

# Integration of Microsoft Azure



## Contents

1. Introduction .....	2
2. Methods of Integration.....	2
3. Configure Azure as Resource Owner Password Credentials (ROPC) .....	2
3.1 Create and configure the Azure Application.....	3
3.2 Connecting with DoubleClue Enterprise Management (DCEM).....	5
3.3 Importing Azure Users to DoubleClue .....	5
4. Configure Azure as a Service Provider Hybrid with Active Directory .....	6
4.1 Creating a federated Azure Domain .....	6
4.2 Configuring DoubleClue for Azure .....	6
4.3 Exporting the DoubleClue metadata .....	7
4.4 Configuring the Azure Domain Federation with Powershell .....	7
4.5 Users in federated Domain .....	9
4.6 Verify Access to Office online .....	10
5. Configure Azure as a Service for DoubleClue .....	10

## 1. Introduction

This documentation describes how to integrate Microsoft Azure with DoubleClue Identity & Access Management (IAM).

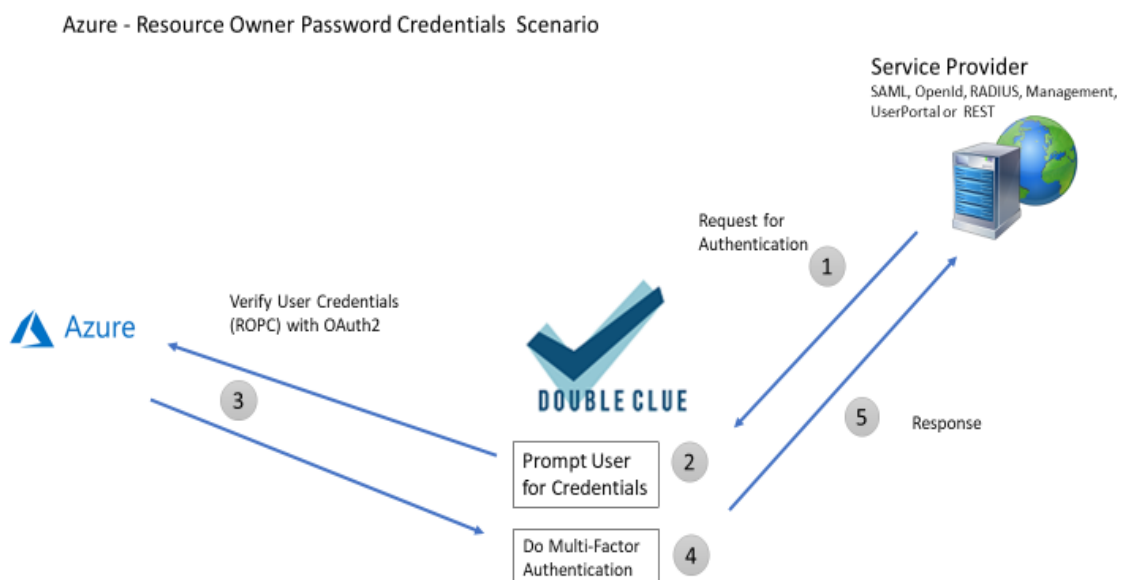
## 2. Methods of Integration

There are three different scenarios to integrate Microsoft Azure with DoubleClue:

- Azure as Resource Owner Password Credentials (ROPC)
- Azure as a Service Provider Hybrid with Active Directory
- Azure as a Server Provider for DoubleClue

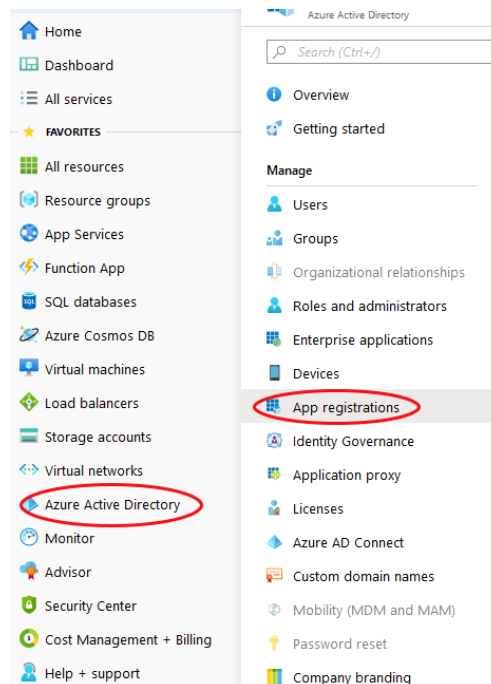
## 3. Configure Azure as Resource Owner Password Credentials (ROPC)

In this scenario, Azure verifies the user credentials for other service providers. To utilize DoubleClue Multi-Factor Authentication (MFA), all Azure users have to be imported into DoubleClue by the administrator or by the users themselves using the DoubleClue UserPortal.



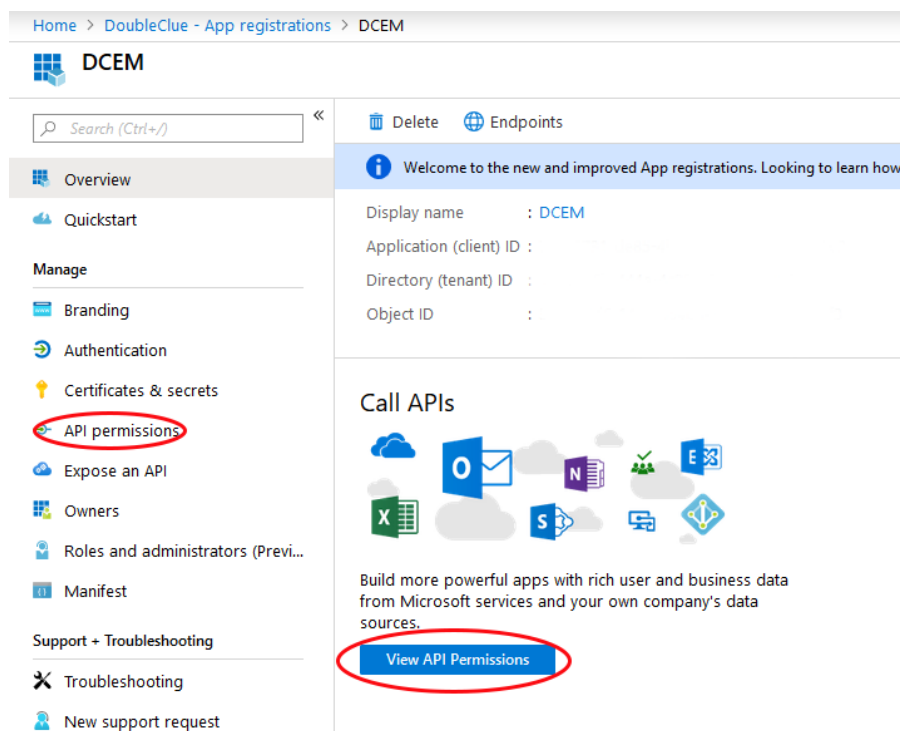
### 3.1 Create and configure the Azure Application

1. Log into your Global Administrator account on <https://portal.azure.com>
2. Go to “Azure Active Directory” and choose “App Registrations” in the submenu.



3. Click on “New Registration”. If you have already registered an app you wish to use, select it instead and skip directly to step 5.
4. Give your application an easily recognisable name, eg. “DoubleClue”. Then choose the account type you want to support and click “Register”.
5. Copy the “Application (client) ID” and “Directory (tenant) ID” from the application side. Store them in a safe location – you will need them later.

- Click on “View API Permissions” or “API Permissions” from the submenu on the left side of the app registration page.

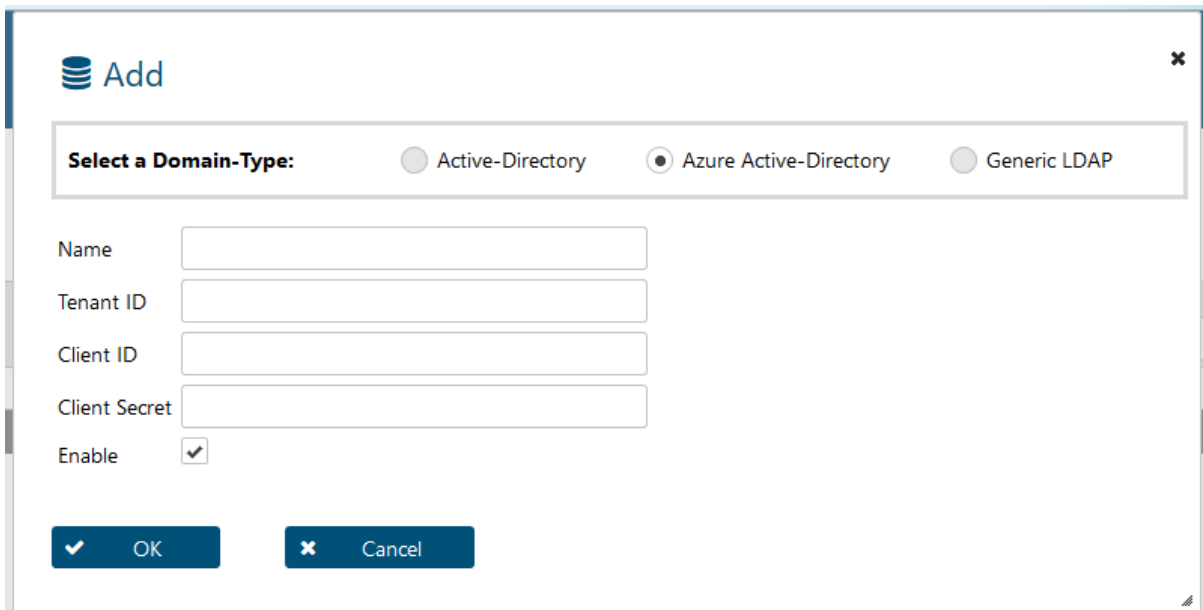


The screenshot shows the Azure portal interface for an application registration. The breadcrumb path is 'Home > DoubleClue - App registrations > DCEM'. The left sidebar contains a navigation menu with 'API permissions' highlighted with a red circle. The main content area displays the application details for 'DCEM' and a 'Call APIs' section with a 'View API Permissions' button also circled in red.

- Choose “Add a permission” and select “Microsoft Graph” then “Application permissions”. This will open the menu to select permissions.
- Open the menu item “Directory” and enable “Directory.Read.All”. Then open the item “Users” and enable “User.Read.All”. Confirm the selection with the “Add Permission”-Button at the bottom of the menu.
- Choose “Add a permission” again and select “Microsoft Graph” then “Delegated permissions”. Open the item “Users” and enable “User.Read.All”. Confirm the selection with the “Add Permission”-Button at the bottom of the menu.
- Make sure to grant Admin consent to all permissions.
- Go to “Certificates & Secrets” in the submenu on the left.
- Add a “New Client Secret” and choose an expiration time.
- Copy the value of the client secret. Be aware that the secret is only shown once! Should it be lost, it can’t be restored and a new secret has to be defined.

## 3.2 Connecting with DoubleClue Enterprise Management (DCEM)

1. Log into DCEM as an administrator.
2. Go to “Administration” in the main menu and then to “Domain” in the sub menu.
3. Add a new Domain.
4. Choose “Azure Active-Directory” as Domain-Type.

A screenshot of a web application dialog box titled "Add". At the top left is a blue icon of three stacked cylinders followed by the text "Add". At the top right is a close button (an 'x' in a square). Below the title bar is a section labeled "Select a Domain-Type:" with three radio button options: "Active-Directory", "Azure Active-Directory" (which is selected), and "Generic LDAP". Below this are four text input fields labeled "Name", "Tenant ID", "Client ID", and "Client Secret". Below the input fields is an "Enable" checkbox which is checked. At the bottom are two buttons: "OK" with a checkmark icon and "Cancel" with an 'x' icon.

5. Select a meaningful and easily memorable name, like the company name. Note that this name will be the prefix users will need to add to their User ID to identify themselves with DoubleClue.
6. Paste the Tenant ID and Client ID from the value you copied in step 3.1.5 in the respective fields.
7. Paste in the Client Secret from the value you copied in step 3.1.12 in the respective field.
8. Confirm the input. You now have a successfully connected your DCEM to the Azure app.

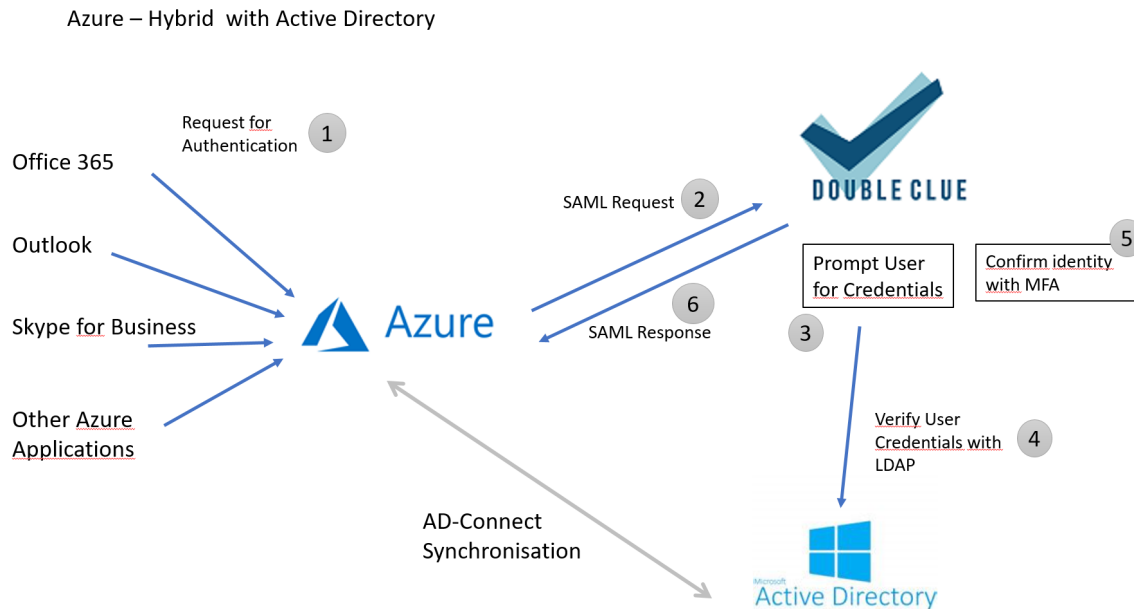
## 3.3 Importing Azure Users to DoubleClue

Azure users must be imported into DoubleClue and register a device in order to use the DoubleClue MFA.

Users can register themselves and their MFA devices in DoubleClue by using the DoubleClue User-Portal. Alternatively, the DoubleClue Administrator can import and activate user devices in bulk mode.

## 4. Configure Azure as a Service Provider Hybrid with Active Directory

In this scenario, Azure acts as a SAML Service Provider and DoubleClue as the SAML Identity Provider.



The federation uses the SAML protocol for the communication between Azure and DoubleClue. Both parties have first to trust each other by exchanging the SAML metadata before establishing the federation.

### 4.1 Creating a federated Azure Domain

- The primary domain “tenant.onmicrosoft.com” cannot be configured for federation. You first need to create a new domain for federation.
- The domain must be configured to Azure AD-Connect Sync with the on premises Active Directory.
- Once a domain is federated, the users have to be synchronized with Active Directory or other Identity Providers. You cannot add users or reset user passwords once the domain has been federated.

### 4.2 Configuring DoubleClue for Azure

DoubleClue comes with a preconfigured Azure metadata. To use it, follow the steps below:

1. Log into DCEM
2. In the main menu, navigate to “SAML” and open the sub menu “Service Providers”
3. Add a new Service Provider and select SP Configuration “Microsoft Azure”

4. Confirm and save the news service provider

### 4.3 Exporting the DoubleClue metadata

Azure does not support the SAML standard metadata format. To establish a federation, you therefore require the following data from DoubleClue:

- Logon URL
- Entity ID
- Certificate

#### Logon-URL

The host name of the Logon-URL is configured in DCEM. In the main menu, navigate to “SAML” and here to “Preferences”. The host URL is defined in the field “SSO Domain” field, for example:

<https://example-url.example-company.com>. The Login URL is composed of the “SSO Domain” and the suffix “dcm/saml”. In our example, the login URL would be <https://example-url.example-company.com/dcm/saml>.

#### Entity ID

The Entity ID is also configured in the “Preferences” under “SAML”. It is defined in the field “IdP Entity ID”.

#### Certificate

You can download the certificate in DCEM under “SAML” -> “Service Providers”. Click on “Download Idp Metadata” and choose “Download Certificate”.

### 4.4 Configuring the Azure Domain Federation with Powershell

The Azure Domain federation is configured with Power Shell commands. To use the Windows PowerShell cmdlets, you must first download the [Azure Active Directory Modules](#).

- 1) Connect to your Azure AD Directory as a tenant administrator with:  
**Connect-MsolService**
- 2) Now use **Set-MsolDomainAuthentication** to federate the azure Domain. Use the following sample with the data you exported from DoubleClue as described in chapter 4.3:

```
$dom = "your.azure.domain.name"
$BrandName = "DoubleClue SAML 2.0 IDP"
$LogOnUrl = https://example-url.example-company.com/dcem/saml
$LogOffUrl = https://example-url.example-company.com/dcem/saml
$EntityId = "example-url.example-company.de"
$MySigningCert = @"
MIIC7jCCAdagAwIBAgIQRrjsbFPaXIIOG3GTv50fkjANBgkqhkiG9w0BAQsFADAzMTEwYDQVQD
EyhBREZTIFNpZ25pbmVzLSB4UzlwMTJSMi0wLnN3aW5mb3JtZXluY29tMB4XDTE0MDEyMDE1M
TY0MFoXDTExMDEyMDE1MTY0MFowMzExMC8GA1UEAxMoQURGUyBTaWduaW5nIC0gV1My
MDEyUjltMC5zd2luZm9ybWVvYmNvbTCCAS1wDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBA
Ke+rLVmXy1QwCwZwqgbbp1/kupQVcjKuKLitVDbsFyqbDTjp7WRjIVMWAHBI3kgNT7oE362Gf2
WMJFf1b0HcrsLin7daRXpq4Qi6OA57sW1YFMj3sqqyTP0eZV3S4+ZbDVob6amsZldlwxalp9Zfyw
g2bLsGnVldB0+XKedZwDbCLCVg+3ZWxd9T/jV0hpLIWw+LCOHqq8n8beJvlivgLmDJo8f+EITnAxW
csJUvVai/35AhHCUq9tc9sqMp5PWtabAEmb2AU72/QIX/72D2/NbGQq1BWYbqUpgpCZ2nSgvlW
DHCiUo//UGsvfox01kjTFlmqQInsJVfRxF5AcCAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAI8c6C4z
aTEc7aQiUgvnGQgCbMZbhUXXLGRpvFLKaQzka9eq7WLjibcSNyGXBa/SfT5wJgsm3TPKgSehGA
OTirhcqHheZyvBObAScY7GOT+u9pVYp6raFrc7ez3c+CGHeV/tNvy1hJNs12FYH4X+ZCNFIT9tprieR
25NCdi5SWUbPZL0tVzJsHc1y92b2M2FxdDohxOgJvyJOpcg2mSBzZZIkvDg7gfPSUXHVS1MQs0R
HSbwq/XdQocUUhl9/e/YWCbNNxlM84BxFsBUok1dH/gzBySx+Fc8zYi7cOq9yaBT3RLT6cGmFGVY
ZJW4FyhPZOCLVNsLnPQcX3dDg9A=="

Set-MsolDomainAuthentication
-DomainName $dom
-FederationBrandName $dom
-Authentication Federated
-PassiveLogOnUri $LogOnUrl
-LogOffUri $LogOffUrl
-SigningCertificate $MySigningCert
-IssuerUri $EntityId
-PreferredAuthenticationProtocol "SAML"

```

\$MySigningCert is the certificate you downloaded from “Exporting the DoubleClue metadata”  
\$LogOnUrl, \$LogOffUrl and \$EntityId are the Logon URL and EntityId from “Exporting the DoubleClue metadata”

- 3) To check the configuration, you can execute  
***“Get-MsolDomainFederationSettings -domainname mydomain.com | format-list -Property \**”**



Microsoft references:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-fed-saml-idp#configuring-a-domain-in-your-azure-ad-directory-for-federation>

[https://docs.microsoft.com/en-us/previous-versions/azure/dn194112\(v=azure.100\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/azure/dn194112(v=azure.100)?redirectedfrom=MSDN)

#### Note

If you converted a domain, rather than adding one, it may take up to 24 hours to set up single sign-on. **Before you verify single sign-on, you should finish setting up Active Directory synchronization, synchronize your directories and activate your synced users.**

## 4.5 Users in federated Domain

Users in federated domain can be created by Azure Ad connect. For more detailed information, see [Integrate your on-premises directories with Azure Active Directory](#).

Windows PowerShell can also be used to automatically add new users to Azure AD and to synchronize changes from the on-premises directory.

The following procedure shows how to add a single user to Azure AD.

1. Connect to your Azure AD Directory as a tenant administrator: *Connect-MsolService*.
2. Create a new user principal:  
PowerShellCopy

#### New-MsolUser

```
-UserPrincipalName john.smith@example.com  
-ImmutableId ABCDEFG1234567890  
-DisplayName "John Smith"  
-FirstName John  
-LastName Smith  
-AlternateEmailAddresses "john.smith@something.com"  
-LicenseAssignment "samIp2test:ENTERPRISEPACK"  
-UsageLocation "DE"
```

For more information about “New-MsolUser”, see <https://technet.microsoft.com/library/dn194096.aspx>

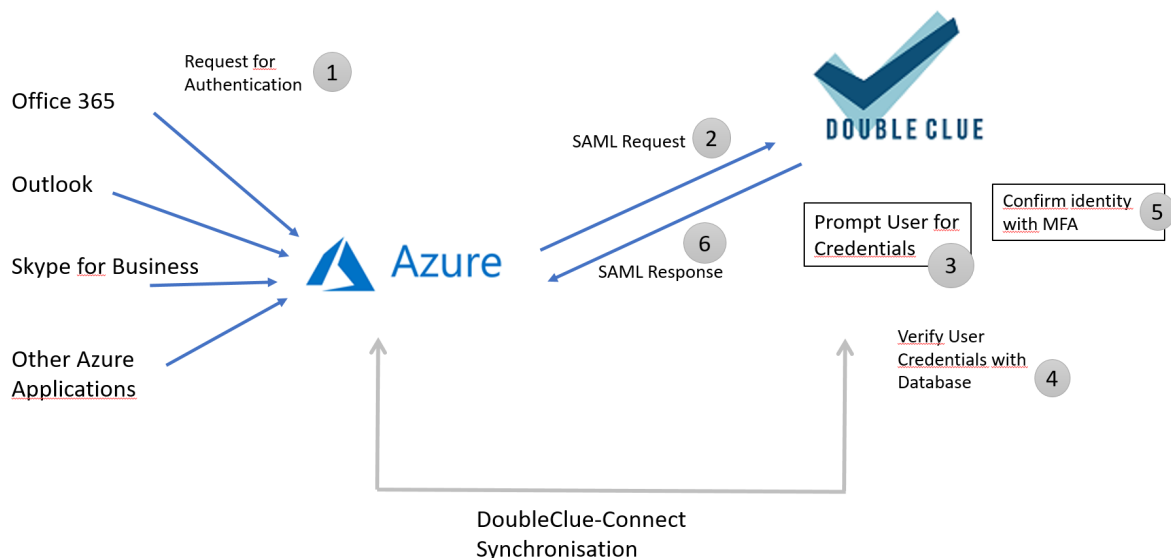
## 4.6 Verify Access to Office online

You can now log into office.com using DoubleClue as your Identity Provider.

- 1) Open your browser and enter <https://office.com>
- 2) As user name, enter the user principal name like [name.surname@your-domain-name](#)
- 3) As your domain is federated, Azure will redirect you to the DoubleClue login page.
- 4) After a successful DoubleClue authentication, you will be automatically redirected to Office.com as a login user.

## 5. Configure Azure as a Service for DoubleClue

Azure - Server Provider for DoubleClue



In this scenario, the Azure domain is a federated domain without synchronization with Active Directory. Azure acts as a SAML Service Provider.

The users are managed in DCEM and are automatically synchronized with the federated Azure domain.

To establish this scenario, you need first to set up the [Resource Owner Password Credentials \(ROPC\)](#) and then enable the Azure auto synchronization.