Administration

Hier finden Sie Hinweise zu modulunabhängigen administrativen Tätigkeiten in iX-Haus.

Programmstart von iX-Haus plus

Per Systemeinstellung `StartIxHausPlus` kann festgelegt werden, dass iX-Haus plus automatisch gestartet wird, wenn iX-Haus gestartet wird. Diese Systemeinstellung befindet sich unter `Fachadministration > System > Systemeinstellungen Datenbank > iX-Haus > Allgemein > StartIxHausPlus`. Diese Einstellung macht Sinn, wenn nahezu alle Benutzer in der Benutzerverwaltung auch für iX-Haus plus freigeschaltet sind und häufig auch in iX-Haus plus tätig sind.

Aufruf von iX-Haus plus Modulen aus iX-Haus

Beachten Sie, dass die Nutzung einiger Module abhängig von einer entsprechenden Lizenz oder Einrichtung ist. iX-Haus-Benutzer werden beim Aufruf eines iX-Haus plus Moduls automatisch in der Benutzerverwaltung von iX-Haus für iX-Haus plus gekoppelt. Benutzerverwaltung von iX-Haus plus. Einschränkungen im Modulzugriff werden u. a. durch die Programmrechte definiert. Mit welcher Benutzerrolle der Benutzer in iX-Haus plus arbeitet und welche Module er dort im Zugriff hat, wird administrativ in iX-Haus plus in der Benutzerverwaltung eingestellt. Beim Aufruf von iX-Haus-Listen aus iX-Haus plus heraus werden die Benutzerrechte ebenfalls geprüft. Damit ist die Möglichkeit, Programmrechte auch auf Ebene einzelner iX-Haus-Listen zu definieren, auch in iX-Haus plus realisiert.

Lizenzverwaltung

In der Lizenzverwaltung sehen Sie unter `Freigeschaltete Module` die jeweils lizenzierten Module und deren zulässige Benutzeranzahl sowie die Gültigkeit der aktuellen Lizenz. Die Gültigkeit kann auf ein Enddatum eingeschränkt sein. Zur Verwaltung der Lizenzen ist eine administrative Anmeldung erforderlich.

Lizenz für iX-Haus plus

Für eine `iX-Haus plus-Lizenz` erhalten Sie gleichnamige `lic`- und `txt`-Dateien per E-Mail von der CREM SOLUTIONS. Die Beschreibung zur Installation einer iX-Haus plus-Lizenz wird auch in der E-Mail beschrieben. Für eine manuelle Installation benötigen Sie administrative Benutzerrechte. Alternativ kann die bereitgestellte Lizenz durch einen Hauptbenutzer als Download abgerufen und über das Fenstermenü `Extras` > `iX-Haus Lizenz einspielen` in iX-Haus oder iX-Haus plus installiert

werden.

Lizenz per Download installieren

Das Einspielen von Lizenzen für iX-Haus und iX-Haus plus kann automatisiert erfolgen. Bei Lizenzänderungen oder Lizenzerweiterungen können neue Lizenzen zentral aus iX-Haus heruntergeladen und installiert werden. Hauptbenutzer finden in iX-Haus plus im Anwendungsmenü unter `Extras` den Punkt `iX-Haus Lizenz einspielen`. Im darauffolgenden Dialog können Sie per Schalter `Lizenzen abrufen` prüfen, ob neue Lizenzen für iX-Haus und iX-Haus plus vorhanden sind. Diese Lizenzen werden über einen SFTP-Server bereitgestellt und automatisch heruntergeladen. Innerhalb des Vorgangs können Sie die Unterschiede zwischen der bestehenden und der neuen Lizenz anzeigen lassen. Durch den Aufruf `Lizenz einspielen` werden die aktuellen Lizenzen eingespielt. Siehe Kapitel Administration > Abschnitt Lizenzinstallation für iX-Haus.

Lizenz manuell installieren

So installieren Sie eine Lizenz als Benutzer mit administrativen Rechten manuell:

1. Sie erhalten von der CREM SOLUTIONS eine E-Mail mit den Dateianhängen `Kundenname_Lizenznummer.lic` (Lizenzdatei), `Kundenname_Lizenznummer.txt` (Textdatei mit Lizenzkey) und einer begleitenden Anleitung als PDF-Datei.
2. Legen Sie die E-Mail-Anhänge so ab, dass Sie im späteren Verlauf auf die einzelnen Dateien zugreifen können.
3. Starten Sie iX-Haus plus. Beim erstmaligen Start von iX-Haus plus erhalten Sie zunächst die Meldung: „Lizenz ist ungültig! Bitte eine gültige Lizenz installieren.“
4. Melden Sie sich mit dem Benutzerkennung `admin` an. (Das Passwort erhalten Sie bei der Installation bzw. ist dem Administrator bekannt.)
5. Nach dem Anmelden öffnen Sie zum Installieren Ihrer iX-Haus plus Nutzerlizenz den Menüpunkt `Extras`. Dort wählen Sie `Lizenz installieren` aus.
6. Bestätigen Sie die Sicherheitsabfrage „Neue Lizenz installieren?“ mit `Ja`.
7. Im Dialog `Öffnen` haben Sie Zugriff auf Ihr Dateisystem. Öffnen Sie die zuvor abgelegt Lizenzdatei mit der Dateiendung `.lic`. Der Dateiname ist kundenspezifisch. Er setzt sich aus dem Kundennamen und der Lizenznummer zusammen.
8. Es öffnet sich der Dialog der Lizenzkey-Eingabe mit der Aufforderung `Bitte Lizenzkey eingeben`. Kopieren Sie aus der zuvor abgelegten .txt-Datei den Lizenzschlüssel. Der Dateiname ist kundenspezifisch. Er setzt sich aus dem Kundennamen und der Lizenznummer zusammen.
9. Bei korrekter Eingabe des Lizenzschlüssels erscheint rechts neben dem Feld ein grünes Häkchen und Sie können Ihre Eingabe mit OK bestätigen.
10. Nach erfolgter Lizenzinstallation muss iX-Haus plus neu gestartet werden.
11. Ihr Programm ist nun freigeschaltet und Sie können mit der Einrichtung des Programms beginnen oder Ihre Arbeit fortsetzen.
12. Starten Sie `iX-Haus plus` nach einer Lizenzinstallation erneut, damit die Änderungen wirksam werden.

Beinhaltet die neue Lizenz Freischaltungen für den Import, müssen Sie das Importmodul für bestimmte Benutzer erst in der Benutzerverwaltung entsperren! I. d. R. wird der Import nur von einem Benutzer ausgeführt.

Verantwortlichen ändern

Mit der Lizenz zum Komfortpaket und als Admin in iX-Haus plus angemeldet können Sie über `Extras`, `Verantwortlichen ändern` die Eintragung eines Verantwortlichen in iX-Haus plus wechseln, z. B. bei einer Aufteilung von Aufgabenbereichen oder beim Ausscheiden eines Mitarbeiters. Dies kann für alle Objekte oder für einzeln benannte Objekte ausgeführt werden. Eine weitere Einschränkung kann mit dem Teamfilter über die Auswahl eines Teams erfolgen. Benennen Sie den Benutzer, dessen Zuordnung als Verantwortlicher entzogen werden soll und den Benutzer der diese Zuordnung übernimmt. Über den Modulfilter bestimmen Sie, in welchen iX-Haus plus-Modulen diese Änderung ausgeführt werden soll.

Globale Einstellungen

CTI-Telefonanbindung

Über die CTI-Telefonanbindung haben Sie die Möglichkeit, bei eingehenden Anrufen direkt zum Anrufer in die Detail-Maske von Personen plus bzw. Kreditoren plus zu wechseln. So haben Sie wesentlichen Daten zur Person direkt auf dem Bildschirm und können den Anrufer persönlich ansprechen. Zudem können Sie aus Personen plus bzw. Kreditoren plus komfortabel anrufen. In Verbindung mit dem Komfortpaket steht Ihnen die Anruffunktion sogar beim Objekt zur Verfügung, um den Hausmeister, zuständigen Installateur etc. anzurufen.

Voraussetzungen

- TAPI-fähige Telefonanlage
- Installierte TAPI-Treiber auf dem Client-Rechner
- iX-Haus CTI Telefonanbindung - Lizenz

Technische Voraussetzungen prüfen

Bevor Sie mit der Einrichtung starten, sollten Sie mit Hilfe von `CTI-Test` prüfen, ob die technischen Voraussetzungen für den Einsatz einer CTI Telefonanbindung bei Ihrer Telefonanlage gegeben sind. Sie finden dieses Testprogramm unter dem Menüpunkt `Hilfe`. Sie können es aber auch im iX-Haus-Verzeichnis unter `nuris\ctitest.exe` starten.

Im Dialog `CTI-Test` wird Ihnen neben dem Eingabefeld zur Auswahl der zu prüfenden Leitung und den Schaltern zum Steuern des Tests ein Protokoll angezeigt. Hier finden Sie entsprechende Testhinweise wie `TAPI Treiber nicht installiert oder nicht konfiguriert.` und Handlungshinweise und -ergebnisse wie `Bitte rufen sie jemanden an oder lassen Sie die ausgewählte Rufnummer anrufen`, … `CTI-Test erfolgreich abgeschlossen!` oder `CTI-Test leider nicht erfolgreich, kontaktieren Sie Ihren Administrator.`



Der CTI-Test ist eine technische Prüfung der bei Ihnen konfigurierten CTI-Einrichtung. Ist

der Test erfolgreich, können Sie mit Lizenz und nach entsprechenden Systemeinstellungen mit iX-Haus und iX-Haus plus CTI-Funktionen nutzen. Ist der CTI-Test nicht erfolgreich, muss Ihr Administrator weitere Einstellungen vornehmen oder konfigurieren. Starten Sie danach den CTI-Test erneut.

1. Starten Sie in iX-Haus plus unter `Hilfe` den `CTI-Test`.
2. Wählen sie im Feld `Telefonleitung` die zu nutzende Leitung. Sollten Sie keine oder mehrere zur Auswahl haben, klären Sie bitte Ihren Administrator, welche Einrichtung noch vorgenommen werden muss oder welche Leitung zum CTI mit Ihrer Telefonanlage gekoppelt ist.
3. Mit dem Schalter `Überwachung starten` starten Sie den Test für die gewählte Telefonleitung.
4. Mit dem Schalter `Anwählen` prüfen Sie die Wählfunktion. Geben Sie im Dialog eine Rufnummer an, die Sie wählen wollen, z. B. das eigene Mobiltelefon oder die externe Rufnummer eines Bürokollegens.
5. Lassen Sie sich zum Test auf der eigenen Rufnummer anrufen.
6. Mit dem Schalter `Überwachung beenden` schließen Sie den Test ab.
   Das Programmfenster bleibt geöffnet und Sie können die Protokollergebnisse prüfen und ggf. weiterleiten (Screenshot vom Fenster mit Alt+Druck erzeugen), insbesondere wenn Sie als Anwender den CTI-Test gestartet haben und der Administrator ggf. in Aktion treten muss.
7. Beenden Sie das CTI-Testprogramm mit Klick auf den X-Schalter rechts oben im Programmfenster des CTI-Tests.

Einrichtung
Wenn alle technischen Voraussetzungen für die CTI Telefonanbindung erfüllt sind und eine entsprechende Lizenz installiert ist, können Sie in iX-Haus unter `Fachadministration – Systemeinstellungen Datenbank` unter `iX-Haus Plus– Globale Einstellungen` die CTI-Kopplung aktivieren sowie die Nummernlänge und Vorwahl für externe Anrufe setzen. Hierzu dienen die einzelnen Systemeinstellungen:

- `PlusGlobalCTIKopplungAktiv`
- `PlusGlobalCTIReactionAbhebebHoerer`
- `PlusGlobalCTIreactionNummernlaenge`
- `PlusGlobalCTIVorwahlExternAnrufe`
- `iXHausCTIKopplungAktiv`

Anschließend kann nach einem Neustart von iX-Haus/iX-Haus plus jeder Benutzer in der `Benutzerverwaltung` von iX-Haus plus in der Sicht `Meine Daten` seine passende Telefonleitung auswählen. Hierzu nutzt er dort das Feld `CTI-Kopplung`.

Wenn die CTI-Schnittstelle aktiv ist, wird ein Hinweis in der Benutzerdetailsicht für den Administrator eingeblendet, um die korrekte Zuordnung von Benutzer und Telefonleitung zu gewährleisten: „Hinweis: Bei der CTI-Kopplung muss jeder Benutzer für sich selbst seine passende Telefonleitung auswählen.“ Die CTI-Kopplung wird bei inaktiver CTI-Schnittstelle oder in der Benutzerdetailsicht eines anderen Benutzers ausgegraut.

Eingehende Anrufe entgegennehmen
Bei einem eingehenden Anruf sucht iX-Haus plus in den iX-Haus-Stammdaten (Personenstamm, Kreditorenstamm sowie Eigentümern) nach Treffern mit der Telefonnummer und zeigt alle Treffer in

einem Dialogfenster. Es öffnet sich ein Dialog iX-Haus plus - eingehender Anruf (mit Rufnummer und Uhrzeit) mit Anzeige der möglichen Treffer und deren Herkunft.

Dadurch haben Sie die Möglichkeit, mit den Schaltern im Bereich Aktionen mit Mausklick direkt zur Startseite oder zu Personen plus bzw. Kreditoren plus Detail-Maske zu wechseln. Weiterhin können Sie direkt eine Meldung oder einen Auftrag erstellen (sofern Sie diese Module lizensiert haben).

Den CTI-Dialog können Sie mit den Funktionen Maximieren/Verkleinern in seiner Darstellung anpassen. Hierzu klicken Sie auf den entsprechenden Schalter in rechten oberen Ecke des Dialogfensters.

Anrufe tätigen
In der Detailsicht können Sie über die Schaltfläche Anrufen (Telefonhörersymbol hinter einem Telefonnummernfeld) können Sie angezeigte Telefonnummer direkt anwählen.

In der Listen-Sicht wird über die Schaltfläche Anrufen ein Dialogfenster mit allen Telefonnummern angezeigt, die für den ausgewählten Datensatz zu Verfügung stehen. Aus dem Dialogfenster Anrufen können Sie dann eine dort ausgewählte Nummern anrufen. Eine Mehrfachauswahl ist hier nicht möglich.

Einstellungen für den E-Mail-Server (SMTP/OAuth2) konfigurieren

Zur Versendung von E-Mails aus iX-Haus plus müssen SMTP/OAuth2-Einstellungen vorgenommen werden. Die Einstellungen werden in Hintergrundprozessen, z. B. beim Zahlungsavis, in der Protokollverwaltung oder für den Scheduler genutzt. Hierzu wird ein Standard-SMTP/OAuth2-Konto eingerichtet. Zusätzlich zum dem Standard-Konto, welches für bestehende Prozesse verwendet wird, können weitere Konten definiert werden. Wird ein Konto nicht als Standard-Konto definiert, werden bestimmte weitere Parameter ein-/oder ausgeblendet.

Zur Konfiguration ist die Anmeldung mit Administratorrechten erforderlich. Die Einstellung erfolgt im Register SMTP/OAuth2 Einstellungen. Sie legen hier entweder einen neuen Datensatz an oder rufen eine bestehende Definition zur Bearbeitung auf. In dem hierzu verwendeten Dialog SMTP-Konto sind die Parameter je nach Mail-Server Autorisierungstyp einzustellen.

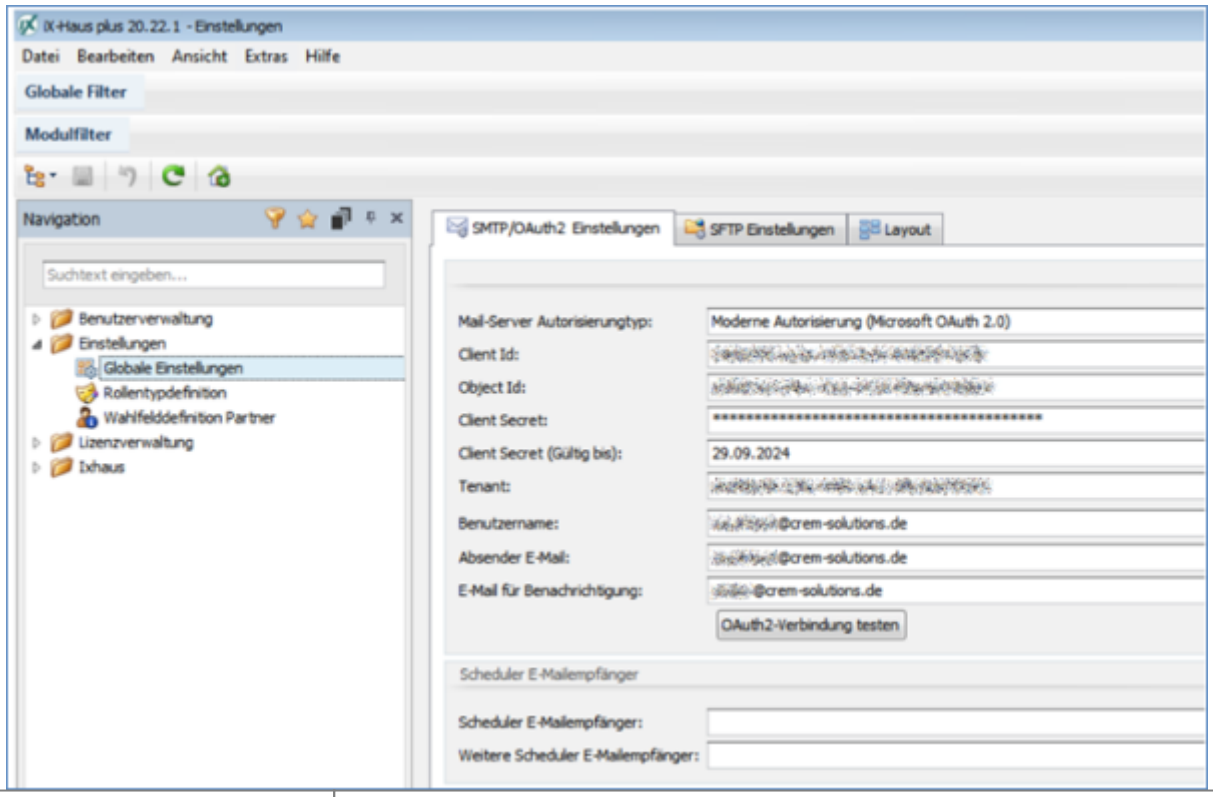
Weitere SMTP/OAuth2-Konten anlegen

Bei Bedarf kann jedem iX-Haus-Modul, welches die Funktion Auto-Zustellweg unterstützt, ein spezifisches SMTP/OAuth2-Konto und damit ein E-Mail-Absender zugeordnet werden. Möchten Sie beispielsweise Mahnungen und Fakturarechnungen von dem E-Mail-Konto buchhaltung@musterfirma.de mailen, so ist dieses darstellbar, indem Sie neben dem Standardkonto ein weiteres Konto definieren und hier unter Freischaltung für Module die gewünschten Varianten der Module markieren sowie die weiteren individuellen Parameter für das Konto definieren. Bei Anlage mehrerer Konten können Sie auch Speichern und Neu aus der Symbolleiste oder dem Datei-Menü nutzen.

Moderne Autorisierung (Microsoft OAuth 2.0)

Zur Konfiguration eines neuen E-Mail-Kontos ist die Auswahl Moderne Autorisierung (Microsoft OAuth 2.0) vorbelegt. Es werden Ihnen somit OAuth2-spezifische Parameterfelder angezeigt.

Ab dem 01.10.2022 wird die Standardauthentifizierung für Outlook- EWS-, RPS-, POP-, IMAP- und EAS-Protokolle in Exchange Online deaktiviert (relevant für Anwender mit Microsoft Exchange Online im Rahmen der E-Mail-Anbindung in iX-Haus plus). Für die Konfiguration der Anbindung muss zur Nutzung einer sicheren Anbindung, Microsoft OAuth 2.0 genutzt werden. Zu dessen Administration liefern wir Ihnen nachfolgend entsprechende Informationen. In iX-Haus plus wird administrativ unter `Einstellung` > `Globale Einstellungen` im Register `SMTP/OAuth2 Einstellungen` eine passende Konfiguration eingestellt. Im Feld `Mail-Server Autorisierungstyp` wählen Sie dann `Moderne Autorisierung (Microsoft OAuth 2.0)`. Sie müssen dort nun die weiteren Parameter eintragen. Mittels der Schaltfläche können Sie dann die `OAuth2-Verbindung testen`.



`Bezeichnung`	Geben Sie hier eine eindeutige Bezeichnung für diese SMTP-Konfiguration an.
`Standardkonto`	Kontrollfeld Eine OAuth2-Konfiguration kann als Standard definiert werden.
`Freischaltung für Module`	Diese Auswahl ist für das Standardkonto nicht verfügbar. Soll die Konfiguration nur für bestimmte Module verwendet werden, wählen Sie diese hier aus.
`Verwalter`	Diese Auswahl ist für das Standardkonto nicht verfügbar. Soll die Konfiguration nur für bestimmte Verwalter verwendet werden, wählen Sie diese hier aus.
`Niederlassung`	Diese Auswahl ist für das Standardkonto nicht verfügbar. Soll die Konfiguration nur für bestimmte Niederlassungen verwendet werden, wählen Sie diese hier aus.
`Mail-Server Autorisierungstyp`	Auswahl: `Moderne Autorisierung (Microsoft OAuth 2.0)`
`Client Id`	Pflichtfeld; Anwendungs-ID (Client) aus der App-Registrierung. Kann auch aus der Übersicht zur registrierten Anwendung ausgelesen werden.

Object Id	Objekt-ID aus der App-Registrierung. Kann auch aus der Übersicht zur registrierten Anwendung ausgelesen werden. Mit diesem Feld wird das Ablaufdatum des Parameters Client Secret abgefragt. Das Ablaufdatum von Client Secret wird beim Verbindungtest automatisch aktualisiert. Bei Einrichtung muss eine zusätzliche Berechtigung für eine registrierte Anwendung vergeben werden, um das Ablaufdatum des Client Secret abrufen zu können. Einzustellen unter Anwendung Berechtigungen > Aplication.Read.All, Delegierte Berechtigungen > Directory.Read.All.
Client Secret	Pflichtfeld; Wert des Secret aus Zertifikate & Geheimnisse zum geheimen Clientschlüssel. Dieser wird bei der Erstellung des Secret nur einmal in Klartext angezeigt.
Client Secret (Gültig bis)	Pflichtfeld; Da der Parameter Client Secret ein Ablaufdatum besitzt, muss dieses bei Einrichtung der Autorisierung gepflegt werden. Der Empfänger wird daraufhin in einem Verlauf von 30 Tagen, 7 Tagen und einem Tag im Vorfeld per E-Mail benachrichtigt (i. d. R. sind diese zwei Jahre gültig und müssen dann erneuert werden).
Tenant	Pflichtfeld; Verzeichnis-ID (Mandant) aus der App-Registrierung. Kann auch aus der Übersicht zur registrierten Anwendung ausgelesen werden.
Benutzername	geben Sie hier den Benutzernamen für die Anmeldung am Mail-Server an.
Absender-E-Mail	Geben Sie hier die E-Mail-Adresse des Absenders an.
E-Mail für Benachrichtigung	Pflichtfeld; siehe Client Secret (Gültig bis); Eingabe einer E-Mail-Adresse für den Empfänger der Erinnerungs-E-Mail vor Ablauf der Gültigkeit des E-Mail-Kontos. Betreff und Inhalt der E-Mail-Benachrichtigung sind systemseitig definiert.
Scheduler E-Mailempfänger / Weitere Scheduler E-Mailempfänger	Hier können zwei globale E-Mail-Adressen für entsprechende Empfänger eingerichtet werden, an die im Fall einer Störung, z. B. wenn ein Job nicht gestartet oder blockiert wird, E-Mails zur Kontrolle gesendet werden. Diese Felder sind nur für die Definition des Standardkontos verfügbar.

Sie können über Bearbeiten im Fenstermenü die OAuth2-Verbindung testen, um die korrekte Datenübermittlung zu prüfen. Geben Sie hierzu eine gültige Empfänger-E-Mail-Adresse ein.

Basic Autorisierung (SMTP)

Zur Definition für einen SMTP-Server wählen Sie im Dialog SMTP-Konto im Feld Mail-Server Autorisierungstyp die Auswahl Basic Autorisierung (SMTP). Es werden Ihnen dann SMTP-spezifische Parameterfelder angezeigt.

Bezeichnung	Geben Sie hier eine eindeutige Bezeichnung für diese SMTP-Konfiguration an.
Standardkonto	Kontrollfeld Eine SMTP-Konfiguration kann als Standard definiert werden.
Freischaltung für Module	Auswahl, für Standardkonto nicht verfügbar Soll die Konfiguration nur für bestimmte Module verwendet werden, wählen Sie diese hier aus. Ansonsten wird hier keine Auswahl angezeigt.

Verwalter	Auswahl, für Standardkonto nicht verfügbar Soll die Konfiguration nur für bestimmte Verwalter verwendet werden, wählen Sie diese hier aus. Ansonsten bleibt das Feld leer.
Niederlassung	Auswahl, für Standardkonto nicht verfügbar Soll die Konfiguration nur für bestimmte Niederlassungen verwendet werden, wählen Sie diese hier aus. Ansonsten bleibt das Feld leer.
Mail-Server Autorisierungstyp	Auswahl: Basic Autorisierung (SMTP).
ObjektId	ID der registrierten Anwendung.
SMTP-Server	Adresse des SMTP-Servers.
Port	Verwendeter Port am SMTP-Server.
SSL erforderlich	[X] Checkbox für den Einsatz von verschlüsselter Übertragung.
Benutzername	Benutzername für die Anmeldung am SMTP-Server.
Passwort	Passwort für die Anmeldung am SMTP-Server. Das eingegebene Passwort wird mit Sternchen verdeckt dargestellt.
Absender-E-Mail	E-Mail-Adresse des Absenders. Für E-Mails durch einzelne Mitarbeiter wie z. B. Schriftgutversand wird die Outlook-Schnittstelle genutzt.
Antwort an (E-Mail-Adresse)	E-Mail-Adresse Geben Sie hier die E-Mail-Adresse an, welche beim Versand als Rückantwortadresse übermittelt werden soll. Antworten auf E-Mails von diesem SMTP-Konto können so an eine abweichende E-Mailadresse gesendet werden.
Scheduler E-Mailempfänger	Geben Sie hier die E-Mail-Adresse des Empfängers ein, an den im Fall einer Störung, z. B. wenn ein Job nicht gestartet wird oder blockiert, E-Mails zur Kontrolle gesendet werden. Das Feld ist nur für die Definition des Standardkontos verfügbar.
Weitere Scheduler E-Mailempfänger	Geben Sie hier weitere E-Mail-Adressen des Empfängers ein, an den im Fall einer Störung, z. B. wenn ein Job nicht gestartet wird oder blockiert, E-Mails zur Kontrolle gesendet werden. Das Feld ist nur für die Definition des Standardkontos verfügbar.

Sie können über Bearbeiten im Fenstermenü die SMPT-Verbindung testen, um die korrekte Datenübermittlung zu prüfen. Geben Sie hierzu eine gültige Empfänger-E-Mail-Adresse ein.

Setzen Sie „Exchange Online“ im Rahmen der E-Mail-Kommunikation ein (z. B. für Protokollverwaltung oder Scheduler), sollten Sie beachten, dass Microsoft hier ab dem 01.10.2022 Änderungen geplant hat. Diese betreffen u. a. den Einsatz der SMTP-Protokolle. Je nach Vorgehensweise müssen Sie für das E-Mail-Konto, welches bei den SMTP-Einstellungen in iX-Haus plus z. B. für die Kommunikation bestimmter Scheduler-Ereignisse verwendet wird, SMTP AUTH (wieder) deaktivieren, um weiterhin SMTP nutzen zu können. Details zu der Umstellung von Exchange Online und weiterführende Informationen finden Sie im Internet in den Onlinedokumenten von Microsoft, z. B. unter https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/authenticated-client-smtp-submission.

SMTP/OAuth2-Verbindung testen

Über diese Funktion aus dem Fenstermenü Bearbeiten im Dialog SMTP-Konto kann die SMTP- bzw. OAuth2-Verbindung für das aktuelle Konto durch den Benutzer getestet werden, um die korrekte Datenübermittlung zu prüfen. Geben Sie hierzu eine gültige Empfänger-E-Mail-Adresse ein. Äquivalent dazu können Sie im Register SFTP Einstellungen einen Verbindungstest durchführen, um den Empfang versendeter E-Mails zu prüfen.

Die Benutzerkennung am SMTP-Server darf hier nicht mit einer Zwei-Faktor-Autorisierung gesichert sein!

COM-Objekt Fehlermeldungen von Microsoftkomponenten

iX-Haus nutzt für die E-Mail-Kommunikation Komponenten von Microsoft. Diese werden installationsbedingt auf der jeweiligen Workstation des Anwenders erwartet. Hinweismeldungen wie `Das COM-Objekt des Typs „Microsoft.Office.Interop.Outlook.ApplicationClass“ kann nicht in den Schnittstellentyp „Microsoft.Office.Outlook.Interop.Outlook._Application“ umgewandelt werden.` beruhen meist darauf, dass das erwartete Element in der Office-Installation der Workstation fehlt. Es kann in diesen Fällen helfen, das Outlookprofil des betroffenen Users zu deinstallieren und nach dem Entfernen von Registry-Resten (bei Outlook Build 16.0 sind dies Registry-Einträge in den Bereichen Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\16.0 …15.0 … etc. sowie Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\16.0 …15.0 … etc.) und einem Rechnerneustart Office erneut zu installieren.

Wenn Outlook keinen programmgesteuerten Zugriff in den Vertrauenseinstellungen aktiviert hat, sollte diese Einstellung auf „Nie fragen“ gesetzt werden. Zusätzlich müssen die folgenden Registrierungseinträge ebenfalls auf den Wert „2“ gesetzt werden:

1. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office<Build Number>\Outlook\Security
    1. „ObjectModelGuard“=dword:00000002
2. HKEY_CURRENT_USER\Software\Policies\Microsoft\Office<Build Number>\Outlook\Security
    1. „PromptOOMSend“=dword:00000002
    2. „AdminSecurityMode“=dword:00000003
    3. „promptoomaddressinformationaccess“=dword:00000002
    4. „promptoomaddressbookaccess“=dword:00000002



Ersetzen Sie in diesem Beispiel die <Build Number> mit der entsprechenden Versionsnummer von Outlook (z. B. 16.0). Die folgenden Registrierungseinträge müssen ebenfalls auf den Wert „2“ gesetzt werden:

- HKEY_CURRENT_USER\software\policies\microsoft\office\16.0\outlook\security promptoomaddressinformationaccess
- HKEY_CURRENT_USER\software\policies\microsoft\office\16.0\outlook\security\ promptoomaddressbookaccess
- HKEY_CURRENT_USER\software\policies\microsoft\office\16.0\outlook\security\ promptsimplemapiopenmessage
- HKEY_CURRENT_USER\software\policies\microsoft\office\16.0\outlook\security\ promptsimplemapinameresolve
- HKEY_CURRENT_USER\software\policies\microsoft\office\16.0\outlook\security\ promptsimplemapisend
- HKEY_CURRENT_USER\software\policies\microsoft\office\16.0\outlook\security\ promptoomsend

Konfiguration Microsoft OAuth 2.0

Nachfolgend ein Auszug des Herausgebers für die verwendete Komponente. (Abschnitt `Send email using Microsoft OAuth 2.0 (Modern Authentication) + EWS/Ms Graph API protocol from Office 365`) mit den relevanten Informationen zur Konfiguration von Microsoft OAuth 2.0, welche dann in iX-Haus plus über die Globalen Einstellungen (s. o.) verwendet werden.

Office 365 OAuth 2.0 Client-Anmeldeinformationen gewähren

Normales OAuth erfordert die Eingabe von Benutzer/Passwort zur Authentifizierung. Offensichtlich ist es nicht für einen Hintergrunddienst geeignet. In diesem Fall können Sie OAuth 2.0 Client Credentials Grant, manchmal auch „Two-legged OAuth“ genannt, verwenden, um auf Web-gehostete Ressourcen zuzugreifen, indem Sie die Identität einer Anwendung verwenden. Dies funktioniert nur für Office365-Benutzer, nicht aber für persönliche Hotmail-Konten.

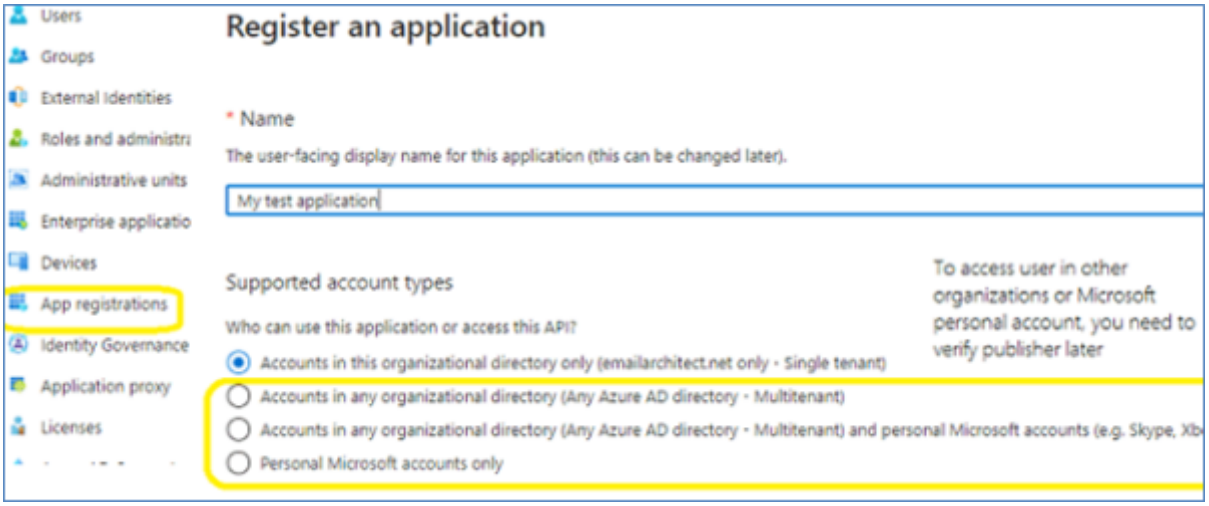
Erstellen einer Anwendung im Azure Portal

Um Microsoft/Office365/Live OAuth (Modern Authentication) in Ihrer Anwendung zu verwenden, müssen Sie eine Anwendung im Azure Portal erstellen.



Sie können jeden Microsoft-Benutzer verwenden, um die Anwendung zu erstellen. Es ist nicht erforderlich, dass der Eigentümer der Anwendung Administrator in Ihrer Office365-Domäne ist. Ihr Office365-Administrator muss jedoch die Anwendung für den Zugriff auf das Benutzerpostfach autorisieren. Es empfiehlt sich daher, direkt den administrativen Account zu nutzen.

- Melden Sie sich beim Azure-Portal entweder mit einem Arbeits- oder Schulkonto oder einem persönlichen Microsoft-Konto an.
- Wenn Ihr Konto Ihnen Zugriff auf mehr als einen Mandanten gewährt, wählen Sie Ihr Konto in der oberen rechten Ecke aus und legen Sie Ihre Portalsitzung auf den gewünschten Azure AD-Mandanten fest.
- Wählen Sie im linken Navigationsbereich den Azure Active Directory-Dienst (`Azure Active Directory service`) aus und wählen Sie dann App-Registrierungen (`App registrations`) → Neue Registrierung (`New registration`).



Einzelmandanten und Multimandanten im Kontotyp

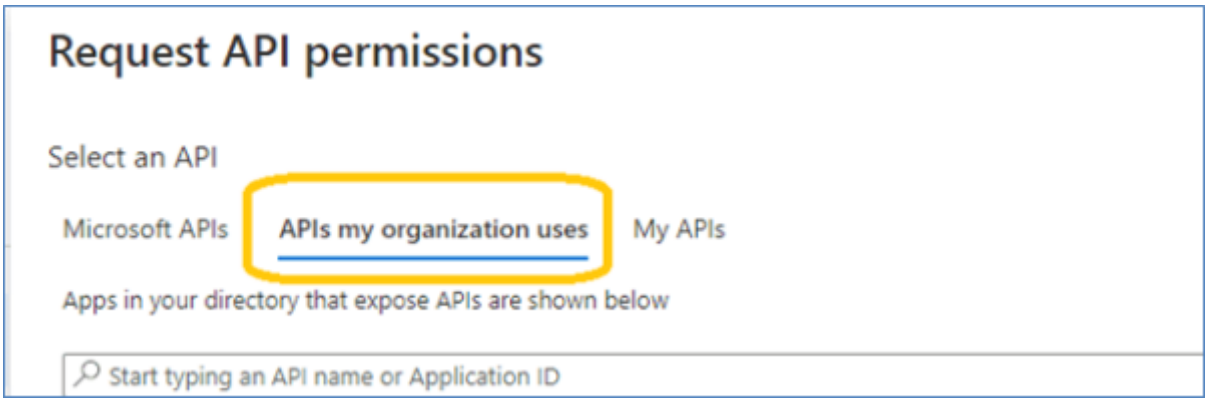
Wenn die Seite zur Registrierung einer Anwendung erscheint, geben Sie einen aussagekräftigen Anwendungsnamen ein und wählen den Kontotyp aus. Hier erscheint eine Auswahl, welche Konten Sie mit Ihrer Anwendung unterstützen möchten.

- Wählen Sie bitte den Typ einzelner Mandant (`single tenant`).

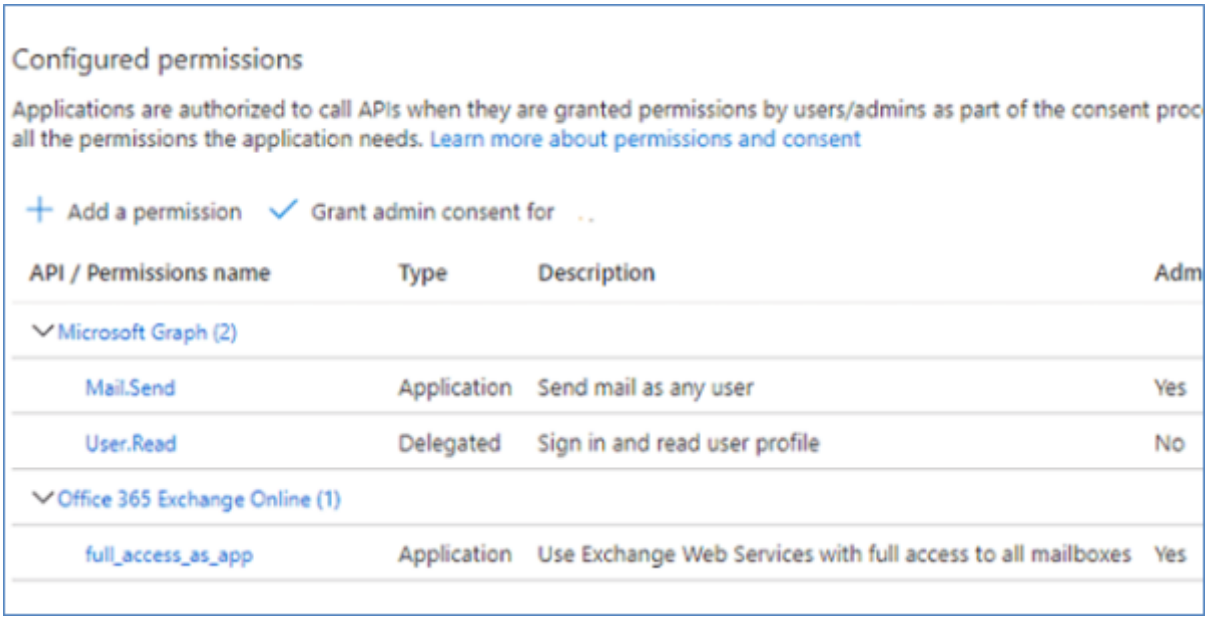
Da wir nur Office365-Benutzer in unserer Organisation unterstützen müssen, wählen Sie bitte nur Konten in diesem Organisationsverzeichnis (`single tenant`). Wählen Sie nicht die Unterstützung von persönlichen Microsoft-Konten aus, da es keine Möglichkeit gibt, auf persönliche Microsoft-Konten im Hintergrunddienst zuzugreifen.

API-Berechtigungen

- Klicken Sie auf Berechtigung hinzufügen (`API Permission`) → `Microsoft Graph` → Delegierte Berechtigung (`Delegated Permission`) → `User.Read`.
- Klicken Sie auf Berechtigung hinzufügen (`API Permission`) → `Microsoft Graph` → Anwendungsberechtigung (`Application Permission`) → `Mail.Send`
- Klicken Sie auf Berechtigung hinzufügen (`API Permission`) → Eine Berechtigung hinzufügen (`Add a permission`) → Von meiner Organisation verwendeten APIs (`APIs in my organization`) → Office 365 Exchange Online → Anwendungsberechtigung (`Aplication Permission`) → Andere Berechtigung (`Other permission`) → `full_access_as_app`



Im Folgenden sehen Sie die Liste der Berechtigungen:



API-Berechtigung manuell hinzufügen

Falls Ihr aktueller Benutzer kein Benutzer in einer verifizierten Domäne oder Office 365 ist, finden Sie Office 365 Exchange Online nicht in der API-Liste. Dann müssen Sie diese API-Berechtigung manuell hinzufügen. Dieser Vorgang ist nicht nötig, sollten Sie zuvor die entsprechende Einstellung gefunden haben.

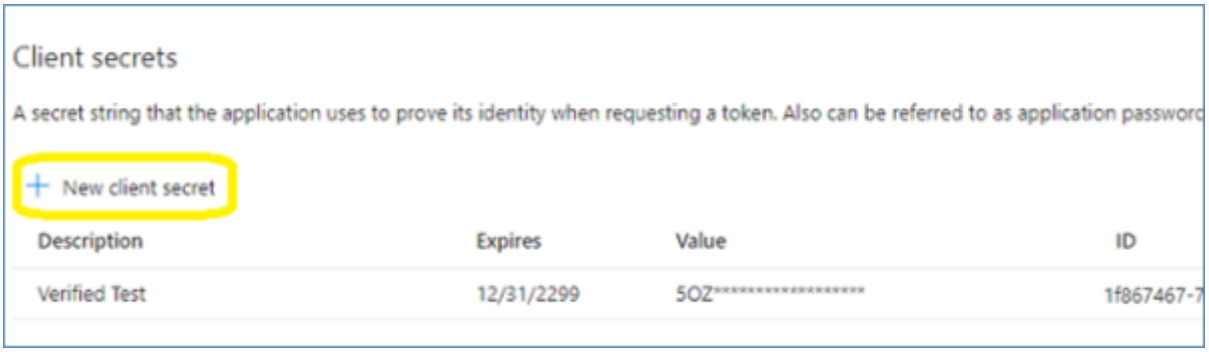
- Wählen Sie `Manifest` in der linken Navigation unter Verwalten (`Manage`).
- Suchen Sie im Manifest die Eigenschaft `requiredResourceAccess` und fügen Sie innerhalb der eckigen Klammern ([]) Folgendes hinzu:

```
{
 "resourceAppId": "00000002-0000-0ff1-ce00-000000000000",
 "resourceAccess": [
    {
       "id": "dc890d15-9560-4a4c-9b7f-a736ec74ec40",
       "type": "Role"
    }
  ]
}
```

- Wählen Sie Speichern (`Save`).
- Wählen Sie unter Verwalten (`Manage`) die API-Berechtigungen (`API Permissions`). Stellen Sie sicher, dass die Berechtigung `full_access_as_app` aufgeführt ist.

Client-Id und Client Secrets

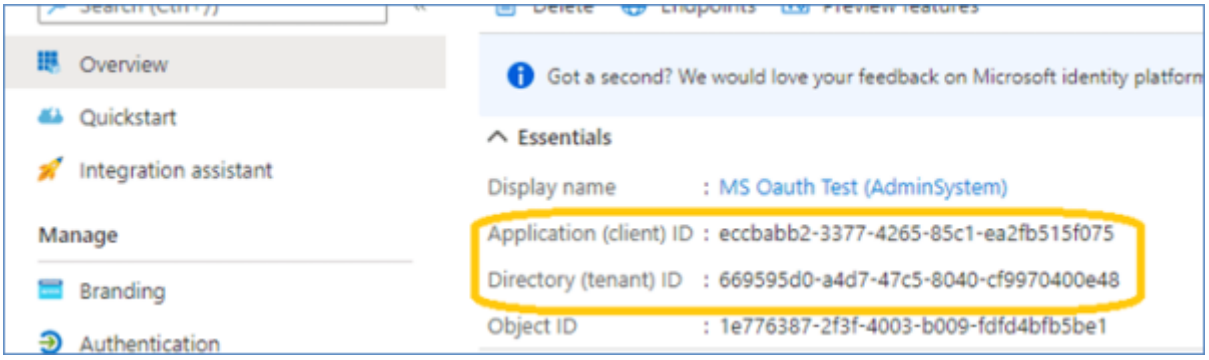
Nun erstellen Sie einen neuen geheimen Clientschlüssel für die Anwendung. Klicken Sie auf Zertifikate und Geheimnisse (`Certificates and Secrets`) → Geheime Clientschlüssel (`Client secrets`) und fügen Sie einen neuen geheimen Clientschlüssel hinzu.



Nachdem der Schlüssel erstellt wurde, speichern Sie den Wert des Geheimnisses an einem sicheren Ort. Bitte speichern Sie den Wert des Kundengeheimnisses selbst, da er bei der nächsten Anzeige nicht mehr sichtbar ist.

Anwendungs- und Verzeichnis-ID

Jetzt können Sie auf Übersicht klicken, um Ihre Anwendungs-ID (Client) und Ihre Verzeichnis-ID (Mandant) zu finden.



Admin-Zustimmung erteilen

Um Ihre Anwendung für den Zugriff auf Benutzerpostfächer in der Office365-Domäne zu verwenden, müssen Sie die Zustimmung des Office365-Domänenadministrators einholen.

- Wenn Sie die Anwendung erstellt haben und der Office365-Administrator sind:
  Klicken Sie unter API-Berechtigung (`API Permission`) auf den Schalter Administratorzustimmung für … erteilen (`Click grant admin consent for …`), um der Anwendung Berechtigungen zu vergeben.
- Wenn Sie die Anwendung erstellt haben und nicht der Office365-Administrator sind:
  Senden Sie den Link an den Office365-Administrator. Bitte ändern Sie die client_id in Ihre Anwendungs-ID:

`https://login.microsoftonline.com/common/adminconsent?client_id=8f54719b-4070-41ae-91ad-f48e3c793c5f&state=12345&redirect_uri=https://login.microsoftonline.com/common/oauth2/nativeclient`

- Der Administrator kann den obigen Link im Webbrowser öffnen. Wenn der Administrator mit den für die Anwendung erforderlichen Berechtigungen einverstanden ist, erteilen Sie die Zustimmung. Wenn nicht, klicken Sie auf Abbrechen (`Cancel`) oder schließen Sie das Fenster.
- Der Administrator kann die Berechtigungen ändern/aufheben, indem er sich am Azure-Portal anmeldet. → `Azure Active Directory` und dann Unternehmensanwendungen (`Enterprise applications`) auswählt.

- Nachdem der Administrator seine Zustimmung erteilt hat, wird der Webbrowser auf die folgende URL umgeleitet und sendet den Mandantenwert an den Anwendungsentwickler. https://login.microsoftonline.com/common/oauth2/nativeclient?admin_consent=True&tenant=79a42c6f-5a9a-439b-a2ca-7aa1b0ed9776&state=12345

Nachdem der Administrator die Berechtigungen genehmigt hat, können Sie Ihre Anwendung verwenden, um auf die Mailbox eines beliebigen Benutzers in der Office365-Domäne zuzugreifen.

Aktivieren von starken Verschlüsselungsalgorithmen in .NET 2.0 und .NET 4.0

Aktivieren Sie TLS Strong Encryption Algorithms in .NET 2.0 und .NET 4.0, da für die Funktionalität HttpWebRequest verwendet wird, um die Zugriffstokens vom Webdienst zu erhalten. Wenn Sie ein älteres .NET-Framework (.NET 2.0 und .NET 4.0) verwenden, müssen Sie starke Verschlüsselungsalgorithmen aktivieren, um Zugriffstoken anzufordern.



Es mag hierbei zu einer Einschränkung anderer Dienste kommen, welche auf ältere Sicherheitseinstellungen basieren. Der Impact sollte vorher kontrolliert und abgewogen werden. Die CREM-SOLUTIONS haftet für keine Folgefehler durch diese Anpassung.

- Fügen Sie den folgenden Inhalt in eine Datei namens `NetStrongEncrypt.reg` ein, klicken Sie mit der rechten Maustaste auf diese Datei → Zusammenführen (`Merge`) → Ja (`yes`).

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v2.0.50727]
"SystemDefaultTlsVersions"=dword:00000001
"SchUseStrongCrypto"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v2.0.50727]
"SystemDefaultTlsVersions"=dword:00000001
"SchUseStrongCrypto"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]
"SystemDefaultTlsVersions"=dword:00000001
"SchUseStrongCrypto"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319]
"SystemDefaultTlsVersions"=dword:00000001
"SchUseStrongCrypto"=dword:00000001
```

Es wird empfohlen, diese Anpassung auf allen Rechner anzuwenden, welche iX-Haus-Plus nutzen. Hierfür bietet sich eine Verteilung per Gruppenrichtlinie oder anderweitiges Softwareverteilungstool an. Erstellen Sie hierfür ein neues Gruppenrichtlinienobjekt auf Ihrem Domaincontroller und weisen Sie die korrekten Benutzergruppe hinzu. In der Bearbeitung des Gruppenrichtlinienobjekts finden sich die Einstellung hierfür unter Benutzerkonfiguration – Einstellungen – Windowseinstellungen – Registrierung vor. Hier können Sie bei Anlage eines neuen Eintrags entweder ein neues Registrierungselement erstellen oder der Registrierungs-Assistent starten, sollten die Anpassung bereits auf einem Rechner existieren. Nach dieser Anpassung sollten für die ausgewählten Rechner beim nächsten Login die Einstellungen automatisch übernommen werden.

Englische Originalfassung

Sie finden die vorstehenden Erläuterungen auch in der englischen Originalfassung auf der Website von https://www.emailarchtitect.net. Wir haben hier Auszüge aus https://www.emailarchitect.net/eagetmail/sdk/html/object_oauth_ews_service.htm (ohne die Abschnitte „Branding and verify publisher“ und „Use EWS OAUTH 2.0 to retrieve email by impersonating user in Office365 domain“) sowie aus https://www.emailarchitect.net/easendmail/kb/tls.aspx?cat=1 (Enable and Use TLS 1.3 Protocol to Send Email on Windows 10 and Windows 11) den Unterabschnitt `Enable TLS Strong Encryption Algorithms in .NET 2.0 and .NET 4.0` genutzt.

SFTP-Einstellungen konfigurieren

Die SFTP-Einstellungen müssen nur dann vorgenommen werden, wenn Sie (nur in iX-Haus-Modulen, z. B. beim batchgesteuerten Serienimport oder für kundenspezifische Importprozesse) eine Anbindung mit SFTP-Server nutzen. Stimmen Sie dies bei Bedarf mit einem Consultant der CREM SOLUTIONS ab.

`SFTP-Server`	Adresse des SFTP-Servers.
`Port`	Verwendeter Port am SFTP-Server.
`Benutzername`	Benutzername für die Anmeldung am SFTP-Server.
`Passwort`	Passwort für die Anmeldung am SFTP-Server. Das eingegebene Passwort wird mit Sternchen verdeckt dargestellt.
`SFTP-Verzeichnis`	Angabe des zu verwendenden Verzeichnisses auf dem SFTP-Server (Zielverzeichnis für Uploads auf den SFTP-Server/Quellverzeichnis für Downloads vom SFTP-Server).
`Lokales-Verzeichnis`	Angabe des zu verwendenden Verzeichnisses auf dem lokalen Server (Quellverzeichnis für Uploads auf den SFTP-Server/Zielverzeichnis für Downloads vom SFTP-Server).
`Originaldateien nach Download löschen`	[X] Originaldateien auf dem SFTP-Server werden nach dem Download in das lokale Verzeichnis gelöscht (Daten verschieben). [ ] Die Originaldateien bleiben erhalten (Kopieren auf den lokalen-Server).
`Originaldateien nach Upload löschen`	[X] Originaldateien im lokalen Verzeichnis werden nach dem Upload auf den SFTP-Server gelöscht (Daten verschieben). [ ] Die Originaldateien bleiben erhalten (Kopieren auf den SFTP-Server).
`SFTP-Verbindung testen`	Schaltfläche Die eingerichtete SFTP-Verbindung können Sie hierüber testen. Hierzu müssen (bis auf die beiden Checkboxen) alle Parameter definiert sein.

Register-Layout konfigurieren

Die Zähler in Registern sind standardmäßig deaktiviert, um die Performance beim Öffnen der Detailansichten zu steigern. Ein Benutzer mit Administratorrechten kann die Anzeige für alle Benutzer reaktivieren. Hierzu setzen Sie unter `Globale Einstellungen` im Register `Layout` den Schalter `Tabreiter Zähler bei allen Usern aktivieren` auf aktiv.

Sofern die Zähler nicht administrativ deaktiviert sind, kann jeder Benutzer diese individuell anzeigen oder ausblenden lassen. In den Benutzereinstellungen wählen Sie dazu die Option `Tabreiter Zähler aktivieren`.

Zusatzfelddefinitionen für Multimedia

Im Multimedia-Bereich können die Felder zur Beschreibung der Dokumente um bis zu fünf individuell definierbare Zusatzfelder erweitert werden. Standardmäßig sind die fünf Zusatzfelder deaktiviert. Diese Felder sind für alle Modulbereiche mit Multimedia in iX-Haus plus identisch. Die Konfiguration erfolgt unter Admin-Kennung. Der Admin legt im Bereich `Einstellungen` unter `Multimedia-Zusatzfelder` über die Zusatzfelderdefinition fest, welche Beschriftung und welchen Typ ein Zusatzfeld hat, ob es ein Pflichtfeld ist und ob es aktiviert oder deaktiviert sein soll.

Verfügbare Typen sind:

- Text
- Ganzzahl
- Fließkommazahl
- Betrag in €
- Checkbox
- Auswahlfeld (Für Auswahlfelder muss in dem nachfolgenden Engabefeld eine mit Semikolon getrennte Liste der zulässigen Auswahlen gepflegt werden. Ein Eintrag aus der Auswahl kann dann später zugeordnet werden. Eine spätere Änderung wird in vorhandenen Datensätzen nicht automatisch validiert.)

Möchten Sie diese individuellen Felder auch nach DocuWare übertragen, sprechen Sie bitte Ihren DocuWare-Consultant an.