SCOPE 4 MATION

Privacy & Security

Insights

V0.6

Table of contents

CHANGE HISTORY

To get a clear overview of our services, we have defined service types for the different service levels. Each service type has a description to explain (in general) what is covered in each level.

Version	Change
nnb [1]	• -
31/10/2024	• ORB Graph rights (4.6) adjusted following optimizations in the ORB, MailSend rights.
16/10/2024	• ORB Graph rights (4.6) adjusted following optimizations in the ORB • Administrative: Table of contents and change history added
12/09/2024	• V0.4 of this support agreement

[1] Non-substantive changes are already included in the change history and communicated at least once a year, or when a substantive change occurs.

INTRODUCTION

An important aspect of our services concerns privacy and security. We process information from our customers that must be in good hands. We are transparent and clear about this. In order to test ourselves, we work in accordance with ISO27001 and have ourselves audited and certified by a recognized organization, TÜV Nederland. With this certification we show that we consider information security important, not only when developing our solutions, but also in terms of business operations. ISO27001 is about controlling and managing risks, because risks are always there. Risks cannot be prevented and it is very important to properly analyze what the risks are, take appropriate measures for this, monitor this (and inform), evaluate this properly and ensure that these risks are reduced. With this document we have named all relevant aspects. Because ISO27001 is about continuous improvement, we would like to get in touch to start a conversation if something is unclear or if something is missing.

The following topics are covered:

- Compliance / Information
- Qixium
- Outlook Room Booker
  - Processing Personal Data
  - Exchange
    - Notifications (“Read”)
    - CRUD (“Writing”)
    - App access
    - Permissions & Functionality
    - Granting rights to us
  - TOPdesk
    - Read/write rights and permissions
  - Process design
- Our Statement

1. INFORMATION

On the website you will find all the latest information about our terms, IB policy and setup, our EULA and our sales conditions. You will also find the most recent version of our DNO (Service Level Agreement) / SLA (Service Level Agreement).

2. COMPLIANCE

Scope4mation meets all legal requirements. On our website we have described how we comply with this and ensure compliance.

We have summarized the following information as a starting point to provide insight into the different aspects that play a role here:

- ISO27001 Certificates/ certification
- Privacy (compliance statement)
- Protection of personal data
  - Processor Agreement
  - Privacy Statement
  - Cookie Policy
- Hosting
  - Location & security of data & servers
  - Network & cloud security
  - Availability and continuity
- Integrity and confidentiality
- Incidents/data breaches or vulnerabilities

3. QIXIUM

When implementing solutions, there are always risks. This also applies to the solutions we offer. Depending on the specific solution, these risks can vary in size and nature. It is essential to determine whether your organization considers these risks to be acceptable and what measures have been taken to mitigate or prevent these risks. There must be a good balance between the benefits and savings and the associated risks. We assume that if your organization decides to use one of our services, this decision has already been made or that we will work together during a pilot period to evaluate the solution, including the information security aspects.

This document is intended to support our efforts in the field of information security. It provides insight into the measures that Scope4mation has taken to limit or prevent risks. In addition, we emphasize our expertise with this. Not only with regard to our product, but also with regard to its processes and design, so that we can provide you with expert advice. The document forms the basis for discussions with various officials within your organization, such as Privacy Officers, Chief Information Security Officers (CISOs) and other relevant roles, to discuss which solutions we use and how we manage the risks. As previously indicated, we consider this to be a very important aspect of our service. By discussing this topic thoroughly, decisions can be made in a well-considered manner.

Our SaaS service Qixium offers solutions for extracting or entering information in TOPdesk for your operational applications and services. If the information security within your own services is well arranged, this supports and provides the cooperation and integration with our solutions.

For a large part of our portfolio, we cover the agreements by means of a processing agreement, which is required in all cases. Each solution that we provide relates to personal data to a greater or lesser extent. In addition, there are solutions for which specific rights are required in the source or target application/service. We have drawn up an overview for this to clarify why these rights are necessary, what measures we take to manage risks, and what the possible consequences are if an incident does occur.

Regarding the security requirements and the testing thereof for our Qixium SaaS platform and its use, we would like to refer you to our website, where these aspects are integrated in our ISO27001 certification. We recommend using Single Sign-On (SSO) in combination with Multi-Factor Authentication (MFA) when logging in. We are of course open to questions and would like to get in touch with you.

4. OUTLOOK ROOM BOOKER [ORB]

For the Outlook Room Booker it is important to manage “bookings” between Exchange (Online), also read: Outlook and TOPdesk. In both environments we need access to do this. From TOPdesk bookings are made based on a room, in Exchange this is based on an organizer. The ORB is an advanced system that provides support in managing bookings in many situations.

In order to do this effectively, it is necessary to analyse the data and draw a conclusion based on this to determine what needs to be done. For example, consider a recurring series, where 3 bookings are excluded and booked at a different location/space. Or a secretariat that makes a booking on behalf of someone else and handles it slightly differently. These diverse scenarios quickly make the management of this complex. Within the ORB, these processes are structured as optimally as possible, with all rights and settings carefully aligned to meet specific scenarios.

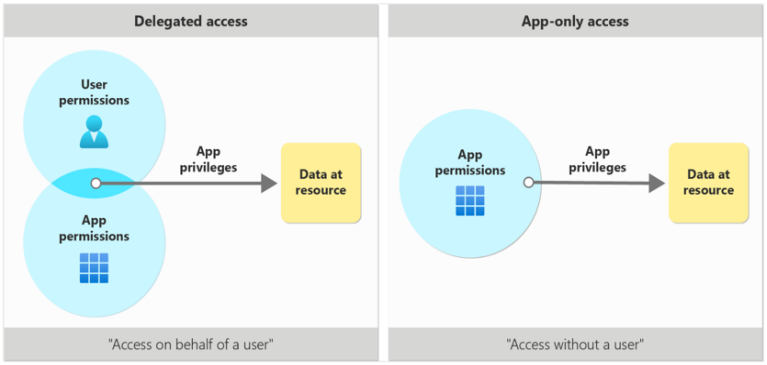
4.1 Processing personal data

Personal data that play a role within the ORB concerns exclusively the e-mail address. This is usually based on a combination of data, such as jan.jansen@bedrijf.nl , on the basis of which a first and last name of a person and the organization for which he or she works can be derived. Because we process personal data, concluding a processing agreement based on the GDPR is a legal obligation. We have made the procedure for this as simple as possible. More information can be found here .

4.2 Exchange access

For access, the ORB uses the access methods provided by Microsoft. This is done by means of an App Registration, which is set up and managed by you. Via the Graph API, the ORB, in combination with the app registration, gains access to your Exchange environment.

Because the ORB must be able to make bookings on behalf of the organizer, the correct permissions are required for this.



4.3 Exchange notifications (“Read”)

Because the ORB works on the basis of the so-called “ Deamon method”, the “app-only access” is required. A Daemon is a process that runs in the background. It does nothing until another program calls on the Daemon . Exchange determines when the ORB has to do what and passes this on. This is done by means of a “subscription”. The ORB conforms to the mandatory Microsoft rules that are used for processing both small and large numbers of bookings. For example, you have to respond within X time, otherwise problems can occur.

Microsoft offers 3 ways to connect to the notification system. The ORB uses Rich Notifications , based on Webhooks . For this an extra security layer has been implemented, which works with a certificate. This is to ensure that the connection is extra secured and encrypted.

Furthermore, the content of a booking is also encrypted and only made readable again within the ORB. Both processes are processed with different certificates. The content of the booking is additionally secured with rotating certificates, so that they change frequently. Only the public key is passed on to Microsoft and Microsoft then encrypts all data of a booking with it. A randomly generated token is provided per subscription that is checked for each incoming notification to determine whether the message has not been modified en route. This principle is called “Anti-tempering” which the ORB uses . The advantage of the notification method is that mailboxes and/or calendars are not scanned by the ORB, but wait for notifications that are intended for the ORB. Bookings in a personal agenda that are not intended for processing by the ORB do not have to be read by the ORB and are therefore not read by the ORB under any circumstances. The data of this booking is therefore not scanned by the ORB and the ORB also has no right to “scan” it.

4.4 Exchange CRUD ("Write")

Bookings are written back to Exchange based on the CRUD principle. CRUD stands for Create, Update, Delete. The highest standard that Microsoft Graph provides for security is the possibility of transport security based on https . Logging in takes place based on the Oauth authorization. This is a proven world standard for security. To reduce risks even further, access is monitored and everything that happens with this access is logged.

Writing of bookings is done in a controlled manner and only data that must be passed on via the ORB is processed. Multiple bookings may be placed next to each other in a personal calendar. This means that the ORB does not have to check (read) whether there is still space available in a personal calendar at a certain time. ORB therefore only manages its own bookings. Bookings in the personal agenda that are not managed by ORB can therefore not be accessed by the ORB in any way.

4.5 Exchange App Access

ORB uses **App Access** . Below is the difference between app access and delegated access.

Feature	App access	Delegated access
ORB Processor	Yes, it is available	**No, method cannot be used**
Definition	With app-only access, the app calls Microsoft Graph with its own identity, without a logged-in user.	With delegated access, the app calls Microsoft Graph on behalf of a signed-in user.
Intended for	Daemon user principle, running in the background.	For example, users who need to "pass through" as themselves within Microsoft Graph via an App.
Consent	Access to the calendar is arranged at admin /administrator level for the entire organization, by means of a one-time confirmation.	Access is arranged at admin /administrator level for the entire organization, by means of a 1x confirmation. *Or* Access must be approved individually, if someone has not done so, this person will not become part of the information towards the Graph API and will be missing from the booking.

Permission detail explanation Microsoft delegated & application permissions

Important to realize that you cannot log in as a "user or administrator" based on the app access. Only the registered app has access. In addition, IP white-listing can be used to ensure that communication can only take place between the Exchange customer environment and the ORB. Access, both at account and IP level, is managed by you as a customer and can be closed at any time if there is reason to do so.

Category	Delegated permissions	Application permissions
Types of apps	Web app / Mobile / Single-page app (SPA)	Web / Daemon
Access context	Get access on behalf of a user	Get access without a user
Who can consent	• Users can consent for their data • Admins can consent for all users	Only admin can consent
Other names	• Scopes • OAuth2 permissions	• App roles • App-only permissions • Direct access permissions
Result of consent	oAuth2PermissionGrant	appRoleAssignment
Supported **signInAudience** types	AzureADMyOrg AzureADMultipleOrgs AzureADandPersonalMicrosoftAccount PersonalMicrosoftAccount	AzureADMyOrg AzureADMultipleOrgs AzureADandPersonalMicrosoftAccount

Additional information: More information and an extensive explanation from Microsoft can be found here .

4.6 Exchange permissions & functionality

The ORB Graph processing is set up according to Microsoft's best-practice rules, based on " least privilege". This only uses the privilege that is necessary for a specific action. And not (as often happens) the "highest right", because "everything can be done so easily with that". The starting principle of " least privilege" is applied to everything the ORB does .

The following rights are applied to the Graph Processor . Below is at least 1 example to explain why a right is required:

Graph API Methods [click for details]	**Functionality**	**Configurable**	**Read/Write**	**Example**
Calendars.ReadWrite	Primary function	No	Read + Write	Retrieving and writing booking(s). Retrieve bookings space, personal calendar. Displaying bookings via the View functionality (display for booking analysis purposes)
Mail.Send	Email	Yes	*N/A*	Sending an email when informing users. This can be limited to 1 user who can only send mail within the organization.
Places.ReadAll List Places Get Place	Spaces	No	Read	The right is Places.ReadAll and we implement the API methods list, get place to read out which Spaces there are.

4.7 Allocate exchange rights to the ORB

For maximum security, the allocation of rights for the app access that the ORB needs, as well as the secret key , is set up by you as a customer and is stored encrypted. Despite the fact that only the ORB can use the app account, we understand, especially if we have only just met, that knowing how your rights are handled by third parties is an important point of attention. Of course, we make agreements about this, we record matters in the processing agreement and we work in accordance with procedures that are audited. However, the most important thing is to have control over the process of allocating rights and not so much the allocation itself, that is a step further. That this is necessary must be seen as the fact and not as the issue, but how it is dealt with. If you have done everything together to ensure maximum security, then everything else is based on trust. A metaphor:

"Imagine that after thorough screening, you are given the key to a beautiful museum. This key gives you the ability to enter at any time and have access to all the valuable works of art and historical artifacts on display there. Although you have the key and can in principle walk in at any time, this does not mean that you have to walk around and touch the works of art or take them home with you. The key is entrusted to you because you are trusted to treat the access with respect.
This metaphor emphasizes the difference between the ability to do something (you have the key) and the right use of that ability (respecting the museum and its artworks). It indicates that you are responsible for how you use the rights and access you have been given, and that you should not abuse these rights."

4.8 TOPdesk read/write rights & permissions

To connect to TOPdesk, we use the TOPdesk API . This is supported in all aspects. The following API methods are used:

TOPdesk API Methods [click for details]	**Functionality**	**Configurable**	**Example**
Reservations	Primary function	No	For loading delta details for bookings. Writing off a booking
Supporting files (Persons)	Primary function	No	Retrieving personal information for an email address

4.9 ORB Fields

Within the ORB, the fields from Exchange or TOPdesk are used. These are listed and explained below. All fields that are listed are available on both sides. Fields that are not necessary for management can be excluded from the display. These are then excluded for everyone and are not visible. The standard display concerns the fields that must be visible for management. Although not necessary and not recommended based on our experience, this can be deviated from by means of configuration.

AGENDA RELATED

Field	**Explanation**	**Privacy Options**
Appointment Type	Simple or repetitive.	*N/A*
Organizer	Organizer of the booking, based on the email address.	*N/A*
Location	Location field, contains all resources.	*N/A,* not used further, only for insight
Room	Space email address where the booking was made.	*N/A*
Participants	Participants linked to the booking.	*N/A*
Subject	Subject of a booking.	Space: - Hide topic on the space itself

		ORB: - Do not include subject
Start / End Time	Start and end time of a booking.	*N/A*
Complexity Index	How many times has the booking been changed? We calculate this to determine how complex the booking has become in the background.	None, is a number, no further data is collected.
Creation date	Date the booking was received in the ORB.	*N/A*

SYSTEM RELATED

Field	Explanation	Privacy Options
ORB Match Id	Key field, used to assist in drawing conclusions quickly.	*N/A*
Correlation Id	Reference field, for insight. Has a relationship with a run that has been performed, so that we can use this in an investigation.	*N/A*
Processor Created	To know on which side the booking was created.	*N/A*
Original Organizer	When registering the booking, this will be filled in once.	*N/A*

STATUS RELATED

Field	Explanation	Privacy Options
Date/Time Last Updated	Timestamp of last processing.	*N/A*
Last Updated Processor	Did Exchange or TOPdesk last handle the booking?	*N/A*
Original Organizer	The organizer at the time of creating the booking.	*N/A*
Failed Date Time	Timestamp of when something went wrong.	*N/A*
Failed Processor	Processor where the error occurred.	*N/A*
Failed Count	Number of times it went wrong.	*N/A*
Number of times retried	Number of times it has been resubmitted to Exchange or TOPdesk.	*N/A*
Status: Exchange/TOPdesk processor	Last known status returned by TOPdesk or Exchange.	*N/A*

4.10 Process design

Based on our experience and methodology, we can ensure that the ORB setup is in line with the processes within your organization. Based on the overview below, we can support you in reducing the risks and making them controllable.

Element	Aspect	Additional Information

Privacy	When you work with the ORB, you only share the email address with the ORB. We can exclude all other information within the ORB. Think of Subject or Content.	ORB Configuration, will be reviewed during the project if appropriate.
Graph best practice	When determining EXCHANGE PERMISSIONS, we work based on Microsoft's best-practice advice and have implemented this in the ORB.	https://learn.microsoft.com/en-us/graph/permissions-overview?tabs=http#best-practices-for-using-microsoft-graph-permissions
Scope	Within Microsoft Graph, you cannot establish a "scope" (area of application) for "app access". What is possible is that mailboxes are excluded, to which we do not have access. See also "Restrict (mailbox) calendar access" below.	Configuration and explanation: https://learn.microsoft.com/en-us/graph/auth-limit-mailbox-access?context=graph%2Fapi%2F1.0&view=graph-rest-1.0
Book a room only	We would like that and TOPdesk can do this just fine. TOPdesk reservation management thinks from a Space. However, Exchange does not work that way. Reserving a space is part of a booking in a personal agenda. This means we have to work from the personal calendar and not from a space. *ORB does support "room only " booking, but we strongly advise against it. In that case, a change to a room reservation from TOPdesk will only update the room in Exchange and not the organizer's calendar with the invitees.*	ORB Configuration, will be reviewed during the project if appropriate.
Restrict (mailbox) calendar access	ORB only works with calendar read and write rights, and only has access to the calendar of a mailbox and has no further access to the mailbox and therefore of course explicitly not to emails either. We do not read out complete user calendars. The ORB makes bookings in a user calendar (of the organizer). ORB only changes bookings with a space that is managed by the ORB.	We have no further access to the calendar.

Has anything changed in the way Exchange or Outlook works in your working methods?	No, nothing will change in the current way of working in the field of privacy. There are undoubtedly privacy and booking rules active in Outlook, these are all honored with the ORB and our way of working. If you put a lock on an agenda item, we cannot view this item (but we can process it). We often also advise to make a separate booking for a room, for example, if you want to be sure that no privacy-sensitive information is shared. Not even in the Room Agenda of Outlook. This has to do with the policy of your organization. We are increasingly seeing the phenomenon that people work with an "Open agenda" policy. In this policy, everyone is free to book how they want and in terms of privacy, it is assumed that you use the general "company rules". This can be done to keep it workable.	
Considerations/ arguments	We can imagine that the following statements will emerge during this process: “How important is booking in or from a personal agenda? How much benefit does this give to the organization in relation to what is needed to arrange this?” “But then you can look at the contents” “You can reach everything then?” “What is the company policy regarding calendars and their use?”	You can read our motivation below under “Our statement”

5. Our Statement

At Scope4mation we believe it is important to provide high-quality and complete services and to be as clear as possible about this. For example, in relation to the ORB and reading and writing in a personal (company) calendar of an employee; This method can be used perfectly for the automatic synchronisation of company activities, such as booking an appointment in TOPdesk for a room. For an employee's calendar, there must be a certain degree of recognisability in the appointments that are made and it should not come as a total surprise that this happens. Of course, ORB does not determine when something is booked, that comes from the employees themselves. They play the leading role in the synchronisation. From a privacy point of view, it is plausible that individual employees do not have to give personal permission for the synchronisation of room bookings between Outlook and TOPdesk. Permission at company level is normally efficient and sufficient. Making it known that this process is active and that the efficiency of booking rooms for appointments is improved by this is certainly a plus. However, we remain realistic that not everyone in an organization can first give explicit consent before bookings with rooms can be synchronized via the ORB. If these bookings were not included, this would also have a direct impact on all other bookings.

Finally, we understand that access to Exchange is an extremely sensitive subject. By applying app access, the " least privilege" method, IP white-listing , encrypting and securing data and communication and the way in which the ORB has been developed with only the functionality and rights described in this document, we have applied all technical methods and means for information security. Apart from these technical aspects, we have also ensured at the organizational level that information security and the handling of (privacy) sensitive data is safeguarded. It is not without reason that we have ourselves audited and certified with a very broad scope and declaration of applicability on the ISO 27001 standard by a renowned and accredited body such as TÜV Nederland.

Are there any questions from your organization? Then it is important that we get in touch with each other. This can be done via privacy@scope4mation.com. You will then be put directly in contact with me and our privacy team. We are happy to work together!

On behalf of Team Scope4mation I hope for a pleasant and safe collaboration!

Marcel van de Steeg
Privacy Officer