OFFICE365 HYBRID USER MANAGEMENT

The Nuvolex platform is a user management console that provides IT administrators with the ability to easily perform user administration and automate the user lifecycle for user identities in on premise Active Directory, as well as public cloud services like Microsoft Office365. Along with identity management are features focused around Exchange online user mailboxes, as well as Office365 license and attribute management.

What makes the Nuvolex platform unique is the capability to manage user identities that span across on premise Active Directory and public cloud services. This is achieved by utilizing the Nuvolex AD Agent that establishes communication between the Nuvolex SaaS platform and on premise Active Directory. The Nuvolex AD Agent writes back AD user and group changes directly into on premise AD. The Nuvolex AD Agent leverages Microsoft's Azure AD Connect to synchronize user and group updates from AD to Office365.

The Nuvolex AD Agent can be installed on any windows-based device joined to an AD domain. Once the Nuvolex AD Agent is deployed, communication between the Nuvolex platform and the Nuvolex AD Agent will initiate exclusively over HTTPS. When the Nuvolex AD Agent has connected to the Nuvolex platform, AD user and group data is imported and merged with users and groups imported from Office365 enabling seamless administration across on premise AD and Office365. Using this capability, you can manage any hybrid Office365 environment anywhere in the world from the cloud.

CHALLENGES MANAGING REMOTE AD ENVIRONMENTS

There are several challenges with managing Remote AD tenants that cause CSPs to increase their headcount, risk, and complexity with management. Customer concerns around direct network and AD access as well as scope of administrative controls make managing customer AD environments difficult and, in some cases not possible. With the commonly used implementation of Directory Synchronization in Office365, organizations of all sizes (even as little as 100 users) need to maintain and manage AD users and groups daily. The Nuvolex platforms hybrid management approach resolves many of these blockers helping Service Providers easily support and manage any number of On Premise AD environments while offering customers a unique way to control access to their network and AD environment.

A major customer concern with allowing a 3rd party service provider manage their AD environment is with network access. Typically, AD environments are locked down and unavailable to any traffic that is outside of the

corporate network. IT administrators will need to have VPN access to connect with an organizations local network where they can then manage AD users and groups. This direct network access by an outside entity raises issues with security and compliance since any number of unknown IT administrators have privileged access to an organization's corporate network. This concern can be remediated using the Nuvolex Remote AD management approach that utilizes a piece of software (Agent) that facilitates any interactions between the IT administrator managing AD users and groups on Nuvolex and the customers AD environment. Since the Agent is the communication point between the customer's network and the Service Provider's IT administrators, there is no need for IT administrators to have direct access to a customers AD environment. All AD management for users and groups is done on the Nuvolex platform. AD user and group changes are sent to the Agent which executes the action in the customers AD environment on behalf of the IT Administrator. Rather than using VPNs and logging in directly to a customers AD environment, IT administrators login to the Nuvolex platform to do their daily AD user identity management tasks and will **never** directly touch a customer's network.

Customers want control and have flexibility with what IT administrators have administrative access to. The Nuvolex remote AD management approach allows customers to fully control a service providers level of engagement with their AD environment. Customers can easily install the Nuvolex AD Agent on behalf of the service provider using an AD Admin account or service account that has delegated rights to OUs and AD actions by utilizing the built in AD delegation features. Having the customer to install the Nuvolex AD Agent on behalf of the service provider gives the customer the ability to use any domain joined device of their choosing while also ensuring that service provider IT administrators do not directly access the customers AD environment. The Nuvolex AD Agent uses any AD administrator user account or service account that can be delegated to one or many OUs and administrative actions as defined by the customer. This allows the customer to clearly define the scope of administrative access the Nuvolex AD Agent has and as a result limiting the exposure of the customer AD environment to service provider IT administrators. Nuvolex gives the customer total control over the AD administration performed by the service provider IT administrators helping build customer confidence and promoting flexibility while not getting in the way of IT administrators supporting users every day.

HOW IT WORKS

The Nuvolex platform aligns with a typical hybrid model where IT administrators manage cloud services and user identities that have been synchronized from on premise AD to a cloud service such as Office365. The common approach used by most cloud services is that on premise write back is not allowed since directory synchronizations only flow 1 way. This makes it so that all AD user and group changes must be performed in on premise AD and then synchronized outward to cloud services. The Nuvolex platform aims to close the gap between managing these distinct environments by offering a unified management approach to how users and cloud services are managed. To do this, Nuvolex uses an Active Directory Agent that is installed inside of an organizations corporate network. This Agent communicates exclusively with the Nuvolex platform to read and write AD user and group data. Anytime an IT Administrator resets an AD user password, adds users to an AD security group, or changes a AD user's OU assignment, a request is generated on the Nuvolex platform and is

sent to the corresponding Agent that resides in a customer's local network. The Agent receives this request and carries out the requested action by contacting a local Domain Controller (AD server) as selected during the Agent installation. Once the request has been fulfilled by the Agent, a confirmation message is sent back to the Nuvolex platform completing the AD update transaction.

Before you can manage a customer's hybrid Office365 tenant, you must start by onboarding the customer's Office365 tenant.

1. You can onboard tenants by going to the **Tenants tab**..
2. Click on **Add Tenant**
3. Select the option for **Add and Onboard Tenant**
    a. Enter the your Office365 tenant **Global Administrator** credentials so Nuvolex can authenticate and onboard your Office365 tenant.
4. Click **Submit** and start the onboard process

You will see that the onboard process will begin by looking at the **Progress panel** at the bottom left side of the screen. You can monitor the progress of your onboard from this panel. Onboarding an Office365 tenant varies in time depending on the number of users, groups and mailboxes that are present in your tenant. The average onboard for a tenant is 5-15 minutes, and this process will only need to be done once.

After the Office365 tenant has been onboarded, you will see users and groups that have been marked as "Synchronized" noting that the source of that user or group is on premise AD. The user or group cannot be updated or changed from Office365 . This is the point where the Nuvolex AD Agent is deployed so that these Synchronized user and groups can be easily managed from a single console. Before an Agent can be installed and linked to a Tenant on Nuvolex, there are several backend resources that need to be created so that the Nuvolex platform. The Nuvolex platform generates backend resources automatically and are used for communicating with the Nuvolex AD Agent that is installed in a customer on premise AD environment.

To create the Agent resources follow these steps:

1. Go to the **Tenants Tab** and select the tenant that you would like to integrate with Active Directory.
2. Click on the **Install Active Directory Agent** icon at the top right corner of the Tenants tab.
3. Enter a **Password** for the Nuvolex Active Directory Agent.
4. Download the Nuvolex Active Directory Agent installer from the Nuvolex platform
5. Copy the Nuvolex Active Directory Agent to a domain joined server or domain joined machine
    a. It is a **best practice** to install the Agent on the same machine that is running AAD Connect or DirSync
    b. You can install the Nuvolex Active Directory Agent on a Domain Controller if you wish
    c. You can install the Nuvolex Active Directory Agent on any highly available domain joined machine
6. Double click the Nuvolex Active Directory Agent EXE installer and follow the installation steps.
7. Once installed, go back to the Nuvolex platform and click the button for "Onboard Active Directory" or simply start a Full Synchronization of the tenant.

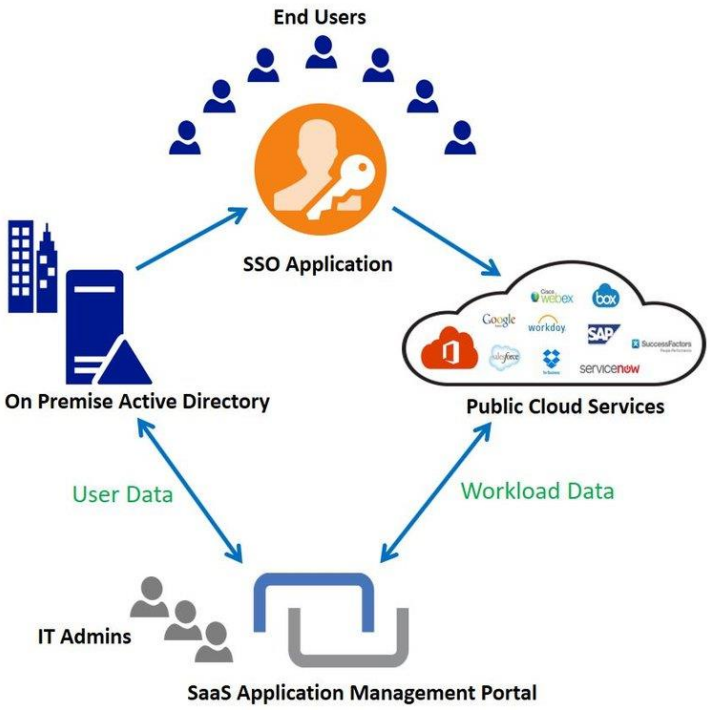
The AD onboarding process performs several of automated tasks that configures your hybrid tenant on the Nuvolex platform. One of the main tasks is merging user and group objects from Office365 with users and groups from on premise AD to create a unified hybrid user on the Nuvolex platform. A hybrid user on Nuvolex is comprised of multiple attributes that tie to AD and another set of attributes that are tied to Office365. To merge users, the Nuvolex platform looks for a consistent user principal name (UPN) that is shared between the

customers Office365 tenant and their AD environment. Using the UPN, the Nuvolex platform is able to identify users and group object relationships between Office365 and AD. The result is the IT administrator only sees a single user that contains attributes from both Office365 and AD, and these attributes can be updated and changed seamlessly across both environment without having to switch between consoles or needing additional access rights. Nuvolex maps attributes to their source so when a change is made, Nuvolex automatically sends the update request to the correct environment. Once this and other background processes are completed, your hybrid tenant is setup and ready to be managed!

USAGE SCENARIOS

Most hybrid deployments follow the same architecture where on premise AD is viewed as the identity source that synchronizes user and group objects one way to Office365 using an SSO application such as AAD Connect, Okta, Centrify, or many others. Once this SSO application is in place, user and group objects are initially replicated to Office365 and any updates made to AD user and group objects are synchronized from AD to Office365. Nuvolex is designed to work in harmony with this hybrid configuration by not impeding with identity synchronization but more so sitting between Office365 and AD making changes to both environments.

Common architecture:

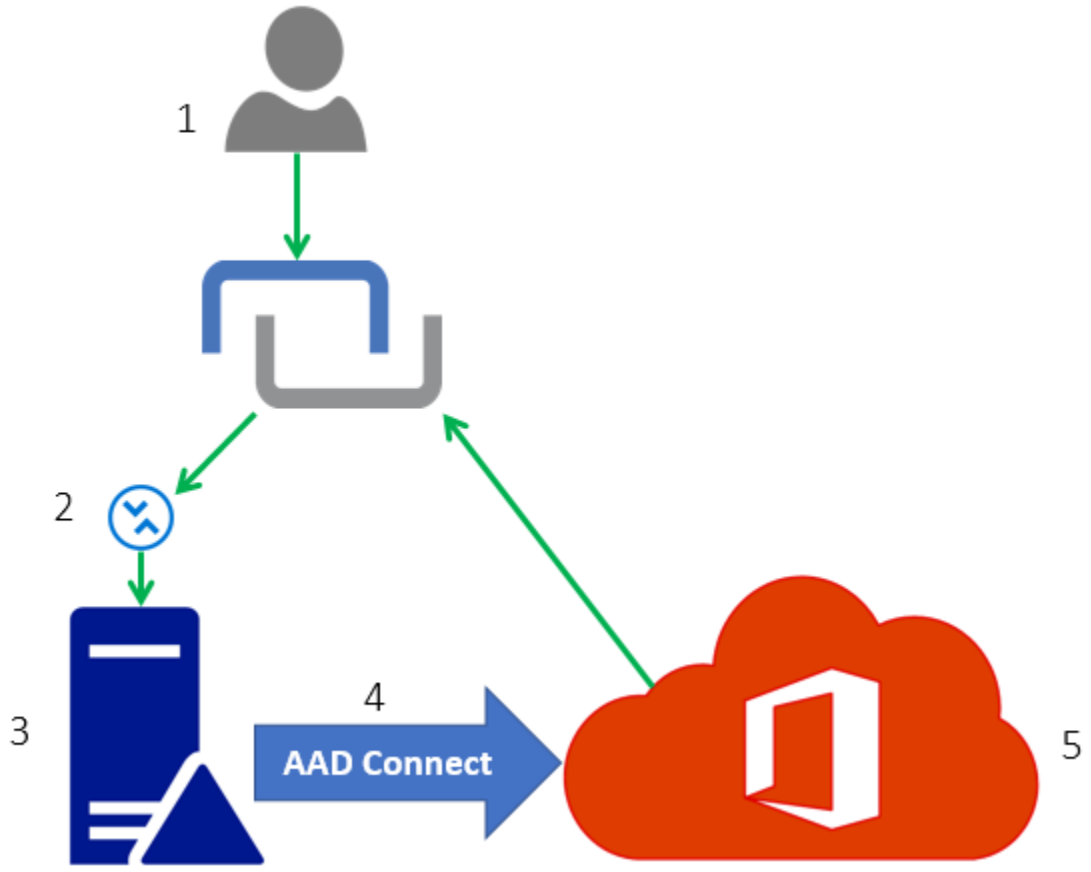


IT administrators use the Nuvolex platform to easily manage both Office365 and AD since the Nuvolex platform is tied to both environments. As seen in the diagram, there is a bidirectional link between the Nuvolex platform and both Office365 and AD. When an IT administrator makes a change to a AD user such as a password reset,

the Nuvolex platform sends the password reset request to the Nuvolex AD Agent which resets the user's password in AD. From there, the password change is synchronized from AD to Office365 using the SSO application (AAD Connect) and then Office365 is updated with the new user password. This entire interaction is triggered by the single click of "Reset Password" on the Nuvolex platform. The IT administrator is masked from the complexity of managing a hybrid environment.

There are several hybrid scenarios that are supported by the Nuvolex platform. Below is an overview of a few common hybrid management scenarios and the outcome of hybrid management actions.

Scenario one covers common Office365 deployments where user identities are synchronized from on premise Active Directory to Office365. The synchronization is handled by Microsoft's Azure Active Directory Connect synchronization tool. Any updates that are made in AD to users or groups are synchronized to Office365. AD users and groups need be managed directly in on premise AD and all Office365 tasks must be performed in Office365. IT Administrators have two environment's that need to be concurrently managed.
Using the Nuvolex platform and deploying the Nuvolex AD Agent, IT Administrators can easily manage users and groups from AD as well as licenses, attributes and mailboxes in the cloud from a single managment interface.

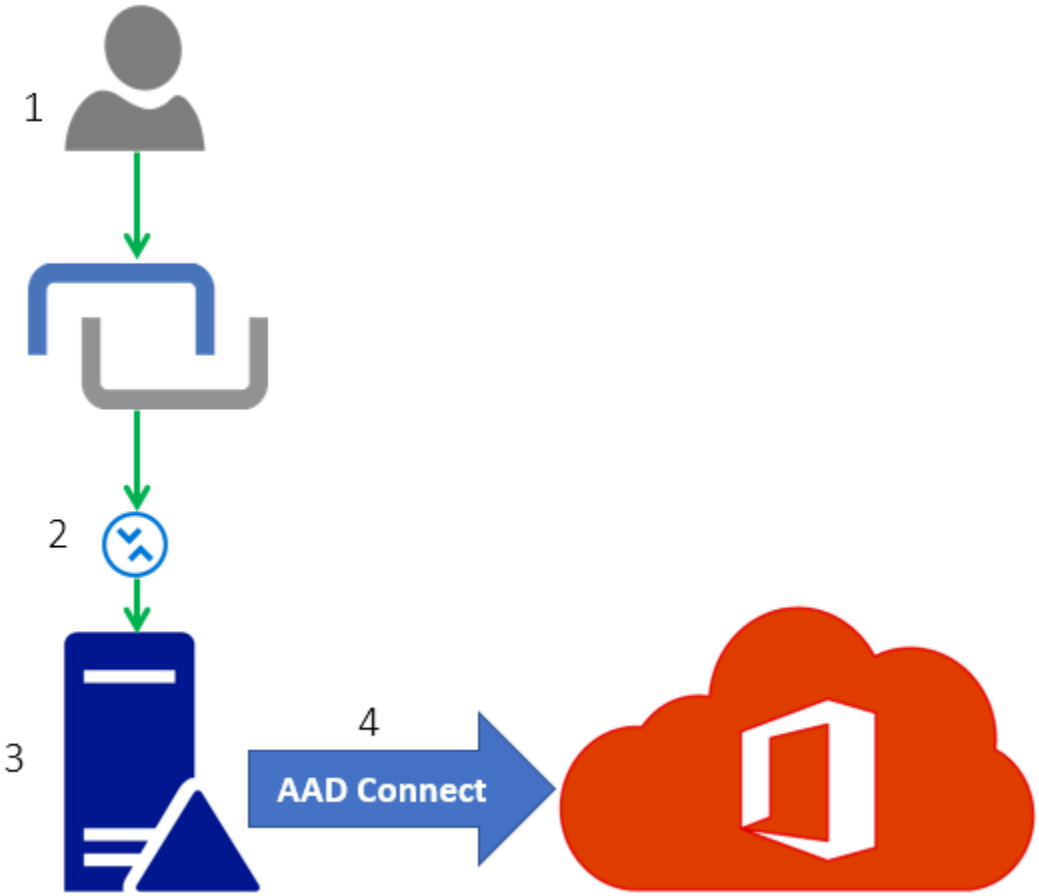


1. An IT Administrator logs into Nuvolex to apply changes to a hybrid Office365 user.
2. The change request is generated on the Nuvolex platform and sent to the Nuvolex AD Agent.

3. The Nuvolex AD Agent connects to a local AD Domain Controller and performs the requested change on an AD user.
4. The AD user update is then picked up by Azure Active Directory (AAD) Connect and runs a synchronization process to update Office365.
5. The AD user is synchronized with Office365 and any new changes to the users are updated in Office365.

End Result: The changes the IT Administrator using the Nuvolex platform performed on the Hybrid Office365 user are applied to the user in on premise AD. AAD Connect synchronizes the user changes from on premise AD to Office365. The Hybrid Office365 user is updated in both on premise AD and Office365.

Scenario two explores the popular task of managing AD user passwords. In this example, AD users are synchronized to Office365 using AzureAD Connect, or any other synchronization platform. Hybrid Office365 users need to have their passwords managed directly in on premise AD. With the Nuvolex AD Agent, an IT Administrator using the Nuvolex platform can reset passwords for any AD users which will write password changes back into on premise AD. Once the password has been updated for an AD users, AAD Connect will synchronize the password change to Office365 automatically.

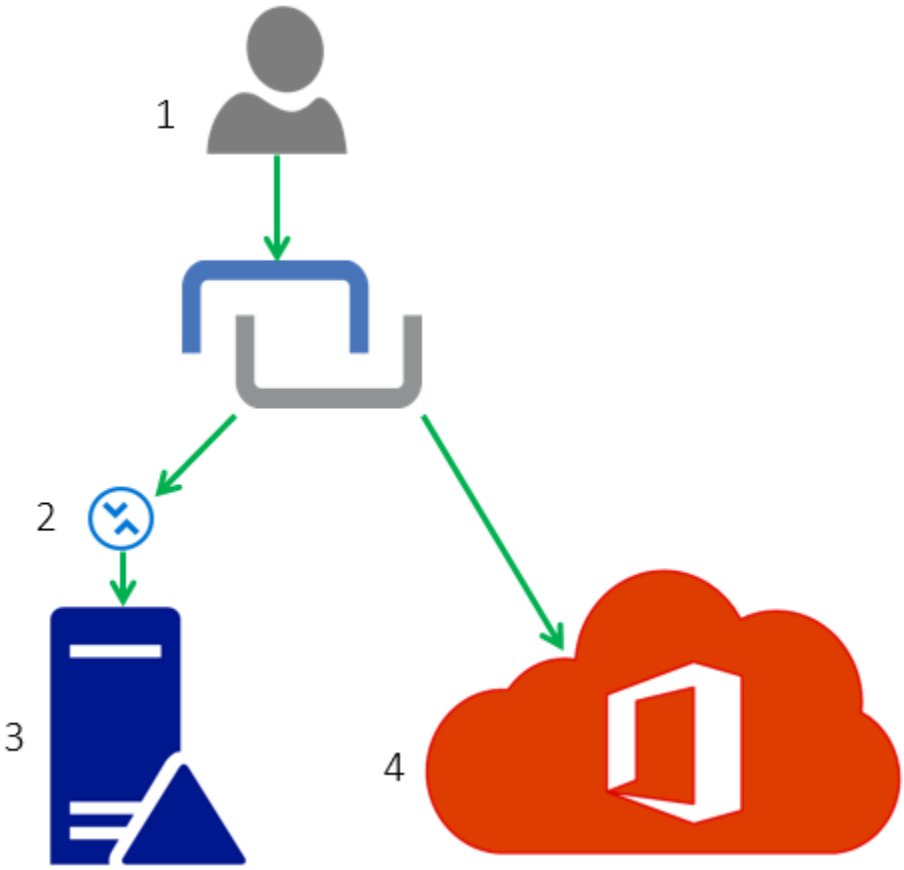


1. An IT Administrator logs into Nuvolex to reset the AD password for an end user.

2. The AD user password reset request is sent from the Nuvolex platform to the AD Agent integrated with the AD users domain.
3. The AD Agent locates the user on a Domain Controller and applies the password reset.
4. Azure AD (AAD) Connect will synchronize the password change to Office365.

End Result: The end user is able to login to the AD Domain and to Office365 services using the new password set by the IT Administrator using the Nuvolex platform.

Scenario three looks at a deployment that does not have any synchronization between on premise AD and Office365. End users exist in both environments and have two identities, one from AD and the other from Office365, but each identity has identical user attributes such as the user principal name.
When the organization's Office365 tenant and on premise AD user and group data is imported into Nuvolex, users from both environments are merged into a single user object on Nuvolex. When updates are performed for end users, the updates are applied in both Office365 and on premise AD.



1. An IT Administrator logs into Nuvolex to reset the AD password for an end user.
2. The AD user password reset request is sent from the Nuvolex platform to the AD Agent integrated with the AD users domain.
3. The AD Agent locates the user on a Domain Controller and applies the password reset.

4. Nuvolex then will send the same password change request for the end user to Office365.

End Result: The end user is able to login to the AD Domain and to Office365 services using the same new password set by the IT Administrator using the Nuvolex platform since the password is reset in both locations.

AD MANAGEMENT FEATURES

The Nuvolex AD Agent supports both Single Domain and Multi Domain Active Directory environments. However, there are some differences between the scope of write back support between these two environments types. The Nuvolex platform focuses common daily user and group management functions and does not have any functionality beyond identity management. The Nuvolex platform is unable to alter group policies, replication settings, and other AD administration functions outside of AD identity management.

The following features are supported for **Single Domain AD Environments:**

1. Reset AD user password
2. Edit AD user attributes
    a. First/Last name
    b. Display name
    c. User Principal Name
    d. Address/Phone Number
    e. Department/Job title
3. Add. remove, or change AD user Proxy Addresses
    a. Change primary SMTP address
4. Add new AD Users
5. Delete AD users
6. Add/Remove users from AD Security Groups
7. Add/Remove from AD Distribution Groups
8. Onboard and automatically construct AD OU tree and user OU assignments
9. Move users between AD OUs
10. Automated OU policy assignment for new users
11. Admin delegation by AD OU

The following features are supported for **Multi Domain AD Environments:**

1. Onboard AD Domains and build a relationship between users and their source AD domain
2. Onboard and automatically construct AD OU trees and user OU assignments for each AD domain
3. Global administration of all identities across all AD Domain
    a. Also segmentation of users by AD domain
4. Automated OU policy assignment for new users

5. Admin delegation by AD domain
6. Admin delegation by AD OU
7. Reset AD user password (*coming soon*)

NUVOLEX AD AGENT DETAILS

Agent:

- The Agent is a listener that sends and receives data to/from the Nuvolex Platform.
- When the Agent receives a request for reading or updating AD objects, standard LDAP calls using the .NET framework are made into the Domain Controller to execute the requested action.
- The Nuvolex AD Agent can be installed on any Windows based device joined to an AD domain.
- The Nuvolex AD Agent is installed using a simple installation wizard with only a handful of configuration steps.
- The device where the Agent is installed must have local connectivity to the Domain Controller you want to manage.
- The Agent uses HTTPS to communicate with the Nuvolex platform. Port 443 must be opened to internet access on the device where you will install the Agent.
- Data in transit between the on premise AD Agent and the Nuvolex Platform uses HTTPS traffic secured using TLS that uses a dedicated RSA 2048-bit key pair that enables 256-bit TLS data encryption
    - The certificate on the server side validates the origin of the server is the Nuvolex Agent endpoint as well as encrypts data.
- The Nuvolex Platform end point is hard coded into the AD Agent, no other servers or IPs can be used to communicate with the AD Agent.
- There is a set of credentials that is created for each AD Agent. Before sending or receiving data, the AD Agent must authenticate to the Nuvolex Platform
- The Agent authenticates to the domain controller using a Domain Admin user or a service account with delegated user and group administration rights. These credentials are not exposed to the Nuvolex platform.
- Nuvolex will never read or store any AD passwords
- Each Agent is unique to the tenant you are managing. If you are managing multiple tenants, you will need to install an AD Agent for each hybrid Office365 tenant you want to manage.
- The Agent requires you to use an AD account that has rights to read and make changes to AD users and groups.
- The Agent runs as a Windows Service and can be started/stopped from Services console.

Platform:

- The Nuvolex Platform will not store or expose the on premise AD Administrator credentials outside of the Agent that resides on premise.
    - All AD credentials remain on premise, never will be sent over the internet.

- We store “low risk” AD data
    - First/Last Name
    - Display Name
    - User Principal Name
    - Domain
    - Phone number
- ANY calls made to the Agent is required come from the Nuvolex Platform using a REST call.
- REST calls can only be made using a valid session started by a user authentication.
- Sessions are generated once a user logs in, and is disposed once the user is logged out.
- Only 1 valid session is allowed per user at a single time.
- Session IDs are a randomized string that are unique to each user authentication.
- Our Role Based Access Controls make it so that REST calls cannot be initiated unless the user making the call is authorized to do the action.
- REST calls cannot be made on tenants that the user does not have access to.
- The platform sits behind a web application firewall (WAF) that analyzes all traffic/requests sent to the platform in order to protect against the OWASP Top 10 Threats such as:
    - SQL, LDAP, OS injections
    - Broken Authentication and Session Spoofing
    - Cross Site Scripting (XSS)
    - Direct Access to Application Resources
    - Data Exposure
    - Cross Site Request Forgery (CSRF)
    - Denial of Service/Distributed DOS
    - Unvalidated redirections and forwards
- Our MySQL Database is encrypted at rest
- Hosted entirely in Azure
    - Strict server access rules for each instance hosted in Azure