled features using speech to text and text to speech conversion

#### Supported legacy APIs

**Azure Active Directory Graph**  
Programmatic access to directory data and objects


**Exchange**  
A powerful, easy-to-use way to access and manipulate Exchange data

2. Select 'Application permissions' as permission requirement.



#### Request API permissions

< All APIs

 **Azure Active Directory Graph**  
<https://graph.windows.net/> Docs

**Azure Active Directory Graph APIs are available via the Microsoft Graph API. You may want to consider using Microsoft Graph instead.**



What type of permissions does your application require?


**Delegated permissions**  
Your application needs to access the API as the signed-in user.

**Application permissions**  
Your application runs as a background service or daemon without a signed-in user.



< All APIs

 **Azure Active Directory Graph**  
<https://graph.windows.net/> [Docs](#) 

 Azure Active Directory Graph APIs are available via the Microsoft Graph API. You may want to consider using Microsoft Graph instead.

What type of permissions does your application require?

**Delegated permissions**  
Your application needs to access the API as the signed-in user.


**Application permissions**  
Your application runs as a background service or daemon without a signed-in user.

Select permissions expand all

Type to search

Permission	Admin Consent Required
> Application	
> Device	
> <b>Directory (1)</b>	
<input checked="" type="checkbox"/> <b>Directory.Read.All</b> Read directory data ⓘ	Yes
<input type="checkbox"/> <b>Directory.ReadWrite.All</b> Read and write directory data ⓘ	Yes
> Domain	
> Member	
> Policy	


- Under **Directory**, select the **Directory.Read.All** permission.
- At the bottom click on 'Add permissions'.
- Add the same permission again, but choose 'Delegated permissions' instead 'Application permissions'.
- After adding those two permissions, you need to add the same '**Directory.Read.All**' permissions for the **Microsoft Graph API** as well.
- Since those permissions require the administrator's confirmation, they must be granted to all accounts (users) in the Directory after saving. For this, click on GRANT ADMIN CONSENT:

 Permissions have changed, please wait a few minutes and then grant admin consent. Users and/or admins will have to consent even if they have already done so previously.

### API permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs.

[+ Add a permission](#)

API / Permissions name	Type	Description	Admin Consent Required	Status
▼ Azure Active Directory Graph (1)				
Directory.Read.All	Application	Read directory data	Yes	 Not granted for Standard...
▼ Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	-	

These are the permissions that this application requests statically. You may also request user consent-able permissions dynamically through code. [See best practices for requesting permissions](#)

### Grant consent

These permissions have been granted for undefined but aren't in the configured permissions list. If your application requires these permissions, you should consider adding them to the configured permissions list.







[Grant admin consent for Standardverzeichnis](#)

8. Finally, the API permissions should look as follows:

Configured permissions

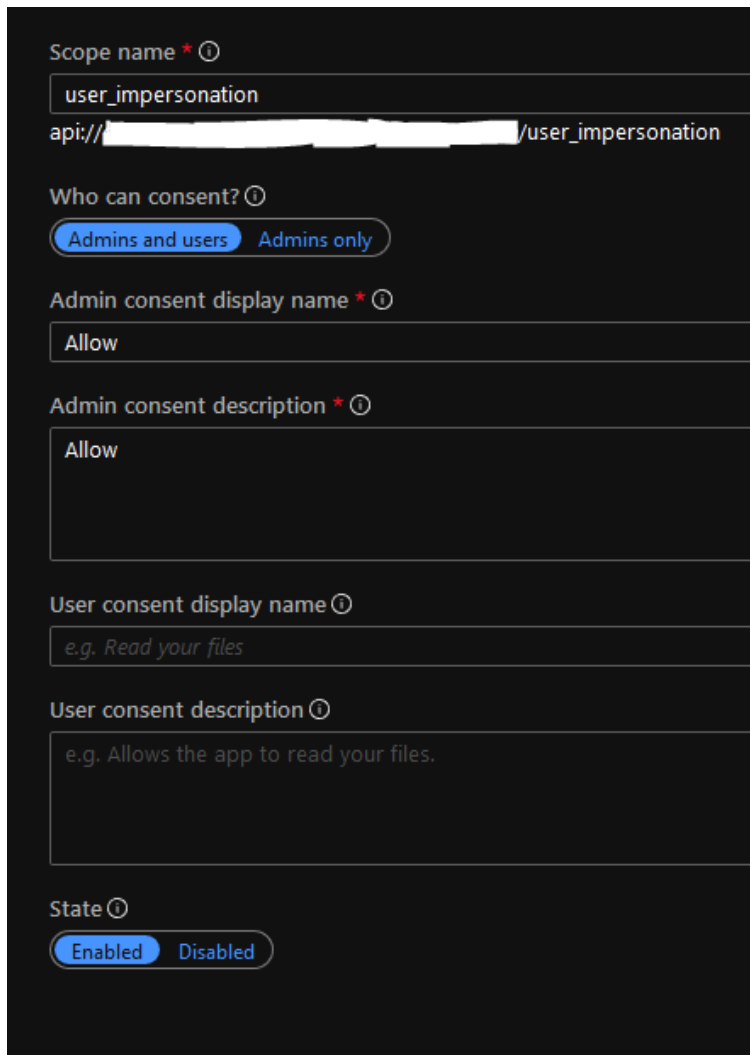
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

[+ Add a permission](#) [✓ Grant admin consent for GBS Europa GmbH](#)

API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Azure Active Directory Graph (3)				
Directory.Read.All	Delegated	Read directory data	Yes	 Granted for GBS Europa... <a href="#">...</a>
Directory.Read.All	Application	Read directory data	Yes	 Granted for GBS Europa... <a href="#">...</a>
User.Read.All	Delegated	Read all users' full profiles	Yes	 Granted for GBS Europa... <a href="#">...</a>
▼ Microsoft Graph (3)				
Directory.Read.All	Delegated	Read directory data	Yes	 Granted for GBS Europa... <a href="#">...</a>
Directory.Read.All	Application	Read directory data	Yes	 Granted for GBS Europa... <a href="#">...</a>
User.Read.All	Application	Read all users' full profiles	Yes	 Granted for GBS Europa... <a href="#">...</a>

*Permissions for User.Read.All only required if LdifSync should export Thumbnails (see TechDoc – LDIF Config -> NoExportUserThumbnails)*

9. Go to 'Expose an API', click on 'Add a scope', and create a scope as follows:



Scope name \* ⓘ  
user\_impersonation  
api://[redacted]/user\_impersonation

Who can consent? ⓘ  
☒ Admins and users ☐ Admins only

Admin consent display name \* ⓘ  
Allow

Admin consent description \* ⓘ  
Allow

User consent display name ⓘ  
e.g. Read your files

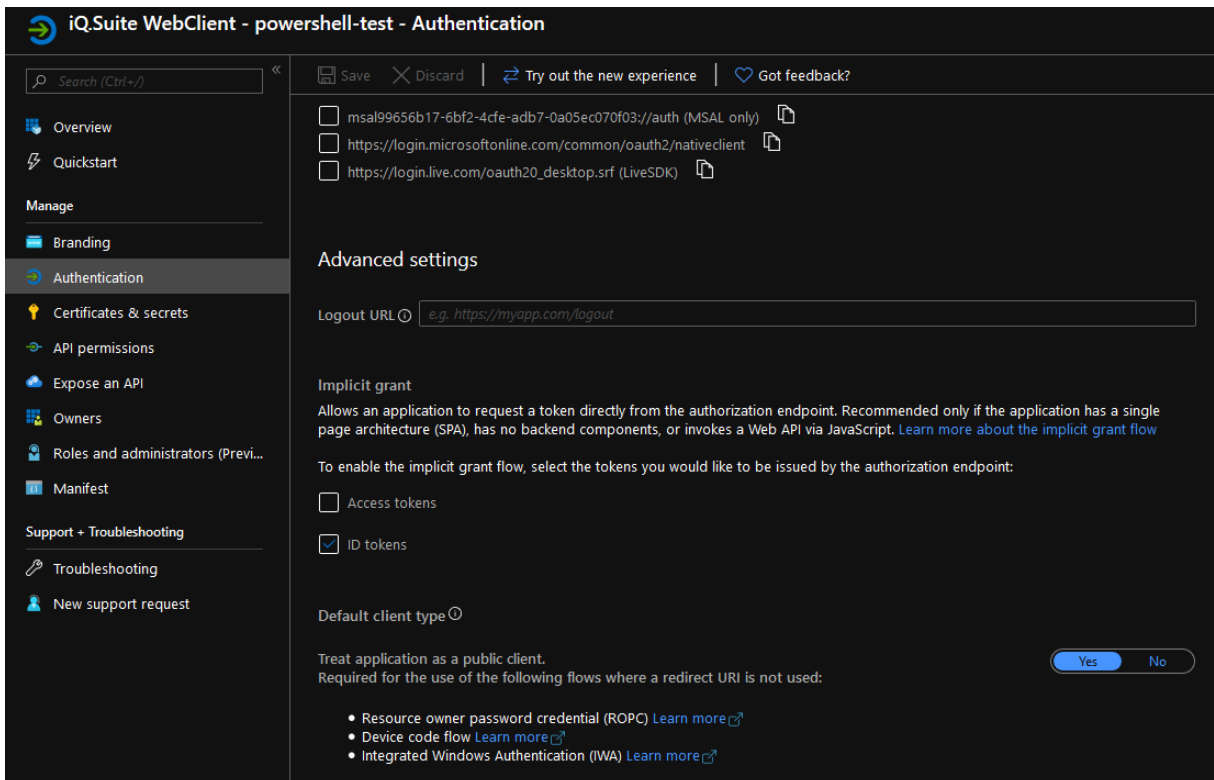
User consent description ⓘ  
e.g. Allows the app to read your files.

State ⓘ  
☒ Enabled ☐ Disabled

### 5.1.4 Creating Azure App for iQ.Suite PowerShell

After having created and configured the Azure App for the WebClient, you need to create another Azure App for the iQ.Suite PowerShell access.

1. After having created this new app, go to the Authentication settings of this app. Activate the option 'ID tokens' and set the option 'Default client type' to 'Yes'



**iQ.Suite WebClient - powershell-test - Authentication**

Search (Ctrl+/) Save Discard Try out the new experience Got feedback?

msal99656b17-6bf2-4cfe-adb7-0a05ec070f03://auth (MSAL only)  
 https://login.microsoftonline.com/common/oauth2/nativeclient  
 https://login.live.com/oauth20\_desktop.srf (LiveSDK)

### Advanced settings

Logout URL

**Implicit grant**  
 Allows an application to request a token directly from the authorization endpoint. Recommended only if the application has a single page architecture (SPA), has no backend components, or invokes a Web API via JavaScript. [Learn more about the implicit grant flow](#)

To enable the implicit grant flow, select the tokens you would like to be issued by the authorization endpoint:

☐ Access tokens  
☒ ID tokens

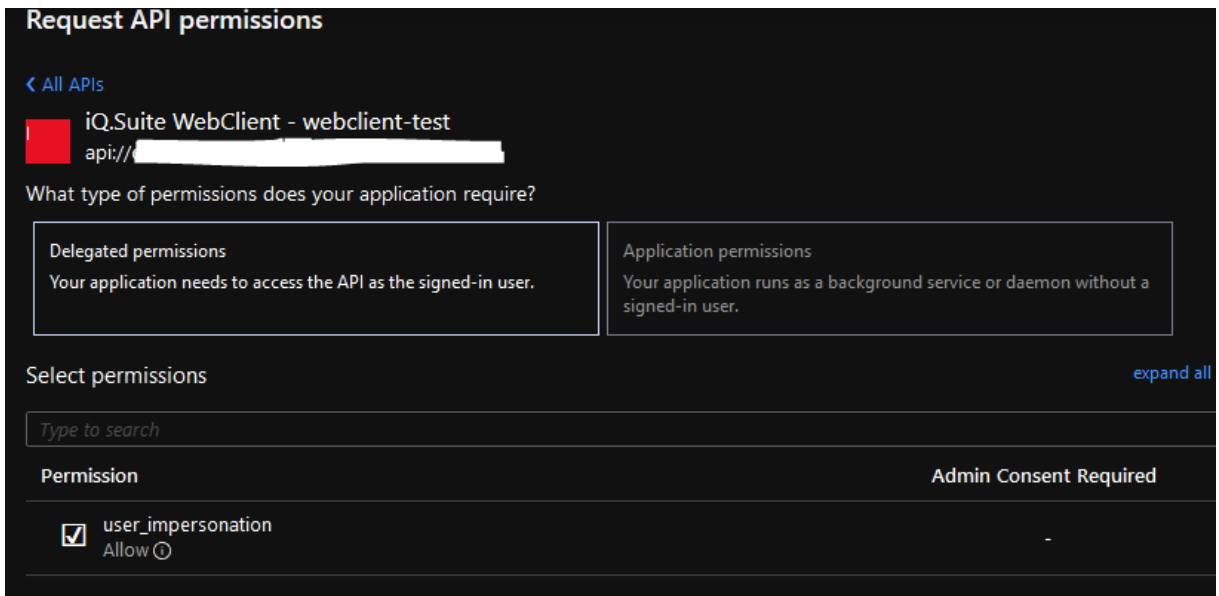
**Default client type**

Treat application as a public client.  
 Required for the use of the following flows where a redirect URI is not used:

- Resource owner password credential (ROPC) [Learn more](#)
- Device code flow [Learn more](#)
- Integrated Windows Authentication (IWA) [Learn more](#)

Yes No

- Go to 'API permissions' and click on 'Add a permission'. Here choose 'My APIs'.  
 Now you should see the exposed API of the Azure app for the WebClient that was created before.
- Click on it and choose 'Delegated permissions'. Select the 'user\_impersonation' permission, that was created before.



### Request API permissions

< All APIs

**iQ.Suite WebClient - webclient-test**  
 api://[redacted]

What type of permissions does your application require?

**Delegated permissions**  
 Your application needs to access the API as the signed-in user.

**Application permissions**  
 Your application runs as a background service or daemon without a signed-in user.

Select permissions [expand all](#)

Type to search

Permission	Admin Consent Required
<input checked="" type="checkbox"/> user_impersonation Allow ⓘ	-

- Click on 'Add permissions'.
- Click on 'Grant admin consent' to allow this permission for the Azure AD.  
 Finally, it should look as follows:

**Configured permissions**

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

[+ Add a permission](#) Preparing for consent

API / Permissions name	Type	Description	Admin Consent Requ...	Status
▼ iqsuite-mc01 (1)				
user_impersonation	Delegated	Access iqsuite-master	-	✔ Granted for GBS
▼ Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	-	✔ Granted for GBS

## 5.2 Settings in the 'dynamic\_configuration.xml'

The dynamic\_configuration.xml for the WebClient has to be changed to authenticate with the Azure Directory. The file can be found under:

*C:\ProgramData\GBS\iQ.Suite WebClient\dynamic\_configuration.xml*

### 5.2.1 Authorization and Group Resolution in Azure AD

Use the access settings to grant access to the Azure Active Directory. Enter the corresponding values in the `Directory` section of the *dynamic\_configuration.xml*:

1. Under **DirectoryType**, change the value to **AZURE**.
2. Under **AzureTenantId**, enter the **domain name** of the Azure Active Directory to be used.  
Example: myazuredirectory.onmicrosoft.com
3. Under **AzureClientId**, enter the **application ID** of the WebClient App (first Azure App).  
Example: 0813E73F-0C81-4D40-A17D-975186FF0478
4. Under **AzurePSClientId**, enter the **application ID** of the PowerShell App (second Azure App).  
Example: 0813E73F-0C81-4D40-A17D-975186FF0478
5. Under **AzureClientSecretKey**, enter the **secret access key** of the WebClient Azure App.  
Example: b8SceHq36Ca/VncDuNV0xNwyqWgBSJTi6hvTX0wa0M=

### 5.2.2 Authorization in Azure AD and Group Resolution in LDIF File

In addition to the settings under [5.2.1](#), the following settings have to be set:

1. **LDIFFilename**:
  - Complete (absolute) path to the LDIF file to be used for the group resolution, if an LDIF file should be used.

- If Azure only authentication should be used without an LDIF file, this field should be empty.
  - If the LDIF Sync is later configured, this should be set to the synced LDIF file.  
E.g. C:\Program Files\GBS\iQ.Suite\Config\iQSuite.ldf
2. **AzureIdentifierLDIFField**: Field of an LDIF entry which contains the **Object ID** of the respective Azure object. For the authentication with Azure AD and our LDIF exports, this field has to be set as *externalid*, if it is not set already.
  3. For the group resolution in the Azure Active Directory, a **call per group** is made to determine the group members. In order to limit the accesses, the recursion depth can be set to a smaller maximum value (default: 10) in the `Directory` section under `AzureGroupSearchDepth`, like for the on-premise Active Directory.
  4. `Roles/AdminGroups`: Enter an Azure user group that should have admin access to the WebClient.

## 5.3 Resetting the SecurityContext

After all settings have been made, the *SecurityContext*, which contains all permissions, must be re-initialized. For this, in the `dynamic_configuration.xml` accesses the value `true`.

**Caution:** Set the appropriate group(s) under `Roles/AdminGroups`, because only users in this/these group(s) have access to the WebClient until the individual access permissions have been defined by an administrator. With **Azure authentication**, this group should therefore also be an **Azure user group**.

Afterwards, the WebClient WebApp must be re-started in the IIS. At this occasion, a backup of the *SecurityContext* (if available) is made and a new *SecurityContext* with the standard permissions is created.

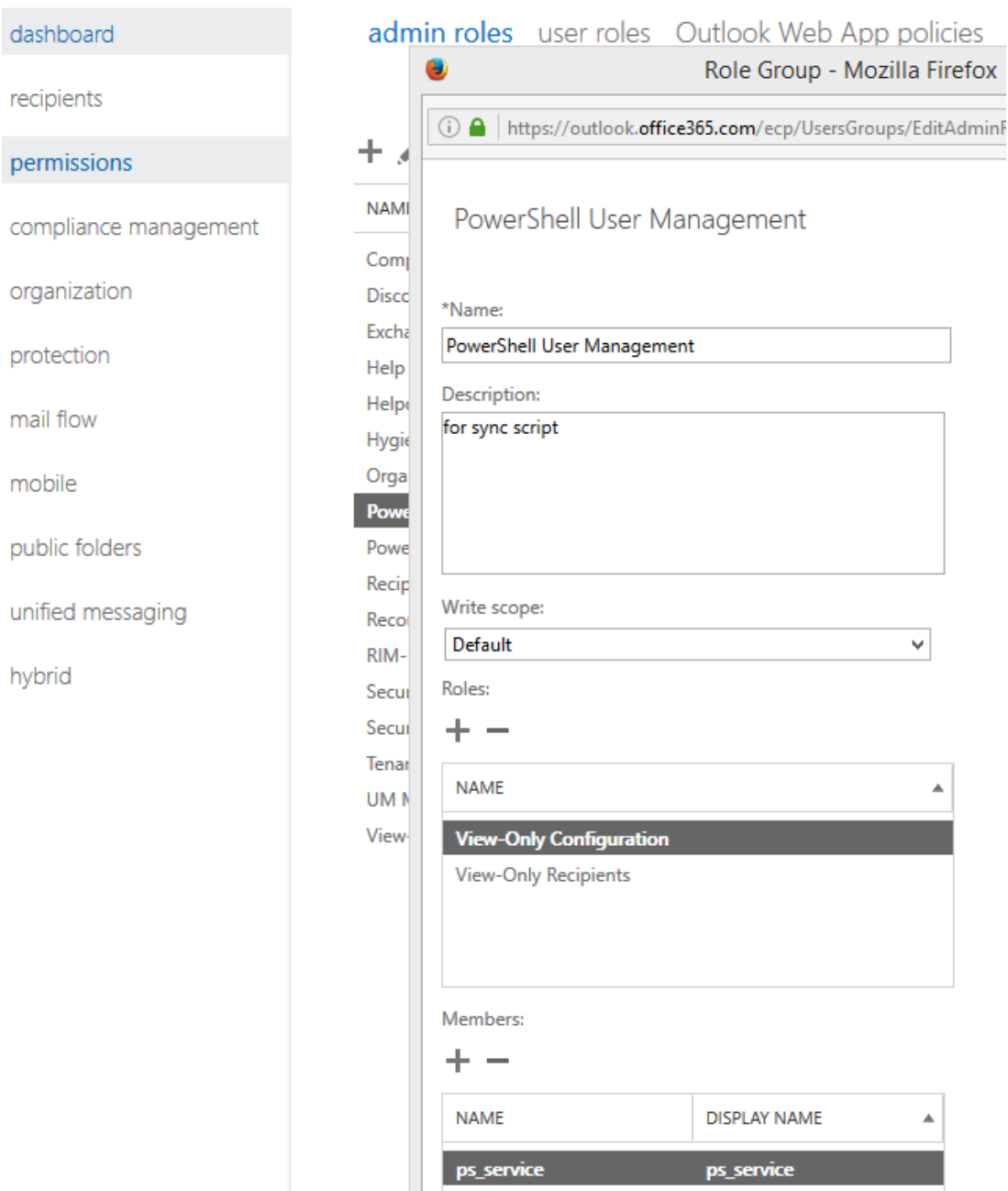
## 5.4 LDIF Sync of Exchange Online directory

For initial testing, this step is not necessary but can still be done.

*Recommendation:* Create a new M365 user (e.g. `ps_service@domain.com`). With this user, the Sync will automatically run later on with a Scheduled Task on the Azure VM. Since this user does not need a mailbox, you do not have to assign a M365 license. Login with the new user in the Microsoft 365 portal, to verify whether the user was created and works, before you continue.

1. In the Exchange Admin Center under **Permissions**, create a new admin role group for the sync user:

## Exchange admin center



admin roles user roles Outlook Web App policies

Role Group - Mozilla Firefox

https://outlook.office365.com/ecp/UsersGroups/EditAdminf

PowerShell User Management

\*Name:  
PowerShell User Management

Description:  
for sync script

Write scope:  
Default

Roles:  
+ -

NAME
View-Only Configuration
View-Only Recipients

Members:  
+ -

NAME	DISPLAY NAME
ps_service	ps_service

It may take up to 10 minutes before the changes in the Exchange Online permissions apply.

- Next you need to enter the user credentials and the Azure app settings in the configuration file of the LDIF sync tool. You can find the configuration file under :  
`"C:\Program Files\GBSVQ.Suite\GrpData\LdifGen\LdifGenCfg.xml"`
- After having added your app and user credentials and changed some values, your configuration should look like this :

```
<?xml version="1.0"?>
<LdifGenCfg xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <Active>true</Active>
  <UseCustomProperties>false</UseCustomProperties>
  <WebClientUri>https://iqsuite-18-1/webclient</WebClientUri>
  <User>admin@yourdomain.onmicrosoft.com</User>
  <Password></Password>
  <PasswordEncrypted></PasswordEncrypted>
  <UseWebClient>false</UseWebClient>
  <AzureTenantId>yourdomain.onmicrosoft.com</AzureTenantId>
  <AzureClientId>d2j1a34b-87xy-331f-aecd-293g4386728b</AzureClientId>
  <AzureClientSecretKey></AzureClientSecretKey>
  <AzureClientSecretKeyEncrypted></AzureClientSecretKeyEncrypted>
  <O365User>sync_service@yourdomain.onmicrosoft.com</O365User>
  <O365Password></O365Password>
  <O365PasswordEncrypted></O365PasswordEncrypted>
  <AzureGroupSearchDepth>5</AzureGroupSearchDepth>
</LdifGenCfg>
```

#### 4. Important: Make sure that

- 'Active' is set to true
- 'UseWebClient' is set to false
- 'WebClientUri' is set to your local WebClient URL
- 'User' and 'Password' are set to a user that has Admin access to the WebClient
- All Azure entries are changed to the values of your Azure tenant and the WebClient Azure app
- The 'M365User' is set to the Microsoft 365 user that was created before with the specified permissions.

If you also want to use custom attributes for your Sync, then you need to set

'UseCustomProperties' to true and enter your properties in the following configuration file:

"C:\Program Files\GBS\iQ.Suite\GrpData\LdifGen\LdifGenCfgCustom.xml"

5. Restart the service 'iQ.Suite LDIF Generator Service' and check the LDIF file under C:\Program Files\GBS\iQ.Suite\Config\iqsuite.ldf for verification. It should now show your user data from your Exchange Online domain. This step may take a while, depending on the size of your domain.
6. After the sync, iQ.Suite can now use the LDIF data and the users from the LDIF should be available in the iQ.Suite as well.
7. An alternative path to the LDIF file can be specified in the configuration file 'LdifGenCfg.xml':



```

<?xml version="1.0"?>
<LdifGenCfg xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <Active>true</Active>
  <UseCustomProperties>true</UseCustomProperties>
  <WebClientUri>https://webclient.local/igsuite</WebClientUri>
  <User>admin@webclient.local</User>
  <Password />
  <PasswordEncrypted>1:YXJlYWx5bmljZXRyeQ==</PasswordEncrypted>
  <UseWebClient>false</UseWebClient>
  <AzureTenantId>webclient.local</AzureTenantId>
  <AzureClientId>00000000-0000-0000-0000-000000000000</AzureClientId>
  <AzureClientSecretKey />
  <AzureClientSecretKeyEncrypted>1:YXJlYWx5bmljZXRyeQ==</AzureClientSecretKeyEncrypted>
  <LDIFCustomPath>C:\Program Files\GBS\iQ.Suite\GrpData\LdifGen\igsuite.ldf</LDIFCustomPath>
  <O365User>ldif.sync@webclient.local</O365User>
  <O365Password />
  <O365PasswordEncrypted>1:YXJlYWx5bmljZXRyeQ==</O365PasswordEncrypted>
  <AzureGroupSearchDepth>5</AzureGroupSearchDepth>
</LdifGenCfg>

```

If this value is set and has a valid file path (but the LDIF file does not have to exist), the generated LDIF is written to this file instead of using the file path from the registry (Section 'General' -> Key 'ldif').

IMPORTANT: This is only available in the single-tenant installation. In the multi-tenant Installation, the LDIF is uploaded directly to the tenant database.

## 6 For using EWS – Use OAuth and set permission

An Information Store access via the iQ.Suite Information Store Access Service (EWS Service<sup>1</sup>) is required for the following actions:

- Scan items for viruses in the Information Store
- Update sent items in in the sender's mailbox
- Display and synchronize Clerk absences in Outlook

Login to the Information Store must be done via **Open Authorization (OAuth)**. The basic authentication (BasicAuth) is no longer supported for Azure AD as of iQ.Suite 21.0.3.

For the authentication of the EWS access for your Azure tenants via OAuth, you must enable the use of OAuth in the **Registry** and set the **full\_access\_as\_app** permission in your app. These steps are described in the following section.

### 6.1 Enable OAuth in the Registry

For the authentication of the EWS access via OAuth, you must enable **OAuth** in the Registry as follows:

HKEY\_LOCAL\_MACHINE\SOFTWARE\GBS\iQ.Suite\EWSScan:

[REG\_DWORD] UseOAuth=1

Possible values:

- 1: OAuth is enabled. The Registry values will be used. The Registry values overwrite the EWS settings made in the iQ.Suite Management Console. You don't have to create an EWS user and the settings in the **Exchange Access** tab will be ignored.
- 0: BasicAuth (default). The EWS settings (EWS user and password) made in the iQ.Suite Management Console (iQ.Suite Servers) will be used. See chapter "Configuring access to the Information Store via EWS" in the iQ.Suite administration manual.

[REG\_SZ] OAuthTenantId => Azure Tenant ID

[REG\_SZ] OAuthClientId => Azure App ID

[REG\_SZ] OAuthClientSecret => Azure App Secret

---

<sup>1</sup> EWS: Exchange Web Service

## 6.2 Setting permission for using EWS

The authentication of the EWS access for Azure tenants is done via OAuth. For the authentication, the data of the Azure tenant from your Azure AD app is used.

For the EWS access via OAuth to be successful, an API permission for EWS must be added to the used app. The tenant sets the permission as described below.



**Note:**



The Azure account whose app is to be used must have a Microsoft 365 license.

To set the API permission for EWS and adjust the app, proceed as follows:


1. Click **Add a permission**:


Home > DIGITALL Nature > Consent GBS App

 **Consent GBS App** | API permissions  ...


<<  Refresh |  Got feedback?


**Overview**


 Quickstart


 Integration assistant


**Manage**


 Branding & properties


 Authentication


 Certificates & secrets


 Token configuration


 **API permissions**

 Expose an API

 App roles



 Owners

 Starting November 9th, 2020 end users will no longer be able to grant consent to new

 The "Admin consent required" column shows the default value for an organization. H

**Configured permissions**

Applications are authorized to call APIs when they are granted permissions by users/a all the permissions the application needs. [Learn more about permissions and consent](#)

 **Add a permission**  Grant admin consent for DIGITALL Nature

API / Permissions name	Type	Description
Microsoft Graph (1)		
User.Read	Delegated	Sign in and read user profile

- Click the appropriate app under **APIs my organization uses**:

## Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Apps in your directory that expose APIs are shown below

<input type="text" value="Office 365 exchange"/>	
Name	Application (client) ID
Office 365 Exchange Online	00000002-0000-0ff1-ce00-000000000000


- Click **Application permissions**.

Under **Other permissions**, the **full\_access\_as\_app** permission must be listed now:

## Request API permissions



[All APIs](#)

 Office 365 Exchange Online  
<https://ps.outlook.com>

What type of permissions does your application require?

Delegated permissions  
Your application needs to access the API as the signed-in user.

Application permissions  
Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Permission

Admin consent required

Other permissions (1)

<input checked="" type="checkbox"/>	full_access_as_app ⓘ Use Exchange Web Services with full access to all mailboxes	Yes
-------------------------------------	---	-----

> Calendars

- Select the **full\_access\_as\_app** permission.

5. To grant this permission, click **Grant admin consent for <organization>**:

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

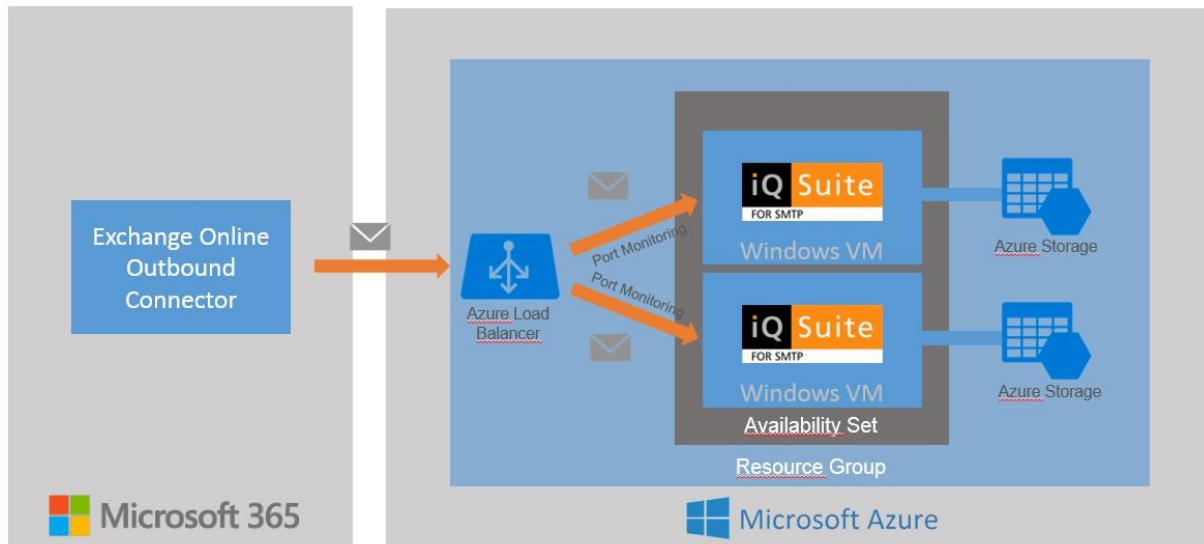
+ Add a permission    ✓ Grant admin consent for gbsdraebenstedt

API / Permissions name	Type	Description	Admin consent requir...	Status
▼ Microsoft Graph (3) ...				
Directory.Read.All	Application	Read directory data	Yes	✓ Granted for g... ...
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for g... ...
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for g... ...
▼ Office 365 Exchange Online (1) ...				
full_access_as_app	Application	Use Exchange Web Services with full access to all mailboxes	Yes	✓ Granted for g... ...

For further information, refer to the section **Configure for app-only authentication** under:  
<https://learn.microsoft.com/en-us/exchange/client-developer/exchange-web-services/how-to-authenticate-an-ews-application-by-using-oauth#configure-for-app-only-authentication>

## 7 High Availability (optional)

To achieve High Availability (HA) in Azure we recommend the following scenario:

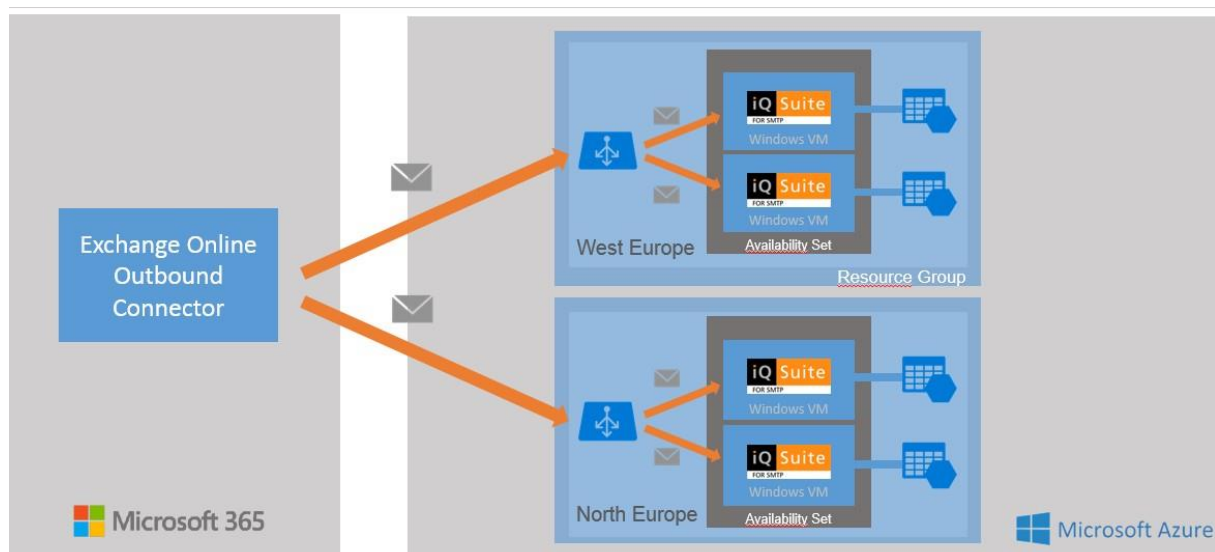


In this scenario, a **Load Balancer** is placed between the Azure Virtual Machines and the Microsoft 365 connector. This way, it will be ensured that the SMTP traffic will only be routed to a VM if the connection is working and stable. This will be regularly tested on the SMTP port through Health Probes from the Load Balancer itself. To make a Load Balancer possible, an Availability Set has to be used in Azure. In an Availability Set, VMs will be grouped together. This grouping ensures that the VMs will not be e.g. restarted together in case of an Azure internal maintenance issue. In general, in case of planned or unplanned maintenance events, an Availability Set with at least 2 VMs will reduce the impact of downtime. Consequently, its usage is highly recommended. With a grouping of at least two virtual machines, at least one machine will still be available and meet the 99,95% Azure SLA (Service Level Agreement).

Furthermore, in an HA environment it is recommended to place each used **VM in a single Storage Account** to further increase the resilience in case of storage failures. For storages, it is also possible to use a geo-redundant replication, which would replicate all your data to a secondary region. This way, your data would be durable even in case of a complete regional outage. But this would be of course more expensive. The secondary regions are determined based on the used primary region and therefore unchangeable.

If a Load Balancer is used, specify the Public IP of the Load Balancer and not the Public IP of the Azure VM in the Microsoft 365 Outbound connector.

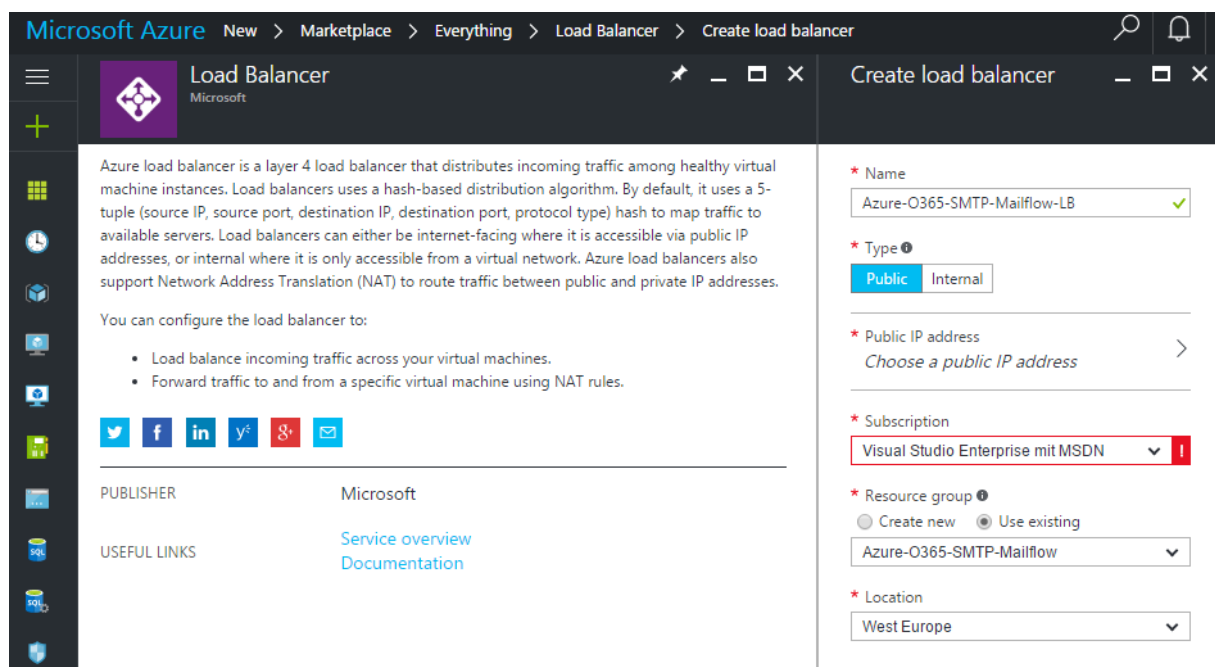
The scenario described above could of course still be further improved regarding the availability. The following shows a “best-case” scenario where two Load Balancers are used and two separate Resource Groups in different regions are created. This scenario could ensure complete availability even in case of a complete regional outage.



In most cases, the first scenario should be enough. But to achieve the highest possible availability, the second scenario should be used.

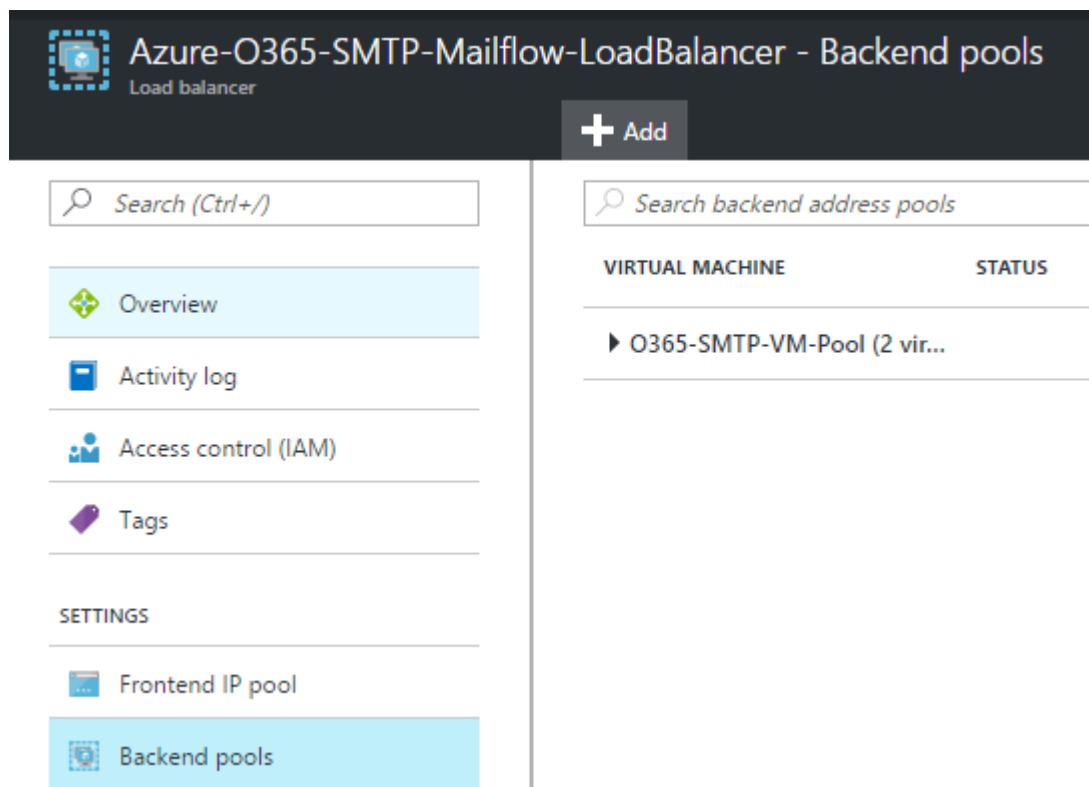
## 7.1 Creating a Load Balancer

In the Azure Portal, create a new Microsoft Load Balancer of the 'Public' type. Assign the Load Balancer to your Resource Group and assign a Public IP:




## 7.2 Configuring the Load Balancer

1. Open the configuration menu of the Load Balancer and configure the DNS name of the public IP. This way, the Load Balancer can be reached with the Public IP and the DNS name from outside the Azure network.
2. Select the **Backend pools** option.
3. Assign the Availability Set with the VMs to your Load Balancer. For this, first click on ADD:




4. Give the Backend Pool a name and select the AV Set to be used. Then, select the VMs of the AV Set which the Load Balancer should use. Confirm with **OK**.




 **Add backend pool**  
Azure-O365-SMTP-Mailflow-LoadBalancer  
Add a backend pool to use one or more virtual machines with a load balancing or outbound NAT rule.

\* Name

Availability set

O365-SMTP-AVSET

Virtual machines 

o365-smtp-vm1	...
o365-smtp-vm2	...

+ Add a virtual machine

After the creation, the new pool should be shown with all assigned VMs.

5. Configure a Health Probe. This way, the connection between the Load Balancer and the VM over the specified port will be tested. First, click in the Load Balancer menu on the **Health Probe** option and there click on ADD. Create a Health Probe for the SMTP port as follows:

\* Name

Protocol

☐ HTTP ☒ TCP

\* Port

\* Interval 

  
seconds

\* Unhealthy threshold 

  
consecutive failures

A Health Probe for e.g. HTTP in relation to the iQ.Suite WebClient would be as follows:

\* Name

CheckWebClient

Protocol

HTTP

TCP

\* Port

80

\* Path ⓘ

webclient/img/logo\_webclient\_small.png

\* Interval ⓘ

10

seconds

\* Unhealthy threshold ⓘ

3

consecutive failures


For HTTP Health Probes, a relative path to a resource on your website has to be specified as verification. It can be, for example, the path to an icon or image.

6. The Health Probe has to be specified in a Load Balancing rule. Create a Load Balancing rule:
  - a) Open the corresponding option in the Load Balancer configuration menu.
  - b) Click on Add and create a rule for the SMTP Traffic:

\* Name

SMTP

Frontend IP address ⓘ

 (LoadBalancerFrontEnd)

Protocol

TCP

UDP

\* Port

25

\* Backend port ⓘ

25

Backend pool ⓘ

O365-SMTP-VM-Pool (2 virtual machines)

Health probe ⓘ

CheckSMTP (TCP:25)

Session persistence ⓘ

None

Idle timeout (minutes) ⓘ

4

Floating IP (direct server return) ⓘ

Disabled

The rule for the HTTP Traffic would be as follows:

\* Name

WebClient

Frontend IP address ⓘ

(LoadBalancerFrontEnd)

Protocol

TCP

UDP

\* Port

80

\* Backend port ⓘ

80

Backend pool ⓘ

O365-SMTP-VM-Pool (2 virtual machines)

Health probe ⓘ

CheckWebClient (HTTP:80/webclient/img/logo\_webclient\_small.png)

Session persistence ⓘ

None

Idle timeout (minutes) ⓘ

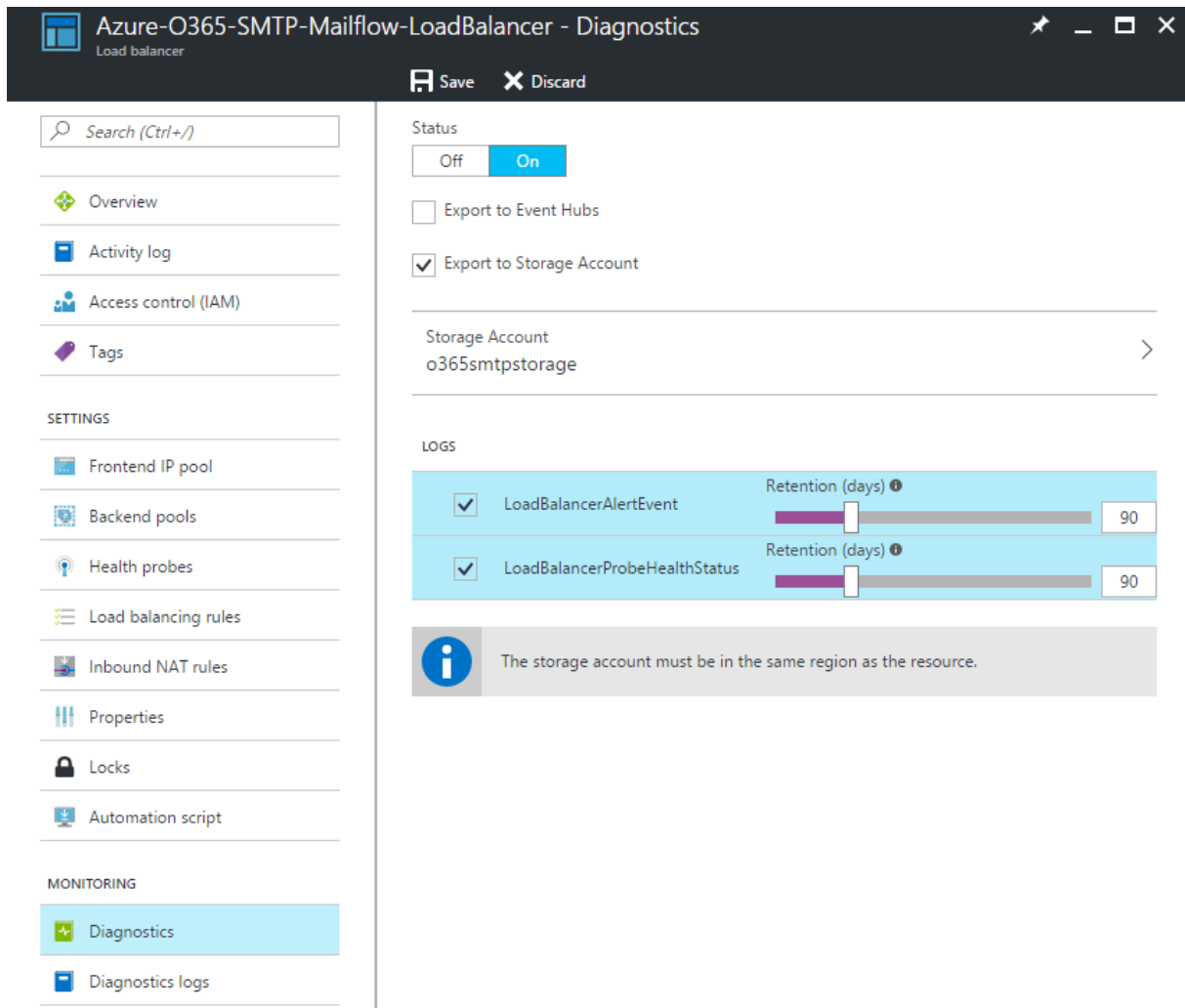


4

Floating IP (direct server return) ⓘ

Disabled

7. Activate the diagnostics for your Load Balancer und assign a Storage Account to it for exporting the log files. We recommend to use one extra Storage Account only for the diagnostics of your Azure resources and the backup of log files.



**Azure-O365-SMTP-Mailflow-LoadBalancer - Diagnostics**

Load balancer

Save Discard

Search (Ctrl+/)

Overview

Activity log

Access control (IAM)

Tags

**SETTINGS**

Frontend IP pool

Backend pools

Health probes

Load balancing rules

Inbound NAT rules

Properties

Locks

Automation script

**MONITORING**

Diagnostics

Diagnostics logs

Status

Off On

☐ Export to Event Hubs

☒ Export to Storage Account

Storage Account

o365smtpstorage

**LOGS**

Log Name	Retention (days)
<input checked="" type="checkbox"/> LoadBalancerAlertEvent	90
<input checked="" type="checkbox"/> LoadBalancerProbeHealthStatus	90

**i** The storage account must be in the same region as the resource.

8. Set the Load Balancer to active. For this, replace the Public IP of the Azure VM with the Public IP of the Load Balancer in the Microsoft 365 Outbound Connector. This way, the mail traffic will be routed over the Load Balancer which will route the traffic to the VMs.

## 8 About GBS

GBS Europa GmbH is a leading vendor of solutions and services in the fields of messaging security and workflow for the Domino and Microsoft collaboration platforms. Over 5,000 customers and more than 4 million users worldwide trust in GBS expertise. The company operates in Europe, North America and Asia.

© 2022 GBS Europa GmbH

Our product descriptions are of a general and descriptive nature only. They do not stipulate any specific features nor do they represent any form of warranty or guarantee. We reserve the right to change the specifications and design of our products without notice at any time, in particular in order to keep abreast of technical developments.

The information contained in this document presents the topics from the viewpoint of GBS Europa GmbH (hereafter 'GBS') at the time of publishing. Since GBS needs to be able to react to changing market requirements, this is not an obligation for GBS and GBS cannot guarantee that the information presented in it is accurate after the publication date.

This document is intended for information purposes only. GBS does not extend warranty for this document, in either explicit or implied form. This also applies to quality, execution, standard commercial practice or suitability for a particular purpose.

All the product and company names that appear in this document may be trademarks of their respective owners.

Web site: [www.gbs.com](http://www.gbs.com)  
Email address: [info@gbs.com](mailto:info@gbs.com)  
Locations: <https://gbs.com/contact-us>

