One Button to Push (OBTP)

> Hierbei geht es um die Anbindung des Videoendpunktes an eine Groupware (z. B. Microsoft Exchange) um das Gerät per Groupware einzuladen. Wenn ein Videoendpunkt mit eingeladen wird, erscheint einige Minuten vor dem Meeting dieses auf dem Display des Endgeräts inklusive eines Button, um direkt dem Meeting beizutreten. Diese Funktion ist optional. Mit dieser Funktion ist es ebenfalls möglich an Microsoft Teams Meetings teilzunehmen. Allerdings benötigt dies eine zusätzliche Lizenz.

Microsoft Exchange Server (on Premise)

Schritt 1: Erstellung Raumressource

Stellen Sie sicher, dass jeder **physische Raum**, in dem sich ein **OBTP-Endpunkt** befindet, über eine zugehörige **Raumressource** mit einer **E-Mail-Adresse in Exchange** verfügt. Alternativ können Sie auch dem Videoendpunkt eine eigene Raumressource mit einer E-Mail-Adresse in Exchange erstellen.

Schritt 2: Konfiguration der Raumressource

Aktivieren Sie die **automatische Kalenderverarbeitung** (auto calendar processing) für jede **Raumressource**, so dass der Raum automatisch **Besprechungsanfragen annimmt**, wenn er verfügbar ist und automatisch eine **Einladung ablehnt**, wenn er bereits gebucht ist.

Kalenderoptionen anpassen

Um die von OBTP angebotene Funktionalität voll auszunutzen, empfehlen wir Ihnen, für die entsprechenden Raum Ressourcen die folgenden **Kalenderbearbeitungsoptionen** gegenüber dem **Standard** zu **ändern**:

Der Text der Besprechungseinladung wird standardmäßig gelöscht. Wenn Sie möchten, dass OBTP die Besprechungsdetails aus dem Textkörper analysiert, müssen Sie die Eigenschaft ***DeleteComments*** auf ***False*** setzen. Wenn Sie diese Eigenschaft auf True setzen, können nur Informationen verwendet werden, die sich in der Kalenderkopfzeilen befinden (da der Textkörper gelöscht wird).
Wenn eine Besprechungseinladung in einem Ressourcenpostfach eingeht, wird der Betreff der Besprechung standardmäßig gelöscht und durch den Namen des Organisators ersetzt.

Da OBTP auf die Besprechungseinladungen über die **Ressourcenpostfächer** zugreift, bedeutet dieses **Standardverhalten**, dass es keinen Zugriff auf den ursprünglichen Betreff hat. Sie können das Standardverhalten aus Datenschutzgründen beibehalten oder die Kalenderverarbeitungsoptionen für jedes Postfach so ändern, dass der Besprechungsbetreff verfügbar ist und somit auf den Endpunkten des Besprechungsraums angezeigt werden kann.

Das Kennzeichen **„Privat“** ist standardmäßig **deaktiviert**. Wenn Sie möchten, dass Besprechungen, die vom Organisator als privat gekennzeichnet sind, im Raumpostfach als privat gekennzeichnet bleiben, müssen Sie das Kennzeichen ***RemovePrivateProperty*** auf ***False*** setzen. Bei Raumressourcen, die mit **PowerShell-Befehlen** erstellt wurden, kann ***AutomateProcessing*** standardmäßig auf ***AutoUpdate*** gesetzt sein. In diesen Fällen sollte es in ***AutoAccept*** geändert werden.
Wenn der Besprechungsraum die **Einladung annimmt**, wird eine Antwort an den **ursprünglichen Anfrager** gesendet (einschließlich Anfrager außerhalb Ihrer Organisation, wenn Sie die Weiterleitung externer Einladungen zugelassen haben). Um Verwirrung darüber zu vermeiden, warum sie eine Antwort von einem Raum erhalten, der nicht in ihrer ursprünglichen Einladung enthalten war, können Sie zusätzlichen **Text konfigurieren**, der an den Anfrager gesendet wird, indem Sie das Flag ***-AddAdditionalResponse*** und die Einstellung -AdditionalResponse verwenden.

Wenn Sie es Benutzern ermöglichen möchten, Einladungen von anderen Organisationen an Ihre OBTP-Raumressourcen weiterzuleiten, müssen Sie das Kennzeichen ***ProcessExternalMeetingMessages*** auf ***True*** setzen.
-> Dies ist erforderlich, da Sie Microsoft Teams-Einladungen von externen Organisationen erhalten und diese Einladungen an Ihre OBTP-Raumressourcen weiterleiten möchten.

> **Powershell command:**
> Set-CalendarProcessing -Identity <resource_email> -DeleteComments $False -DeleteSubject $False -AddOrganizerToSubject $False -RemovePrivateProperty $False -AutomateProcessing "AutoAccept" -AddAdditionalResponse $true -ProcessExternalMeetingMessages $true -AdditionalResponse "Die Teilnehmer können von diesem Raum aus über Webmeeting OBTP an der Besprechung teilnehmen."

Schritt 3: Erstellen eines Dienstkontos in Exchange

In diesem Schritt erstellen Sie ein **Dienstkonto**, mit dem Sie sich bei Exchange anmelden, um auf die Kalender der Raumressourcen zuzugreifen, die für OBTP verwendet werden. Dieses **Servicekonto** sollte nur für OBTP verwendet werden. Sie können jedoch das gleiche Exchange-Servicekonto für **mehrere OBTP-Integrationen** verwenden.

Sie können ein neues **Dienstkonto** mit **PowerShell** wie folgt **erstellen**:

Mit dem **ersten Befehl** kann der Administrator ein **Kennwort** für das Dienstkonto als **sichere Zeichenfolge** eingeben. Diese Passwortvariable wird dann im **zweiten Befehl** verwendet, um ein **Postfach** für das Servicekonto zu **erstellen**. Der **dritte Befehl** stellt sicher, dass das **Kennwort** des Dienstkontos **nicht abläuft**.

> **Powershell command:**
> $Passwort = Read-Host „Passwort eingeben“ -AsSecureString
> New-Mailbox -Name „<Kontoname>“ -UserPrincipalName „<UPN>“ -Passwort $password -Alias „<Kontoname Alias>“ -FirstName „<Kontovorname>“ -LastName „<Kontonachname>“ -DisplayName „<Kontoname>“
> Set-ADUser -Identity „<UPN>“ -PasswordNeverExpires $true

> **Beispiel:**
> New-Mailbox -Name „Webmeeting OBTP Service Account“ -UserPrincipalName webmeeting-obtp-svc@domain.com -Password $password -Alias webmeeting-obtp-svc -FirstName „webmeeting OBTP“ -LastName „Service Account“ -DisplayName „webmeeting OBTP Service Account“
> Set-ADUser -Identity webmeeting-obtp-svc@domain.com -PasswordNeverExpires $true

Schritt 4: Konfigurieren der Anwendungs-Impersonation (Impersonation) auf dem Dienstkonto

In diesem Schritt **erstellen** Sie eine neue **Verteilergruppe** und fügen die Räume, die für OBTP verwendet werden sollen, der **Gruppe** hinzu. Anschließend stellen Sie mit PowerShell-Befehlen sicher, dass das Dienstkonto nur die Mitglieder dieser Gruppe impersonieren kann.
Die Konfiguration der **Anwendungs-Impersonation** auf diese Weise bedeutet, dass, wenn **Räume** zur Gruppe **hinzugefügt** oder aus ihr **entfernt** werden, **automatisch aktualisiert** wird, ob das Dienstkonto sie impersonieren kann oder nicht.

Erstellen einer neuen Verteilergruppe

Melden Sie sich in Ihrem Exchange Admin Center als Administrator an und gehen Sie zu **Empfänger -> Gruppen**.
Wählen Sie das **+-Symbol** und wählen Sie **"eine neue Verteilergruppe hinzufügen"**.
Fügen Sie die Räume, die Sie impersonieren möchten, der Gruppe hinzu.
Beachten Sie, dass das Dienstkonto nicht als Mitglied dieser Verteilergruppe hinzugefügt werden sollte. Stattdessen erlaubt dieser Schritt dem Dienstkonto, jedes Mitglied dieser Verteilergruppe zu impersonieren (d.h. jede der Raumressourcen).
Stellen Sie sicher, dass Sie die Option, den **Gruppenbesitzer zum Gruppenmitglied** zu machen, **deaktivieren**. Andernfalls kann sich das Dienstkonto als Ihr Konto ausgeben.
Vergewissern Sie sich auch, dass Sie die **Gruppe sperren**, damit sich niemand versehentlich als

Gruppenmitglied hinzufügen kann. Wählen Sie dazu **"Geschlossen: Mitglieder können nur von den Gruppeneigentümern hinzugefügt oder entfernt werden."**
Wir empfehlen, dass Sie kombinierte PowerShell-Befehle verwenden, um die Anwendungsvertretung für das Dienstkonto zu konfigurieren. Auf diese Weise können Sie **Variablen** verwenden und so mögliche **Fehler** beim **Kopieren** und **Einfügen** reduzieren.
Konfigurieren Sie die folgenden Variablen mit den Werten, die Sie tatsächlich verwenden wollen:

otj_group_id: die E-Mail-Adresse der Verteilerliste, deren Mitglieder Sie impersonieren möchten.
otj_service_account: die E-Mail-Adresse des Dienstkontos, dem Sie die Impersonation gewähren wollen.
management_scope_to_create: der Name, den der neu erstellte Verwaltungsbereich haben soll.
impersonation_role_name_to_create: Der Name, den die neu erstellte Impersonation-Rolle haben soll.

Zum Beispiel:
$obtp_group_id = „obtprooms@domain.com“
$obtp_service_account = „webmeeting-obtp-svc@domain.com“
$management_scope_to_create = „OBTP Verwaltungsbereich“
$impersonation_role_name_to_create = „OBTP Impersonation“
Erstellen Sie den Verwaltungsbereich:
$obtp_group = Get-DistributionGroup -Identity $obtp_group_id
$obtp_group_dn = $obtp_group.DistinguishedName
$restriction_filter = „MemberOfGroup -eq ‚“$obtp_group_dn“"“
New-ManagementScope -Name $management_scope_to_create -RecipientRestrictionFilter $restriction_filter

Beispiel für die Ausgabe:
Name ScopeRestrictionType Exclusive RecipientRoot RecipientFilter
---
obtp Management Scope RecipientScope False MemberOfGroup -eq 'CN=obtp Rooms2111430164340,OU...
Richten Sie die Anwendungsimpersonation unter Verwendung des zuvor erstellten Verwaltungsbereichs ein:
New-ManagementRoleAssignment -Name $impersonation_role_name_to_create -Role ApplicationImpersonation -User $obtp_service_account -CustomRecipientWriteScope $management_scope_to_create

Beispiel für die Ausgabe:
Name Rolle RoleAssigneeName RoleAssigneeType AssignmentMethod EffectiveUserName
---

> obtp Impersonation ApplicationImp... webmeeting-obtp-svc User Direct

Überprüfen Sie, ob die oben genannten Befehle wie erwartet funktionieren. Ersetzen Sie im folgenden Befehl ***<resource_email>*** durch die E-Mail der **Mailbox** der Raumressource, die Sie **testen** möchten. Wenn es sich um einen Raum handelt, der Mitglied der **Verteilerliste** ist, sollte er die **OBTP-Impersonation** in den zurückgegebenen Rollen anzeigen. Wenn es sich um einen **anderen Raum außerhalb der Verteilerliste** handelt, sollte die OBTP-Impersonation nicht aufgeführt sein, was bedeutet, dass das **OBTP-Servicekonto keine Berechtigung** hat, diesen Benutzer zu **impersonieren**.

> Get-ManagementRoleAssignment -Role ApplicationImpersonation -WritableRecipient "<resource_email>" | Format-List Name, Role, RoleAssignee, CustomRecipientWriteScope

> **Beispiel für die Ausgabe:**
> Name: OBTP Impersonation
> Role: ApplicationImpersonation
> RoleAssignee: webmeeting-obtp-svc

Schritt 5: Firewall-Einstellungen

Die webmeeting Server in unseren Rechenzentren benötigen Zugriff auf den Exchange Server EWS Dienst. Dafür müssen folgende Freischaltungen eingerichtet werden:

Quelle Name	Quelle IP-Adresse	Ziel	Port
ntcxdc1pxp01.netconnexhost.local	192.168.12.160	Exchange EWS	https (tcp/443)
ntcxdc1pxp02.netconnexhost.local	192.168.12.161	Exchange EWS	https (tcp/443)
ntcxdc2pxp02.netconnexhost.local	192.168.12.162	Exchange EWS	https (tcp/443)
ntcxdc1pxp03.netconnexhost.local	192.168.12.163	Exchange EWS	https (tcp/443)
ntcxdc2pxp03.netconnexhost.local	192.168.12.164	Exchange EWS	https (tcp/443)
ntcxdc1pxp05.webmeeting.eu	192.168.12.167	Exchange EWS	https (tcp/443)
ntcxdc2pxp05.webmeeting.eu	192.168.12.168	Exchange EWS	https (tcp/443)

Die webmeeting Server in unseren Rechenzentren benötigen ebenfalls Zugriff auf die Videoendpunkte um die entsprechenden Informationen zu den Meeting-Details zu senden. Dafür müssen folgende Freischaltungen eingerichtet werden:

Quelle Name	Quelle IP-Adresse	Ziel	Port
ntcxdc1pxp01.netconnexhost.local	192.168.12.160	Videoendpunkte	https (tcp/443)
ntcxdc1pxp02.netconnexhost.local	192.168.12.161	Videoendpunkte	https (tcp/443)
ntcxdc2pxp02.netconnexhost.local	192.168.12.162	Videoendpunkte	https (tcp/443)
ntcxdc1pxp03.netconnexhost.local	192.168.12.163	Videoendpunkte	https (tcp/443)
ntcxdc2pxp03.netconnexhost.local	192.168.12.164	Videoendpunkte	https (tcp/443)
ntcxdc1pxp05.webmeeting.eu	192.168.12.167	Videoendpunkte	https (tcp/443)
ntcxdc2pxp05.webmeeting.eu	192.168.12.168	Videoendpunkte	https (tcp/443)

Revision #12
Created 3 January 2025 10:02:46 by Peter Großmann
Updated 16 January 2025 11:50:55 by Lukas Haag