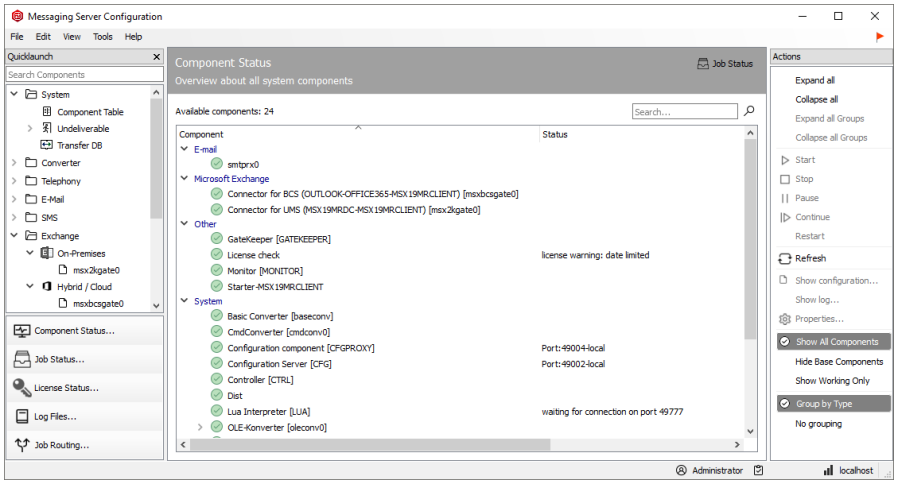
APPLICATION NOTE

DOKUMENTATION

OFFICEMASTER FÜR MICROSOFT OFFICE365

No. 2020-01

Revision 1.2



Application Note | Ferrari electronic

I. Revision History

Revision	Date	Author	Changes
1.0	31.08.2020	Marko Riebe	Initial Release
1.1	08.09.2020	Marko Riebe	Transferkontovoraussetzungen geändert
1.2	17.09.2020	Marko Riebe	Powershellvoraussetzungen und Hinweise aktualisiert

Einleitung

Diese Dokumentation beschreibt die Connectoren für Office365™ ab Version 7.1.0. Diese Beschreibungen geben die technische Grundlage zur Erarbeitung weiterer Dokumentationen.

Haftungsausschluß

Die in diesem Dokument zusammengefassten Informationen wurden mit besten Wissen und Gewissen zusammengetragen. Für etwaige Fehler, sowie Änderungen die dem technischen Fortschritt dienen wird keine Haftung übernommen.

Beabsichtigte Leserschaft

Dieses Dokument richtet sich an Erstverwender/Betatester der dokumentierten Software, sowie an interne Mitarbeiter zur technischen Dokumentation des Produktes.

Symbole

Folgende Symbole werden im Dokument verwendet und haben folgende Bedeutung.

Warnung

Warnungen sollen auf unbedingte Kenntnisnahme hinweisen, um die korrekte Funktion der Software entsprechend zu gewährleisten.

Hinweis

Hinweise informieren den Benutzer über Besonderheiten im Gebrauch der Software.

Anmerkung

Anmerkungen geben zusätzliche Informationen zum Gebrauch oder der Funktionsweise der Software.

Copyright und rechtliche Hinweise

INHALT

1. Allgemein

1.1 Moderne Authentifikation

Die sichere Authentifikation bildet die Grundlage für die Installation und Administration der Komponenten im Microsoft Office365. Das Konzept der „Modernen Authentifikation“ bezeichnet in diesem Fall die manuelle Anmeldung per Web, i.d.R. mit OAuth 2.0-Mechanismen zusammen mit Multifaktor-Authentifikation, um eine sichere interaktive Anmeldung zu gewährleisten.

Auch Anwendungen/Programme, die per Internet auf die Schnittstellen des Exchange Online (Exchange Web Services) oder des Microsoft Graph Interface (AzureAD, etc.) zugreifen, müssen diese „Moderne Authentifikation“ unterstützen. Ältere Programme, die im Design für On-Premises-Exchange Server entwickelt wurden, können für die Kommunikation mit den Schnittstellen, die Basic-Authentifikation nutzen. Da diese jedoch entsprechend unsicherer ist, wird die Unterstützung dieser Authentifikation sukzessive in der Zukunft abgeschaltet.

Die Konfiguration der Modernen Authentifikation steht ab Juli 2020 im AzureAD-Portal unter dem Punkt „Moderne Authentifikation“ bereit:

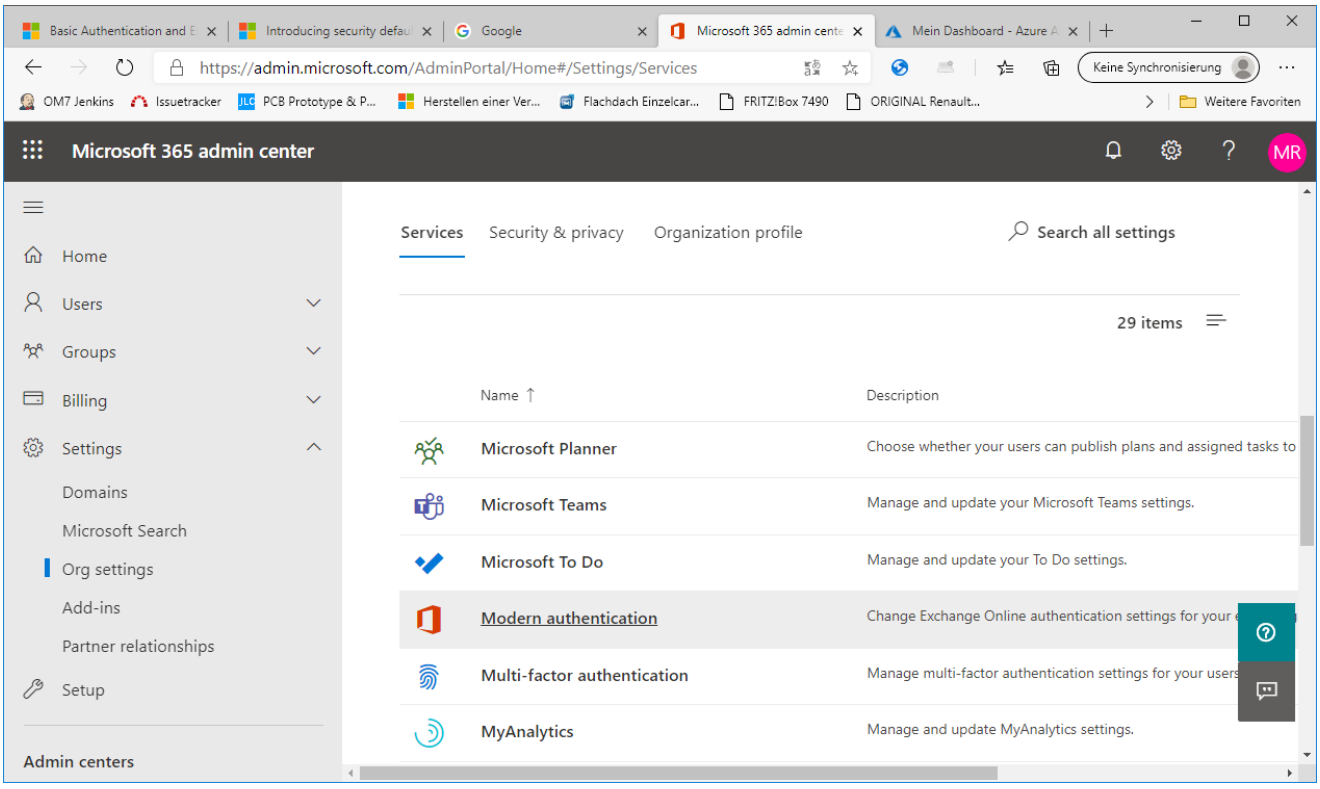


Abbildung 1: Organisationskonfiguration - Moderne Authentifikation

Nähere Informationen können dem Exchange Team Block entnommen werden:

https://techcommunity.microsoft.com/t5/exchange-team-blog/basic-authentication-and-exchange-online-july-update/ba-p/1530163

Der OfficeMaster BCS-Connector kommuniziert über die Exchange Web Services mit dem Office365, somit muss auch dieser die Moderne Authentifikation benutzen können. Da die OfficeMaster-Benutzeradministration und der Installationsassistent die Online-Powershell-Module benutzen, müssen auch diese Komponenten die Moderne Authentifikation, insbesondere Multifaktor-Authentifikation unterstützen.

Mit einem ehemals für Oktober 2020 angekündigten Update zur Abschaltung der Basic Authentifikation wird in der Organisationskonfiguration die Basic Authentifikation für alle kommunikativen Programmteile der Cloud abgeschaltet. Falls die eingesetzte Software die Moderne Authentifikation nicht unterstützt, kann die gesamte Umstellung bzw. ausnahmsweise bestimmte Teile davon wieder rückgängig gemacht werden. Informationen dazu können folgender Seite entnommen:

https://docs.microsoft.com/de-de/exchange/clients-and-mobile-in-exchange-online/disable-basic-authentication-in-exchange-online

1.2 Bestehende Installationen

Bei einem reinen Update auf die OfficeMaster Version 7.1 ändert sich nicht die Zugriffsmethode der Connectoren. Das reine Update aktualisiert alle Programmkomponenten. Die Cloudinstallation bleibt so bestehen, wie vor der Installation.

- Wenn sich die Einstellungen zur Modernen Authentifikation nicht ändern, muss die bestehende Installation nicht verändert werden.
- Wenn sich die Einstellungen zur Modernen Authentifikation schon geändert haben bzw. eine Änderung absehbar ist, sollte der Connector überinstalliert werden und die Kommunikation (siehe Punkt 5) geändert werden.

1.3 Neuinstallationen

Im Zuge einer sicheren Kommunikation zu den Diensten der Cloud sollte die Moderne Kommunikation während der Installation des Connectors aktiviert werden. Die Installation wird weitestgehend automatisiert durchgeführt. Der Grad an manuellen Eingriffen kann während der Installation gewählt werden.

2. Installation des Connectors for BCS

Der Installationsassistent des Connectors for BCS unterstützt zwei Arten der Cloud-Installation:

- Cloud-Only - In diesem Fall ist kein lokales Active Directory vorhanden.
- Hybrid - Diese Installation setzt ein lokales Active Directory voraus, dass als Benutzeradressbuch benutzt wird.

Die Installation soll hier am Beispiel einer Cloud-Only-Installation erfolgen:

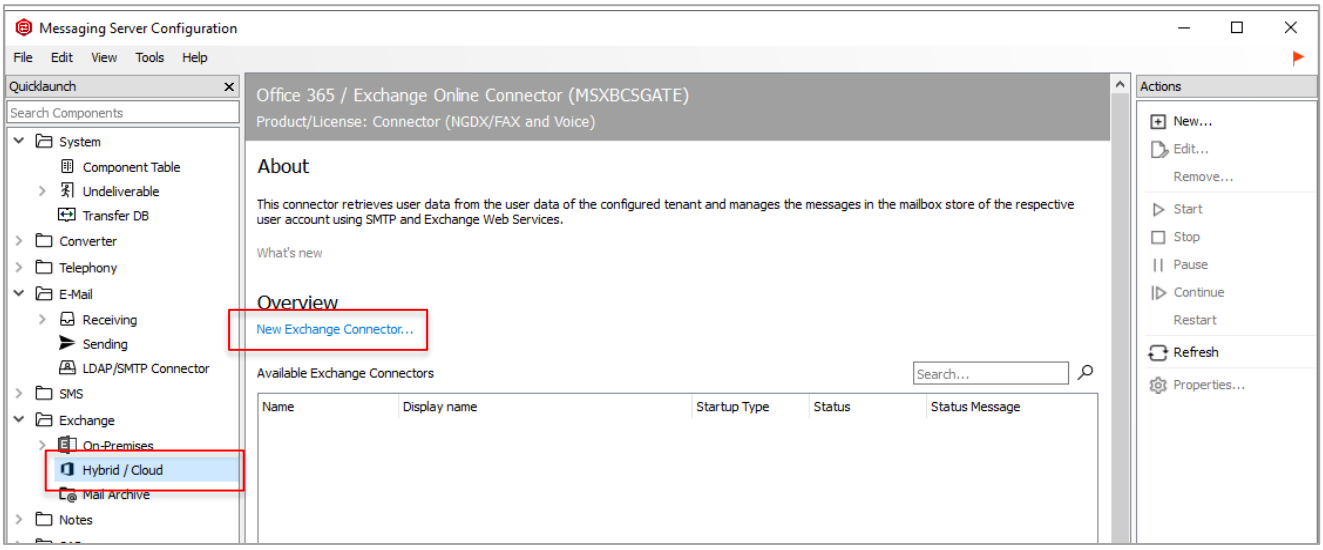


Abbildung 2: Anlegen eines neuen Online Connectors

Wenn man einen neuen Connector hinzufügen möchte, bzw. den aktuellen Connector ändern möchte, öffnet sich der Installationsassistent für BCS-Connectoren.

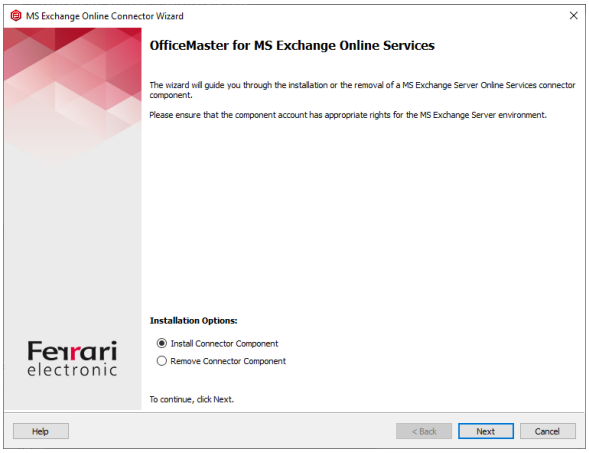


Abbildung 3: Willkommensbildschirm

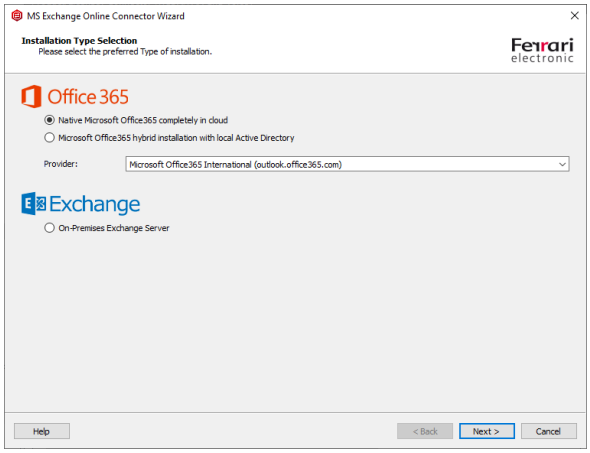


Abbildung 4: Auswahl der Installation

Abbildung 4 zeigt den Auswahldialog des Installationsassistenten. Wenn die Office365-Installationen ausgewählt werden, wird darauffolgend eine Anmeldung an die Office365 Cloud vorgenommen. Die Cloud-Anmeldung unterstützt die Multifaktor-Authentifikation.

Hinweis!

Diese Anmeldung wird intern über eine Remote Powershell vorgenommen. Dafür sind gewisse Voraussetzungen zu erfüllen:

- Vorhandensein von Microsoft Powershell mindestens Version 5.0
- Der erweitere Sicherheitsmodus für den Internet Explorer **MUSS** abgeschaltet sein. Die Powershell-Module arbeiten bei den Login-Dialogen mit einem internen Browser-Modul, welches ohne Javascript-Ausführung und Zugriff auf die Cloud-Anmelde-Endpunkte nicht korrekt arbeiten kann.

Hinweis!

Sollte diese Anmeldung an die Cloud das erste Mal von dem installierenden Konto erfolgen, müssen gegebenenfalls noch Module nachinstalliert werden. Dies kann einen Moment dauern. Ein Dialog weist auf die Nachinstallation hin. Nach dem Schließen dieses Dialoges kann sich die Anzeige des Anmeldefensters ebenfalls noch um eine ca. 30 Sekunden verzögern.

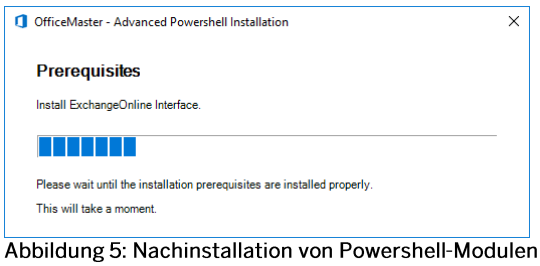


Abbildung 5: Nachinstallation von Powershell-Modulen

Mit der erfolgreichen Anmeldung in die Cloud gelangt man zur nächsten Assistentenseite. An dieser Stelle wird der Transport vorkonfiguriert. Dieser Schritt unterscheidet sich nicht zur Vorgängerversion.

Anmerkung

- Die erfolgreiche korrekte Anmeldung an der Cloud zeigt sich mit der korrekten Darstellung des Namens der Organisation.
- BCS-Connectoren arbeiten in der Cloud ausschließlich im Service Transfer Modus, d.h. die ausgehenden Nachrichten werden in einem vorher erstellten Postfach gesammelt. Dieses Transferpostfach kann auch eine Postfachfreigabe (Shared Folder) sein. Das Postfach muss zuvor manuell angelegt werden. **Dieses Postfach darf nicht Standardempfänger sein! Bei Einsatz der modernen Authentifikation muss immer ein solches Transferpostfach bereitgestellt werden!**
- Die Transferdomänen werden standardmäßig mit dem Namen der Organisation erstellt. Dies sollte aus Erfahrung in kürzere Domänen umgewandelt werden. Diese Domänen müssen keinen DNS Mail Exchanger Record besitzen, da die Mails per Regel abgefangen werden.
- Die Transferdomänen sollten einen vox-Typ besitzen, um Gelesen-Bestätigungen für Voice zu unterstützen. (Abschalten von MWI-Lampen bei gelesenen Voicemails.)

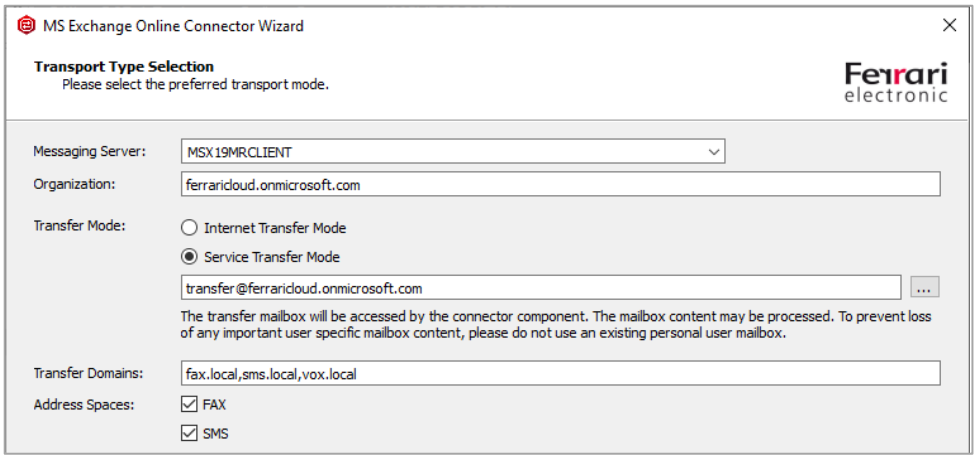


Abbildung 6: Transporttyp und Routing

Im darauffolgenden Schritt gelangt man zu den Konten- und Sicherheitseinstellungen.

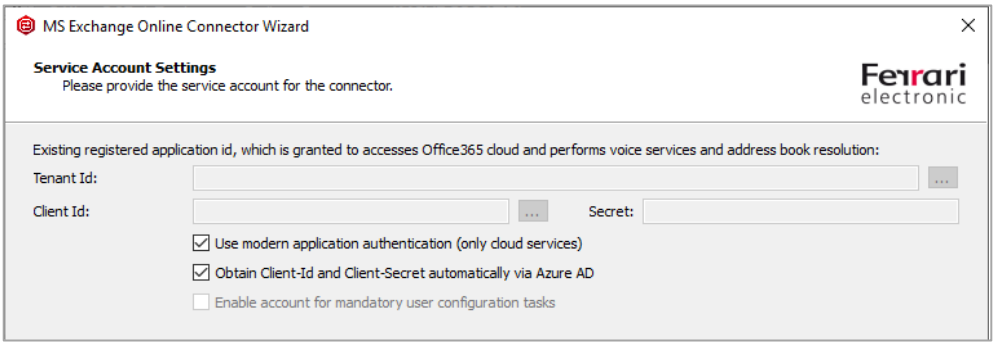


Abbildung 7: Konten- und Sicherheitseinstellungen für moderne Authentifikation

Die Installation ist standardmäßig auf „Moderne Authentifikation“ ausgelegt, und die maßgeblichen Sicherheitseinstellungen werden automatisch bestimmt und erstellt. Es werden dabei intern folgende Schritte für eine Applikationsregistrierung ausgeführt:

- Die Tenant-Id (Mandanten-Id) wird bestimmt.
- Es wird im AzureAD eine Applikation mit dem Namen „OfficeMaster EWS“ erstellt.
- Für die Applikation „OfficeMaster EWS“ wird eine Client Id (Anwendungs-Id) und ein Client Secret (Geheimnis) mit einer Gültigkeit von 5 Jahren erzeugt.
- Für die Applikation „OfficeMaster EWS“ werden API-Berechtigungen vergeben:
    - Exchange Online EWS: full_access_as_app (als Applikationsberechtigung)

      Diese Berechtigung berechtigt die Applikation zum Lesen und Bearbeiten der Transfermailbox, sowie zum Zugriff auf die Benutzerpostfächer, um Voice-Aufgaben vornehmen zu können. Ebenfalls wird damit die Konfiguration der Benutzer über die OfficeMaster Exchange Administration ermöglicht, da in einer Cloud-Only-Installation die benutzerspezifischen Werte im Postfach gespeichert werden.
    - Microsoft Graph: People.Read.All (als Applikationsberechtigung)

      Diese Berechtigung wird für Anfragen an die Adresslisten der Cloud benutzt.
    - Microsoft Graph: User.Read (als delegierte Berechtigung)

      Diese Berechtigung wird automatisch gesetzt und hat für den Connector keine Bedeutung.
    - Microsoft Graph: User.Read.All (als Applikationsberechtigung)

      Diese Berechtigung wird für Anfragen an die Adresslisten der Cloud benutzt.

Wenn die Client Id und das Client Secret zuvor manuell erstellt worden sind, so können diese auch einfach nur eingegeben werden. In diesem Fall ist die Option „Obtain Client Id and Client Secret automatically via AzureAD“ zu deaktivieren. Die Werte können dann einfach angegeben werden.

Falls in einem solchen Fall die Tenant-Id (Mandanten-Id) nicht bekannt sein sollte, kann diese über den Browser-Knopf automatisch bestimmt werden.

Die Installation bietet noch eine weitere Möglichkeit der Vorkonfiguration. In einigen Fällen wurde die Applikation „OfficeMaster EWS“ bereits im AzureAD registriert. In diesem Fall sollte vielleicht keine neue Applikation angelegt werden. Wenn dem so sei, kann über den Browser-Knopf der Client-Id ein Applikationsbrowser aufgerufen werden.

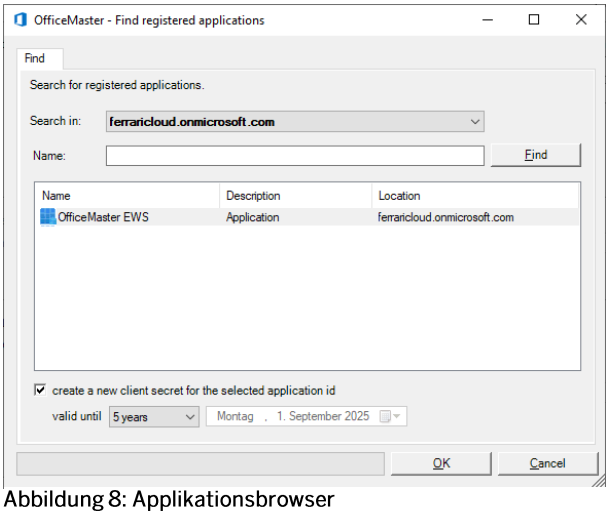


Abbildung 8: Applikationsbrowser

Die Besonderheit bei einer ausgewählten Applikation ist, dass kein Geheimnis (Client-Secret) ausgelesen werden kann. Wenn dieses Geheimnis nicht bekannt ist, kann ein neues Geheimnis während der Auswahl erstellt werden. Solche Geheimnisse haben eine bestimmte zeitliche Befristung. Diese kann im Dialog eingestellt werden.

Hinweis!

Ein spezielles Dienstkonto ist augenscheinlich für den Zugriff per Exchange Web Services bei der modernen Authentifikation mit Tenant-Id, Client-Id und Client-Secret **nicht** notwendig. In diesem Fall wird trotzdem ein Transferpostfach für die ausgehenden Nachrichten benötigt. Ob dieses Postfach einen Multifaktor-Authentifikationsschutz besitzt, ist nicht von Bedeutung und spielt für den Connector keine Rolle. Das Transferpostfach wird im Fall der modernen Authentifikation als Zugangspunkt für Adressbuchauflösungen verwendet und ist somit Voraussetzung für den reibungslosen Betrieb.

Hinweis!

Sollte im Installationschritt für die Konten- und Sicherheitseinstellungen der Haken zum Benutzen der modernen Authentifikation deaktiviert werden, so kann wie in der Vorgängerversion der Benutzername und das Passwort eines Dienstkontos angegeben werden. In diesem Fall wird für den Zugriff per Exchange Web Services die Basic Authentifikation benutzt. **Dies wird allgemeinhin nicht mehr empfohlen.**

Mit den nachfolgenden Installationsschritten kann der Connector, wie bei der Vorgängerversion installiert werden.

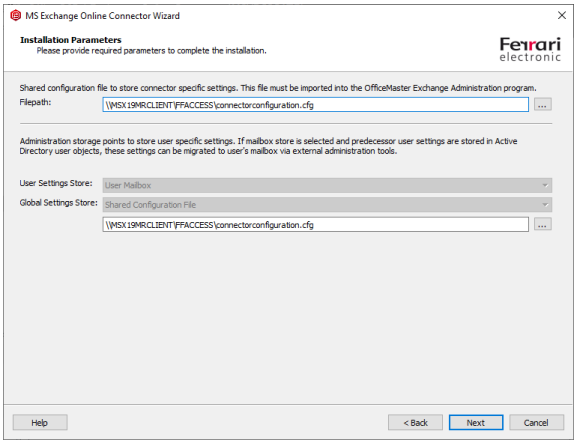


Abbildung 9: Speicher der Einstellungen

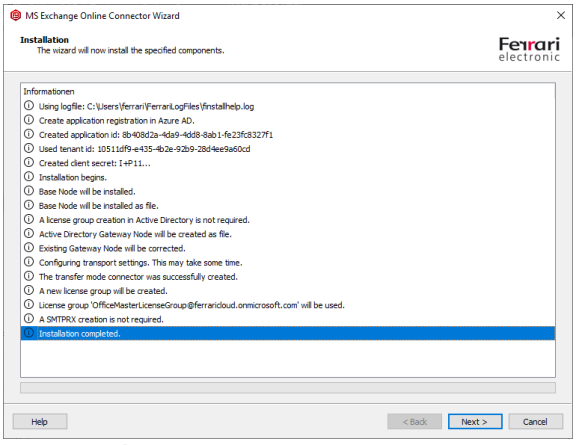


Abbildung 10: Installation

Bei der Installation mit moderner Authentifikation erscheint währenddessen ein Hinweis:

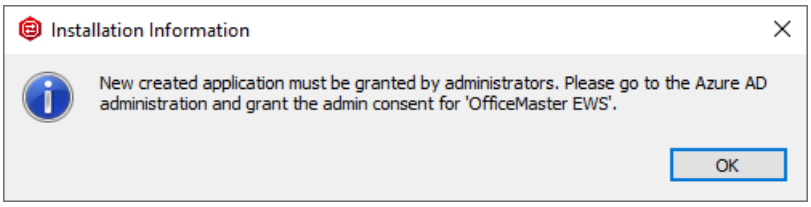


Abbildung 11: Hinweis zum Admin Consent

Dieser Hinweis bezieht sich auf die API-Berechtigungen. Es wurde aus Sicherheitsgründen bewusst darauf verzichtet, die Freigabe der API-Berechtigungen automatisiert zu bestätigen. Dies muss nach der Installation von einem Administrator im AzureAD vorgenommen werden.

Man meldet sich dazu am AzureAD des Office365-Mandanten an und navigiert zur Applikation „OfficeMaster EWS“:

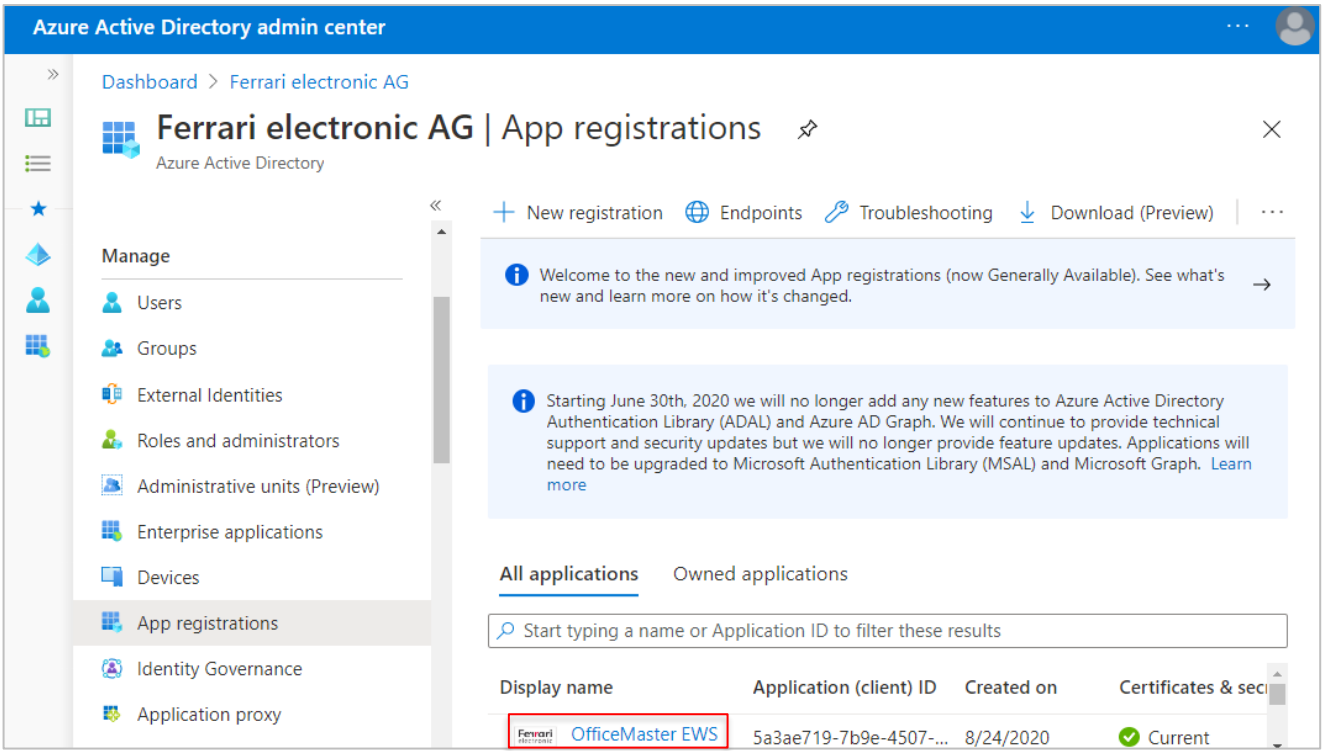


Abbildung 12: AzureAD Applikation

Nach Auswahl der Applikation lässt man sich die API-Berechtigungen auflisten.

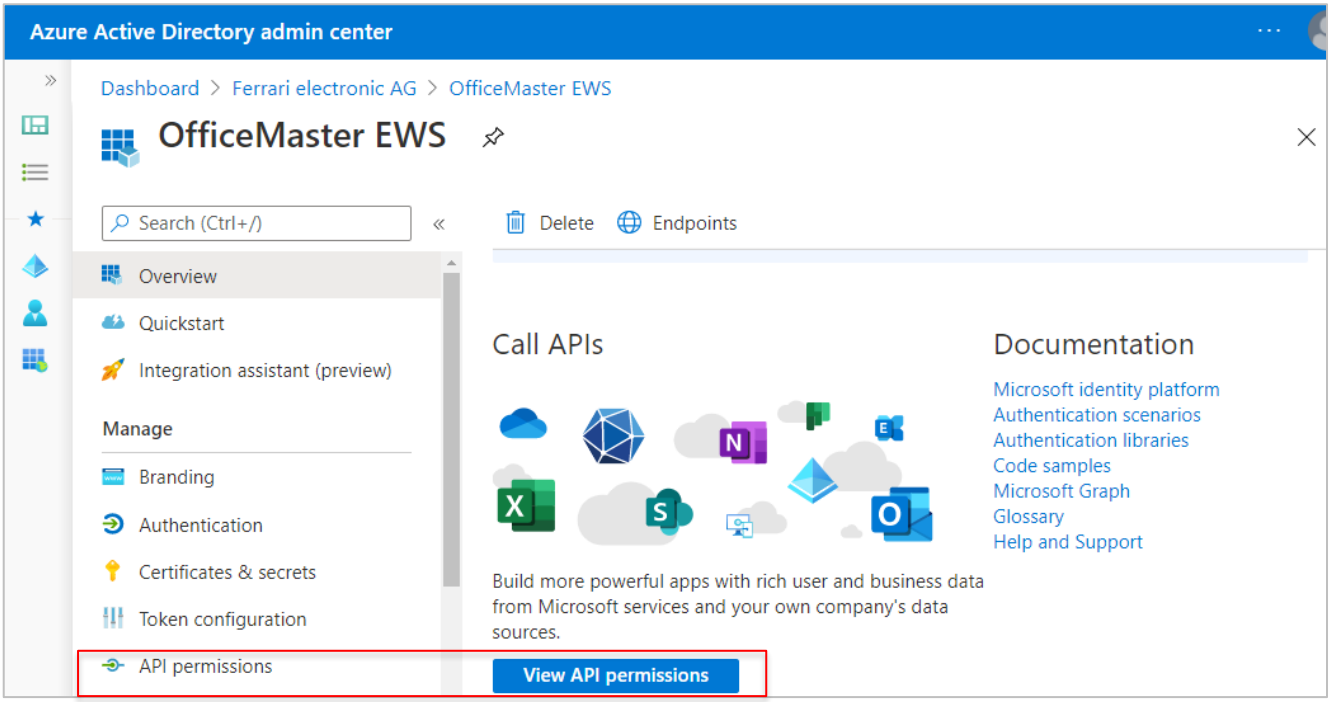


Abbildung 13: API-Berechtigungen

Die API-Berechtigungen müssen nun bestätigt werden. Dieser Schritt muss für eine Applikation nur einmal vorgenommen werden.

Hinweis!

Bei diesem Schritt können die Berechtigungen nach Kundenwunsch umgestaltet werden. Es soll hier nochmal darauf hingewiesen werden, dass für den laufenden Betrieb des Connectors, ein Zugriff per Exchange Web Services ohne Einschränkungen möglich sein muss. Ein Verändern der Berechtigungen hat möglicherweise einen destruktiven Einfluss auf den produktiven Betrieb des Connectors.

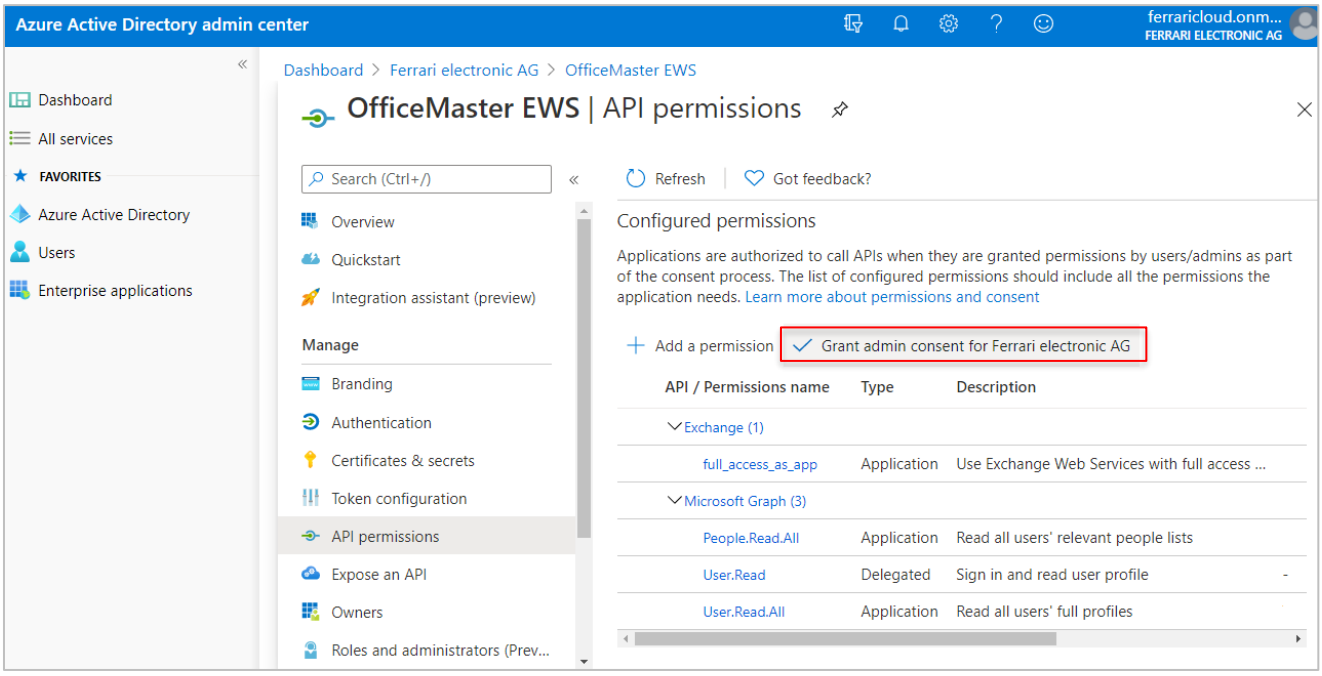


Abbildung 14: API-Berechtigungen freigeben

Nach dem Freigeben der API-Berechtigungen kann der Connector, wie die Vorgängerversion in Betrieb genommen werden.

3. Administration der Modernen Authentifikation

Die Einstellungen, die während der Installation für die Moderne Authentifikation vorgenommen worden, spiegeln sich in den Connector-Eigenschaften in der Registerkarte für die Exchange Web Services wider.

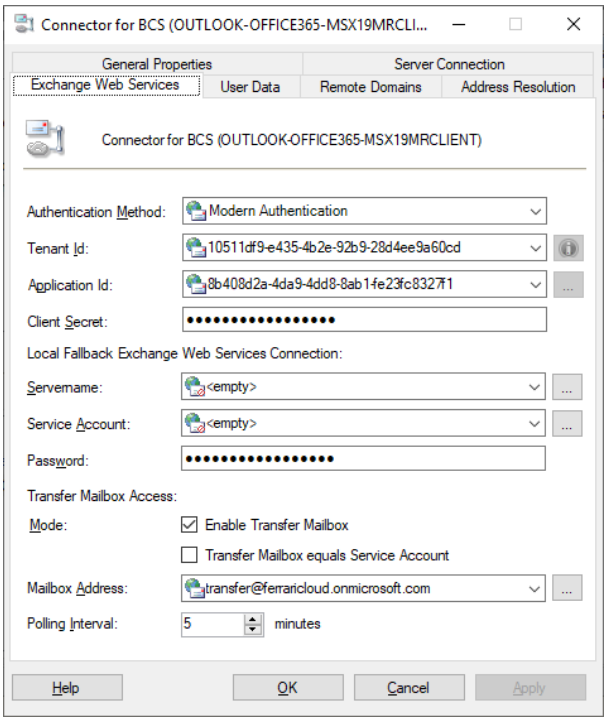


Abbildung 15: Connectoreigenschaften / EWS-Einstellungen

Die maßgeblichen Einstellungen für die Moderne Authentifikation bzw. die Umstellung auf die Moderne Authentifikation verbergen sich in den folgenden vier Feldern:

Authentication Method

An dieser Stelle kann zwischen „Moderner Authentifikation“ und „Basic Authentification“ umgeschaltet werden. Je nach Einstellung ändern sich die Folgeeinstellungen von Username auf Client-Id und Password auf Client-Secret. Die Tenant-Id ist nur im Falle der modernen Authentifikation freigeschaltet.

Tenant Id

Die Tenant Id (Mandanten-Id) ist nur im Falle der modernen Authentifikation von Bedeutung. Der Info-Knopf kann diese Id automatisch ermitteln. Für diese Ermittlung ist gegebenenfalls eine weitere Anmeldung notwendig.

Client Id

Im Falle der modernen Authentifikation muss hier eine Client Id (Anwendungs-Id oder Application-Id) angegeben werden. Diese kann mit dem Browserknopf ausgewählt werden bzw. muss vorher manuell ermittelt werden, um dann direkt eingegeben zu werden.

Client Secret

Das Client Secret (Geheimnis) ist eine Art Passwort für die Client-Id. Wenn dies zuvor bekannt ist, kann dies hier angegeben werden. Wenn die Client-Id mit dem Browser ermittelt wurde, so kann dieser Browser das Client-Secret nicht bestimmen, es sei denn es wird entsprechend neu erstellt. Dies kann in dem Application Browser angegeben werden. Neu erstellte Geheimnisse haben in der Regel eine zeitliche Befristung. Diese muss entsprechend im Browser angegeben werden (siehe Abbildung 8).

4. Manuelle Registrierung der Anwendung via Exchange Online- und AzureAD Portal

4.1 Registrierung der Anwendung

Im Zuge der Installation ist es eventuell notwendig die Applikation manuell zu registrieren. Die notwendigen Schritte sollen hier kurz erläutern werden.

Im ersten Schritt meldet man sich an der Cloud an und navigiert zum AzureAD.

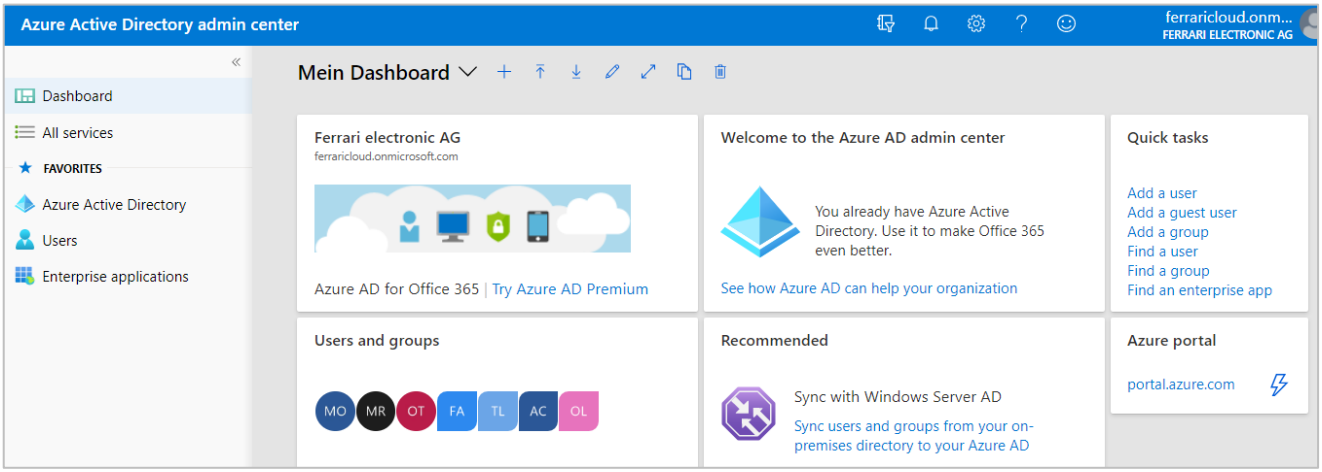


Abbildung 16: AzureAD Dashboard

Für eine Registrierung der Anwendung navigiert man nun zu den registrierten Anwendungen (App registrations).

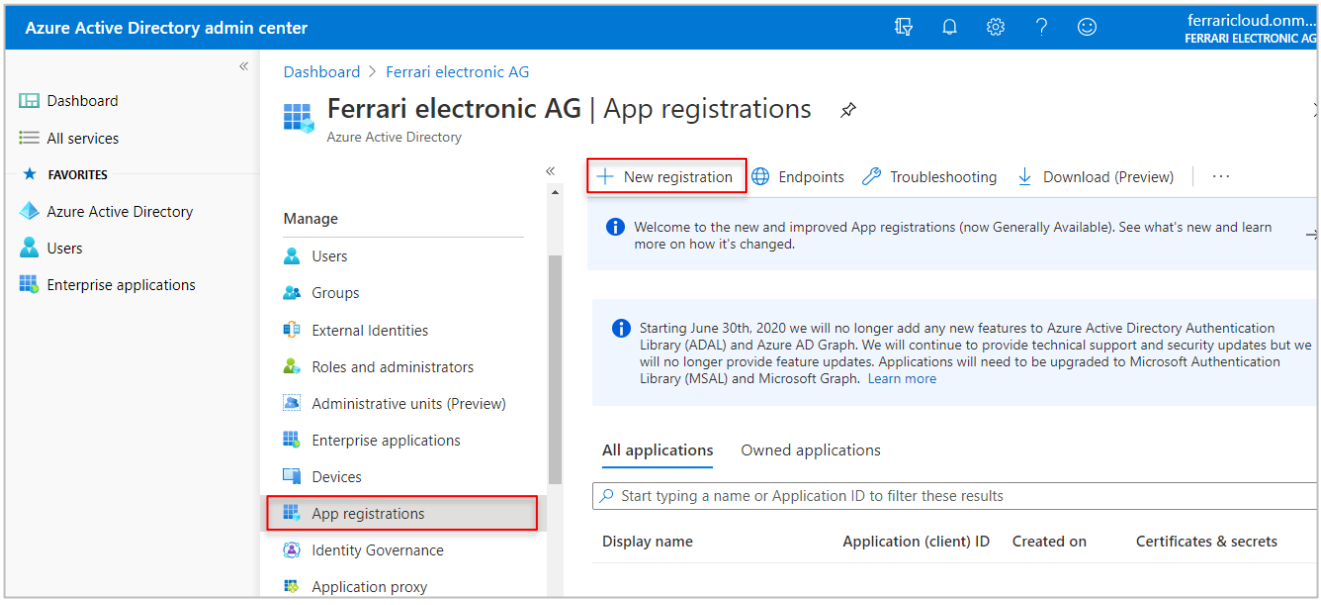


Abbildung 17: AzureAD - Anwendungsregistrierung

An dieser Stelle kann eine neue Anwendung für den Zugriff auf die Cloud registriert werden.

Die Registrierung sollte folgende Werte enthalten:

Name der Anwendung: OfficeMaster EWS

Man kann hier jeglichen Namen angeben. Der automatische Installationsassistent wird den Namen „OfficeMaster EWS“ verwenden.

Unterstütze Konten: Konten in dieser Organisation

Man kann hier auch die Anwendung für mehrere Mandanten vorbereiten. Der automatische Installationsassistent wird den Zugriff auf die angemeldete Organisation beschränken (Single Tenant).

Umleitungs-URI: Public Client/Native (mobile) urn:ietf:wg:oauth:2,0:oob

Weitere Informationen findet man unter https://docs.microsoft.com/de-de/azure/active-directory/develop/scenario-desktop-app-registration.

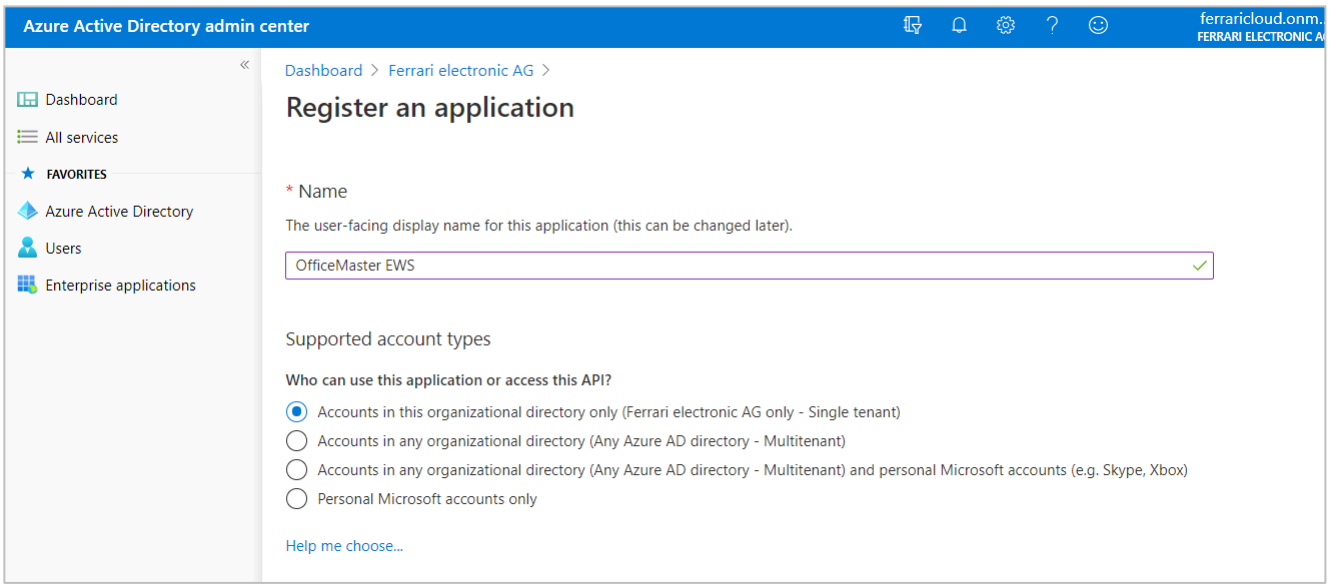


Abbildung 18: Registrieren einer Anwendung

Wenn die Anwendung initial registriert wurde, ist dies ein guter Moment, die Tenant Id und die Client Id zu notieren.

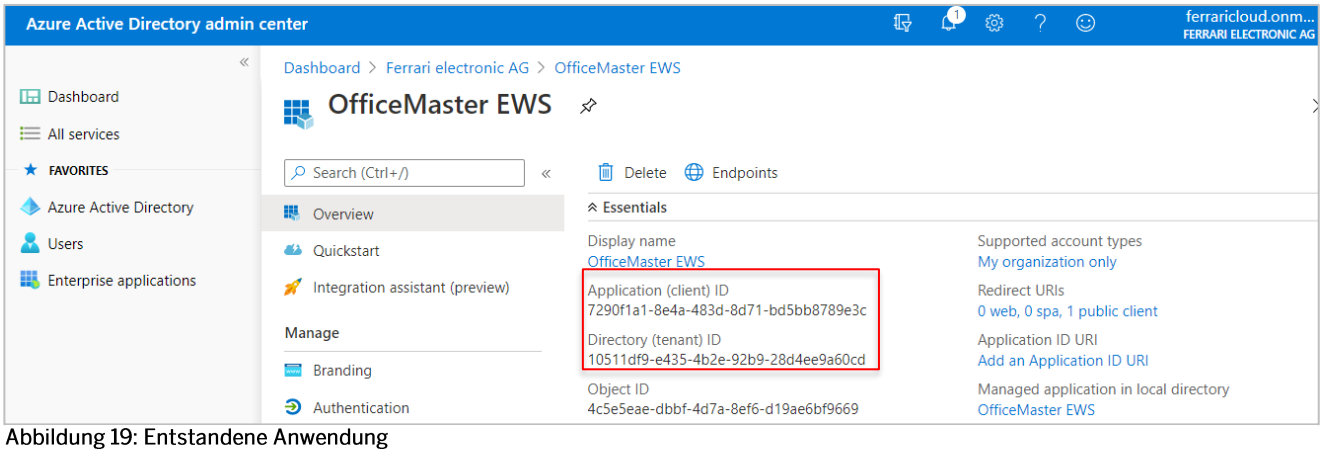


Abbildung 19: Entstandene Anwendung

4.2 API-Berechtigungen

Nun sollten die API-Berechtigungen gesetzt werden. In der registrierten Applikation navigiert man dazu zu den API-Berechtigungen.

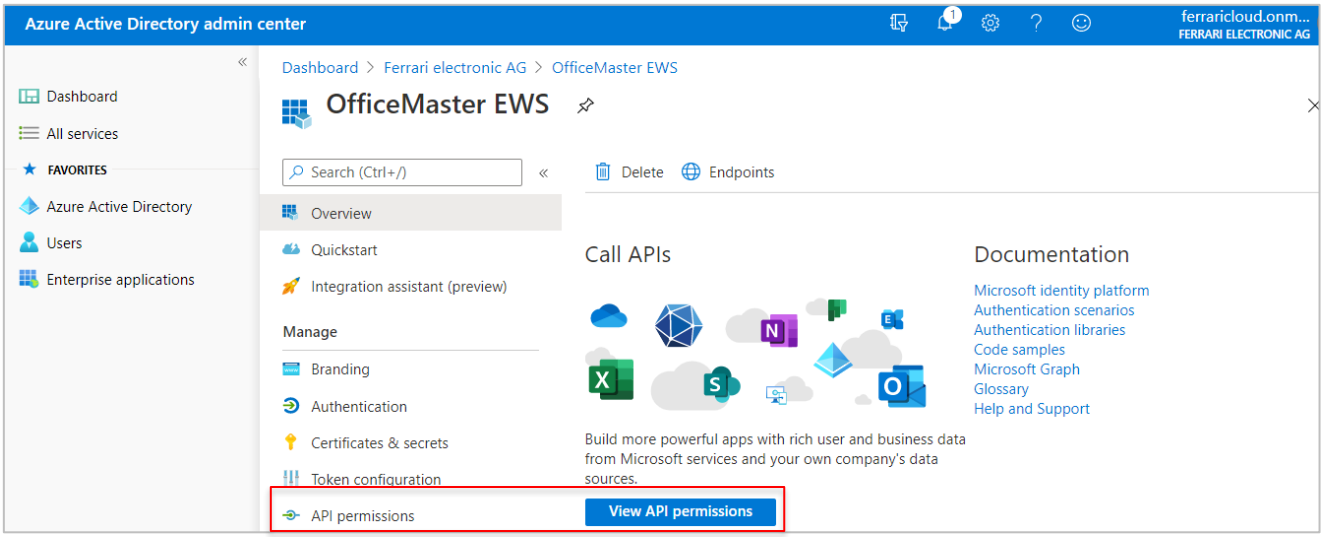


Abbildung 20: Navigation zu den API-Berechtigungen

Man kann sehen, dass in der allgemeinen Erstellung bereits eine API-Berechtigung automatisch angelegt wurde. Dies ist eine Basisberechtigung. Für den weiteren Betrieb werden weitere Berechtigungen benötigt.

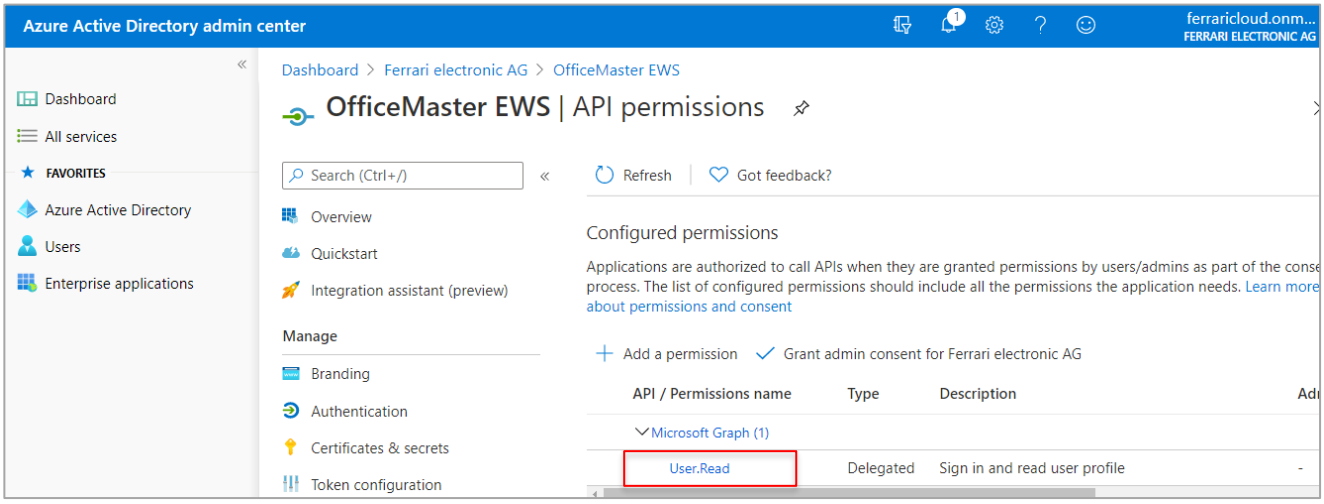


Abbildung 21: API-Berechtigungen hinzufügen

- Exchange Online EWS: full_access_as_app (als Applikationsberechtigung)

  Diese Berechtigung berechtigt die Applikation zum Lesen und Bearbeiten der Transfermailbox, sowie zum Zugriff auf die Benutzerpostfächer, um Voice-Aufgaben vornehmen zu können. Ebenfalls wird damit die Konfiguration der Benutzer über die OfficeMaster Exchange Administration ermöglicht, da in einer Cloud-Only-Installation die benutzerspezifischen Werte im Postfach gespeichert werden.

- Microsoft Graph: People.Read.All und User.Read.All (als Applikationsberechtigung)

  Diese Berechtigungen werden für Anfragen an die Adresslisten der Cloud benutzt.

Um die Berechtigungen hinzuzufügen hakt man die entsprechenden Punkte an.

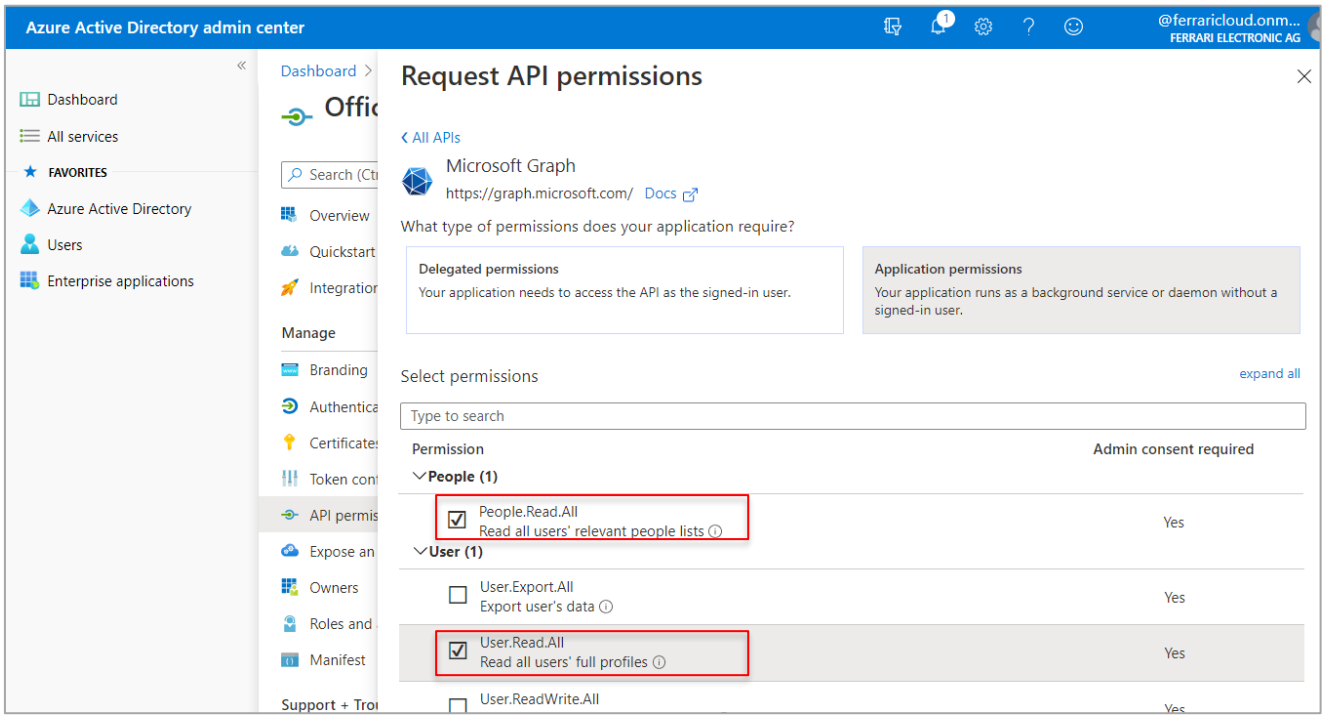


Abbildung 22: Microsoft Graph Berechtigungen setzen (stilisiert)

Die Berechtigung für die Exchange Web Services muss ebenso angehakt werden. Diese findet man beim Icon für das Exchange Online.

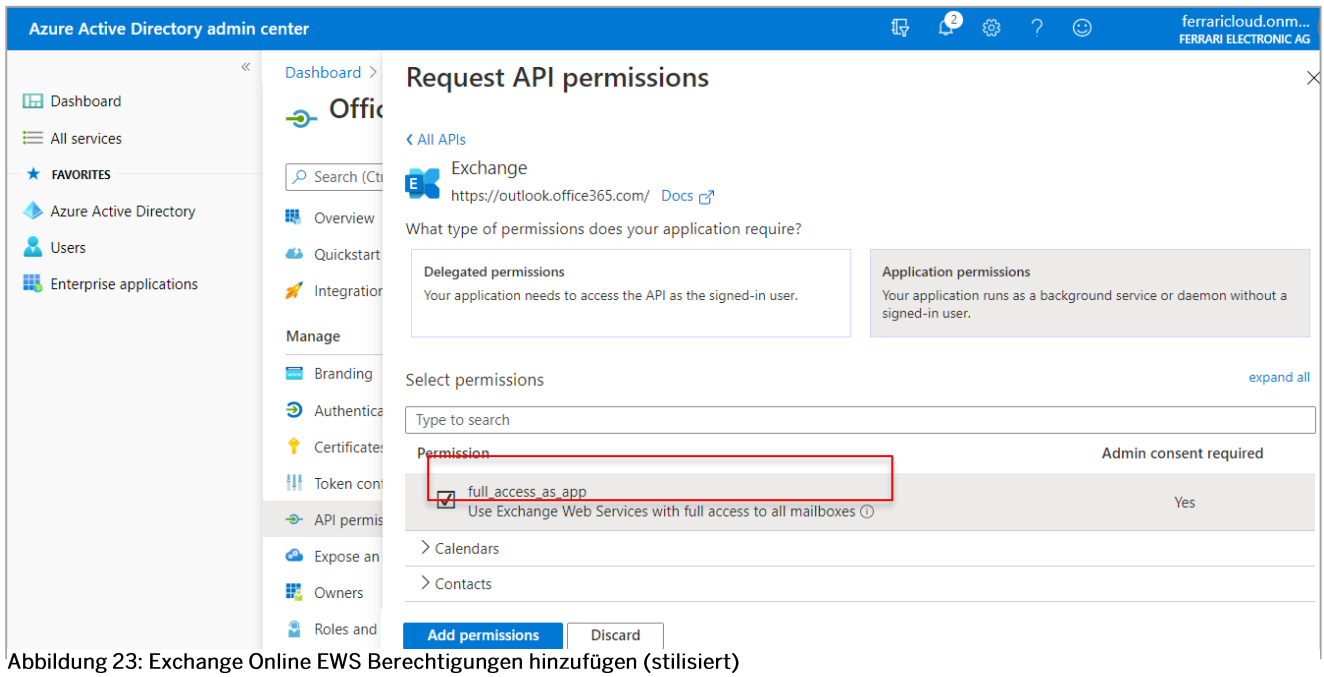


Abbildung 23: Exchange Online EWS Berechtigungen hinzufügen (stilisiert)

4.3 API-Berechtigungen freigeben

Nachdem die Berechtigungen hinzugefügt wurden, müssen diese durch einen Administrator freigegeben werden (Grant admin consent).

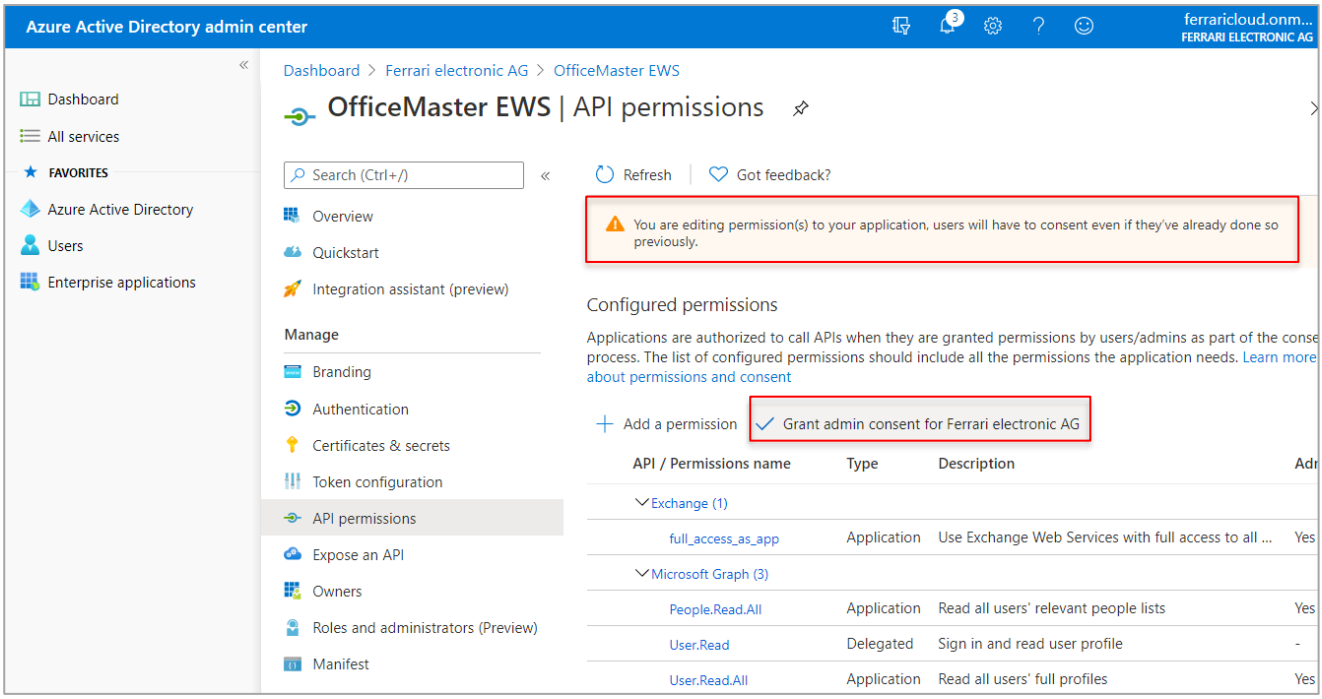


Abbildung 24: API-Berechtigungen freigeben

Nachdem die API-Berechtigungen freigegeben wurden, sind diese durch einen gründen Haken zu sehen.

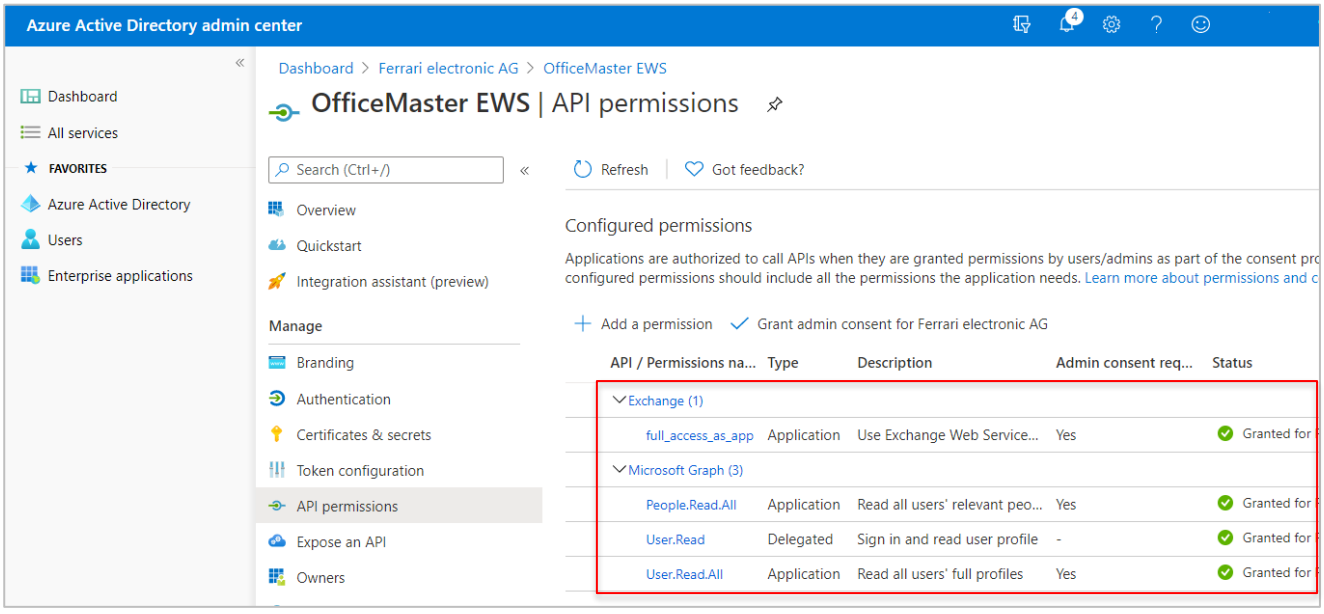


Abbildung 25: Freigegebene API-Berechtigungen

4.4 Anwendungsgeheimnis (Client Secret) erstellen

Zum Zugriff mit der Client-Id der registrierten Anwendung wird ein Geheimnis (Client Secret) benötigt. Um dieses zu erstellen, navigiert man in der registrierten Anwendung zum Punkt Zertifikate und Geheimnisse (Certificates and secrets). Dort kann man dann ein Geheimnis erstellen. Der Name des Geheimnisses spielt nur für administrative Zwecke eine Rolle. Da solche Namen mehrfach vergeben werden können, sollte dies ein sinnvoller Name sein.

Die Geheimnisse haben in der Regel eine Gültigkeitsdauer. Der automatische Installationsassistent erzeugt ein Geheimnis mit einer Gültigkeit von 2 Jahren. Dies muss nach Ablauf der Gültigkeit wieder aktualisiert werden.

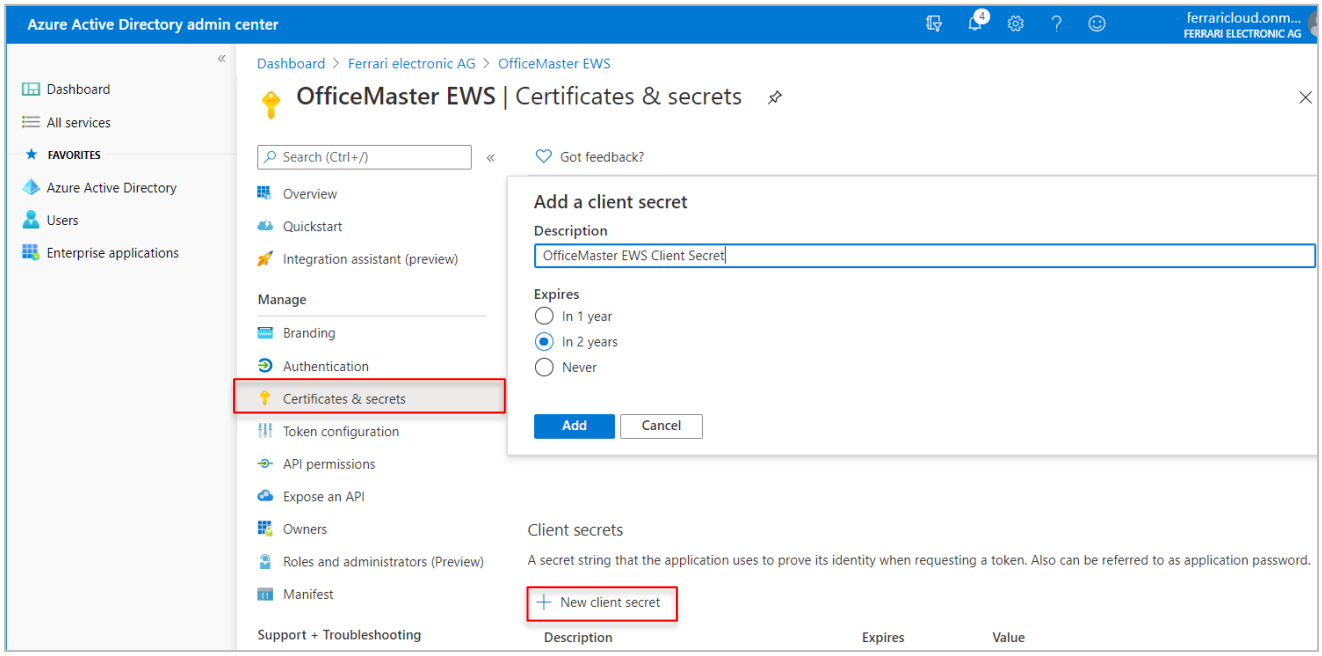


Abbildung 26: Geheimnis erstellen

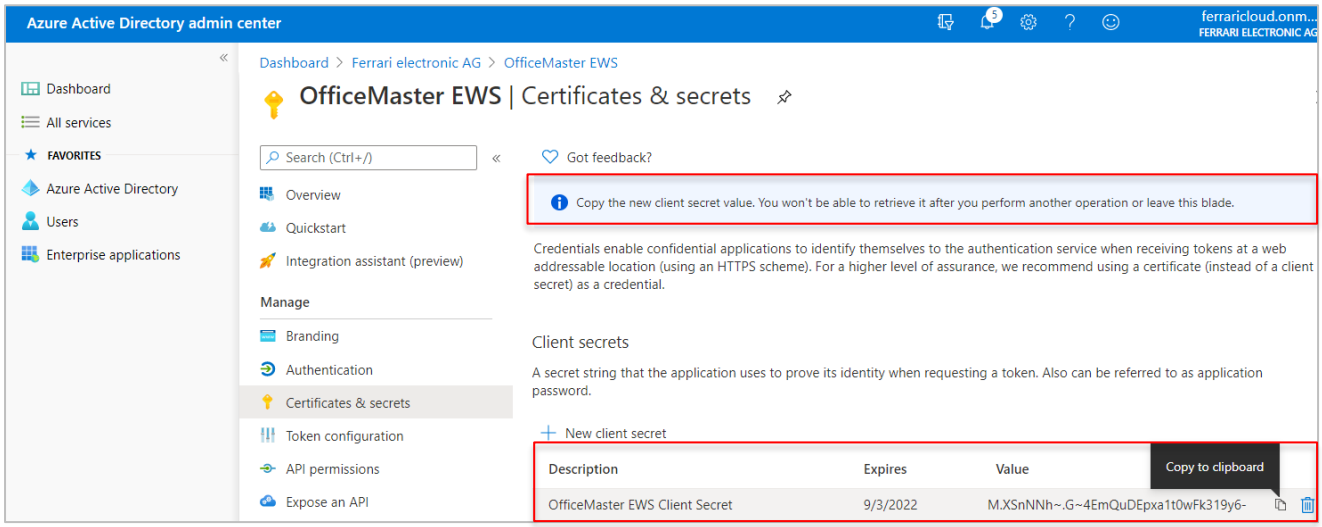


Abbildung 27: Erstelltes Geheimnis

Nachdem das Geheimnis erstellt wurde, steht dieses nur für diesen Augenblick zum Kopieren zur Verfügung. Dieses sollte unbedingt dann notiert werden. Mit der Tenant Id (Mandanten-Id), der Client Id (Anwendungs Id) und dem Client Secret (Geheimnis) stehen dann alle notwendigen Werte zur Verfügung, um diese während der Installation (siehe Punkt 2) oder nachträglich (siehe Punkt 3) einzugeben.

5. Umschaltung eines bestehenden OfficeMaster 7.1 auf die moderne Authentifikation

5.1 Manueller Umstieg

Wenn ein bestehendes System der OfficeMaster Version 7.1 auf die moderne Authentifikation umgestellt werden, so kann man dies manuell vornehmen. In diesem Fall sind zwei Schritte notwendig:

1. Die OfficeMaster Anwendung muss nach Punkt 4 manuell registriert werden.

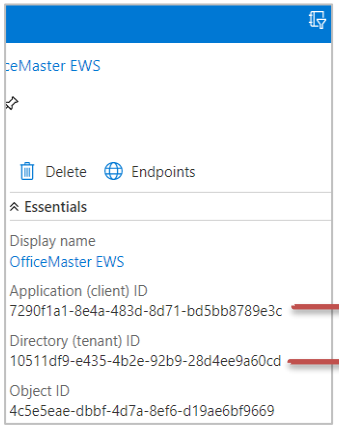


Abbildung 28: EWS Anwendung

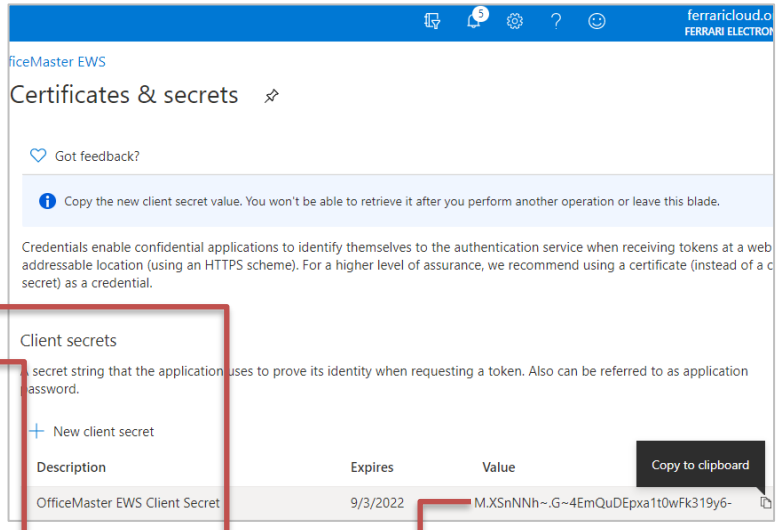


Abbildung 29: Neues

Dabei werden die drei wichtigen Felder: Tenant Id, Application (Client) Id und Client Secret notiert.

2. Die ermittelten Werte werden in die Konfiguration des Connectors in der OfficeMaster Exchange Verwaltung eingetragen. Der Connector wird dann auf „Moderne Authentifikation“ umgestellt.

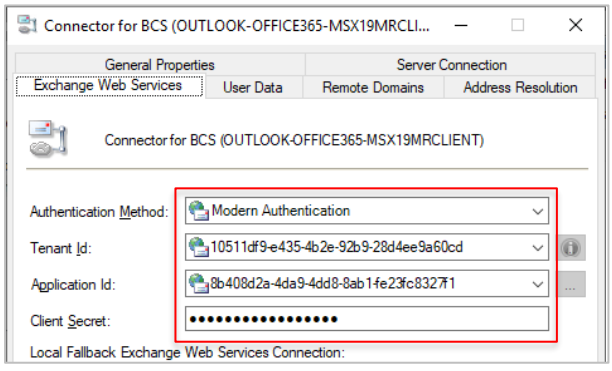


Abbildung 30: EWS-Einstellungen

5.2 Automatisierter Umstieg

Ein etwas einfacherer Umstieg ist der automatisierte Umstieg. In diesem Fall wird der Connector mit dem Installationsassistenten des OfficeMaster Messaging Server Konfigurationsprogrammes einfach überinstalliert. Bei dieser Überinstallation müssen die Transferdomänen und das Transferpostfach noch einmal explizit angegeben werden. Wenn diese Eintragungen nicht verfügbar sein sollten, empfiehlt sich die Methode in Punkt 5.1.

Anhang

I Technische Referenzen und Downloads

Technische Referenzen

Weitergehende technische Artikel können unter folgender Webadresse angezeigt werden:

http://ferrari-electronic.de

Die Ferrari electronic AG betreibt ein Partnerforum. Für die Anmeldung am Forum wenden Sie sich bitte an Ihren zuständigen Partner Account Manager.

http://forum.officemaster.de

Download von Handbüchern:

Handbücher zum OfficeMaster für Exchange können unter folgender Webadresse immer aktuell heruntergeladen werden:

http://www.ferrari-electronic.de

Download aktueller Software:

Offizielle Software zum OfficeMaster für Exchange können unter folgender Webadresse immer aktuell heruntergeladen werden:

http://www.ferrari-electronic.de

Weitergehende Artikel der Firma Microsoft:

Registrieren von Anwendungen in der Cloud:

https://docs.microsoft.com/de-de/azure/active-directory/develop/scenario-desktop-app-registration

Unterstützung für die Basic Authentication:

https://developer.microsoft.com/en-us/office/blogs/deferred-end-of-support-date-for-basic-authentication-in-exchange-online/

Abschalten der Basic Authentication im Exchange Online:

https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/disable-basic-authentication-in-exchange-online

Änderungen, die dem technischen Fortschritt und der Weiterentwicklung des Produkts dienen, sind vorbehalten!