Whitepaper

Okta Cloud Connect for Office 365

October 18, 2016

Tevora
1 Spectrum Pointe Dr., Suite 200
Lake Forest, CA 94107

info@tevora.com
949-250-3290

Comprehensive Identity Lifecycle Management for Office 365 Using Okta Cloud Connect for Free

If you are an existing or prospective Office 365 customer, you may be familiar with the challenges and limitations of the Microsoft-provided solutions for the management of user identities. This whitepaper defines the limitations of the prescribed Office 365 integration scenarios and offers a better, cost-effective alternative that provides true cloud identity management.

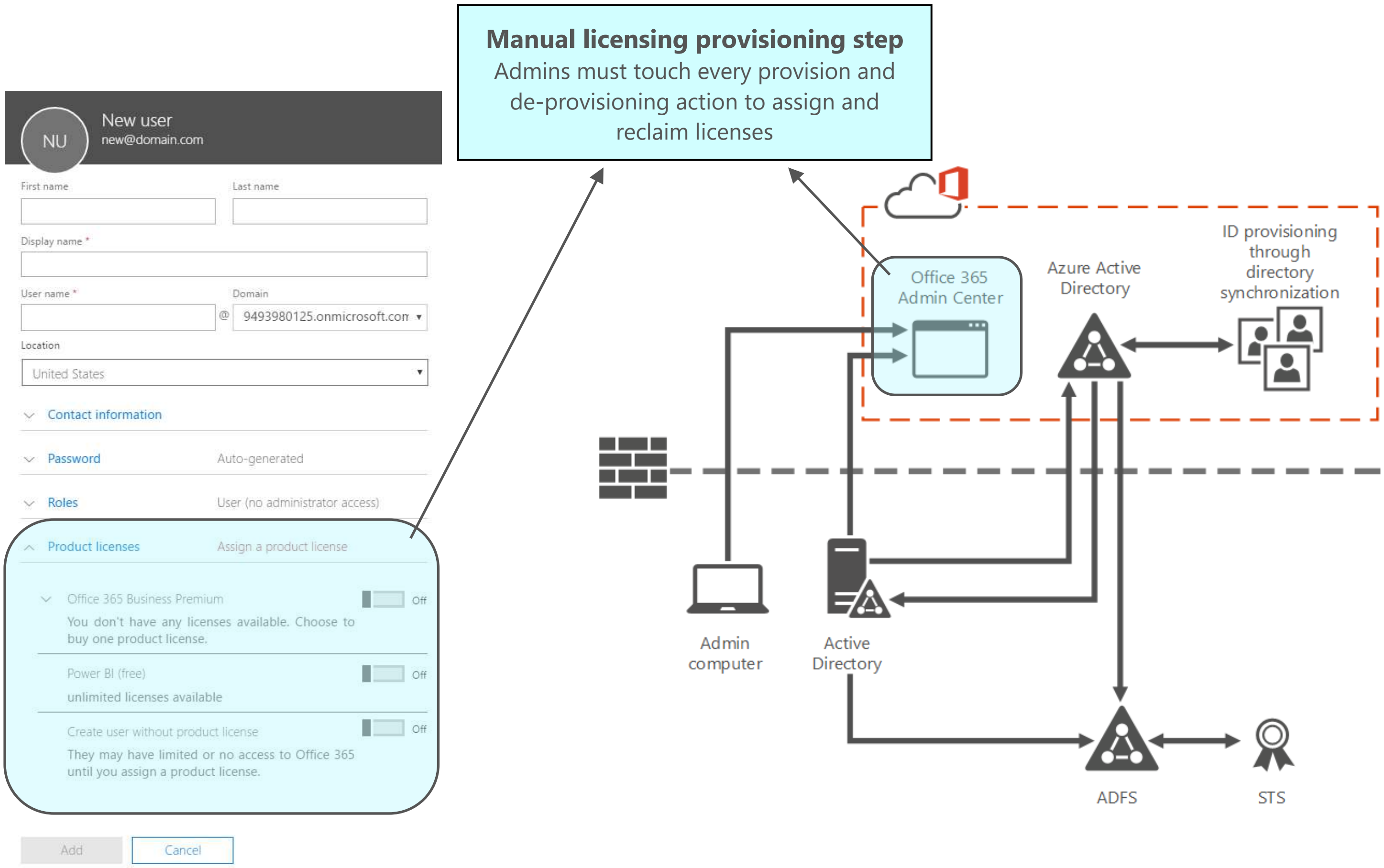
The Problem

Incomplete Provisioning and De-provisioning Lifecycle

Through the careful use and configuration of Active Directory Federation Services (ADFS), DirSync, and Azure AD Connect (AAD Connect), it is possible to synchronize on-premises Active Directory information with Office 365 and provide Single Sign-On (SSO) capability. The crucial step of assigning a user to an Office 365 licensing level is a manual process. While it is possible to cobble together PowerShell scripts or middleware applications to assign users a license in Office 365, there is currently no easy, Microsoft-supported method to achieve this.

This licensing problem also happens in reverse: user licenses are not reclaimed when users are disabled or deleted. There is not an effective way to provision, de-provision, and re-provision accounts automatically in Office 365 using supported Microsoft tools.

Manual Provisioning through a Browser



Manual licensing provisioning step
Admins must touch every provision and de-provisioning action to assign and reclaim licenses

NU New user
new@domain.com

First name
Last name
Display name *
User name *
Domain @ 9493980125.onmicrosoft.con
Location: United States
Contact information
Password: Auto-generated
Roles: User (no administrator access)
Product licenses: Assign a product license
Office 365 Business Premium — Off
You don't have any licenses available. Choose to buy one product license.
Power BI (free) — Off
unlimited licenses available
Create user without product license — Off
They may have limited or no access to Office 365 until you assign a product license.
Add
Cancel

Figure 1 - Microsoft Office 365 Identity Management (Microsoft, 2016)

Let’s look at the powershell method. These scripts will have to be maintained and run by in-house IT personnel and are not supported by Microsoft.

Scripted Provisioning Step 1: License Verification

Verification that there are available licenses to assign – if no licenses are available the creation of the user account and mailbox will fail (Goosen, 2016):

```
# Licensing Phase - Check if any users need to have licenses assigned
$NeedLicense = Get-AdGroupMember -Identity O365_License
If ($NeedLicense) {
        $HasMbxArray = @()
        Connect-MSOL
        Foreach ($User in $NeedLicense) {
            $UserInfo = Get-ADUser $User.SamAccountName -Properties *
            $Username = $UserInfo.SamAccountName
            $UserEmail = $UserInfo.Mail
            $UserLic = $UserInfo.extensionAttribute1
            $UserLoc = $UserInfo.c
            $UPN = $UserInfo.UserPrincipalName
            $MsolUser = Get-MsolUser -UserPrincipalName $UPN
            $HasLic = $MsolUser.IsLicensed
                If ($MsolUser -and $UserLic -and $UserLoc) {
                    Try {
                        If ($HasLic) {
                        $ExistingLic = $MsolUser.Licenses.AccountSkuId
                        Set-MsolUserLicense -UserPrincipalName $UPN -RemoveLicenses $ExistingLic
                        }
                        If ($UserLic -eq 'Exchange 2') {
                        Set-MsolUser -UserPrincipalName $UPN -UsageLocation $UserLoc
                        Set-MsolUserLicense -UserPrincipalName $UPN -AddLicenses $EP2SKU
                            Remove-AdGroupMember -Identity O365_License -Members $Username -Confirm:$False
                        }
                        ElseIf ($UserLic -eq 'E3') {
                        Set-MsolUser -UserPrincipalName $UPN -UsageLocation $UserLoc
                        Set-MsolUserLicense -UserPrincipalName $UPN -AddLicenses $E3SKU
                            Remove-AdGroupMember -Identity O365_License -Members $Username -Confirm:$False
                       }
                     }
                    Catch {
                    $EmailSubject = 'Office 365 Provisioning Error'
                    $EmailBody = @"
    }
```

Scripted Provisioning Step 2: Mailbox Creation

Assigning the license and creating the mailbox in the simplest form – logic for assigning additional product licenses based on AD attributes will have to be added:

```
# Mailbox Enablement Phase - Check if any new mailboxes need to be provisioned
$NeedMailbox = Get-AdGroupMember -Identity O365_Provisioning
If ($NeedMailbox) {
    Connect-Exchange
    Foreach ($User in $NeedMailbox) {
    $Username = $User.SamAccountName
    $UserInfo = Get-ADUser $Username -Properties *
    $UserLic = $UserInfo.extensionAttribute1
    $UserLoc = $UserInfo.c
    If ($UserLic -and $UserLoc){
        Try {
            Enable-RemoteMailbox $Username -RemoteRoutingAddress "$Username@$RoutingDomain"
            Add-ADGroupMember -Identity O365_License -Members $Username
            Remove-AdGroupMember -Identity O365_Provisioning -Members $Username -Confirm:$False
                }
        Catch {
        $EmailSubject = 'Office 365 Provisioning Error'
        $EmailBody = @"
        }
    }
}
```

Infrastructure Overhead of ADFS

Achieving SSO using Microsoft ADFS 2.0 or AAD Connect can be cumbersome. While these tools have improved ADFS still requires on-premises infrastructure and provides limited support for authentication standards beyond Microsoft's proprietary WS-Fed architecture.

ADFS authenticates Office 365 users to their Active Directory account by requiring Active Directory to directly respond to the user authentication requests. Organizations must configure and manage a network path from the internet to your ADFS servers, and from ADFS to your domain controllers. Network connectivity from the cloud, all the way to Active Directory servers must be highly available. If anything on premises fails, users cannot authenticate to Office 365. ADFS does not provide a simple and effective identity architecture for broad cloud-based authentication.

The Solution

Okta is a fully-featured cloud identity platform and is the leading identity management service for Office 365 that can handle the entire identity lifecycle automatically. Users want a simple, unified SSO experience and administrators want fully automated identity management.

Notice that for the most common account and mailbox provisioning use cases, the Microsoft stack of AAD Connect, Azure AD, and ADFS require a manual step. At best, this manual step can be automated but it is not supported and must be managed independently from the as shown above.

Provisioning Workflow

Step	Microsoft Stack	Okta
Create User and Map AD Attributes	Automated	Automated
Map custom attributes and perform non-standard mappings	Manual	Automated
Grant Office 365 admin rights	Manual	Automated
Allocate licensing and perform fine-grain provisioning	Manual	Automated
Sync passwords	Automated	Automated

De-provisioning Workflow

Step	Microsoft Stack	Okta
Disable User	Automated	Automated
Reclaim license for reallocation	Manual	Automated

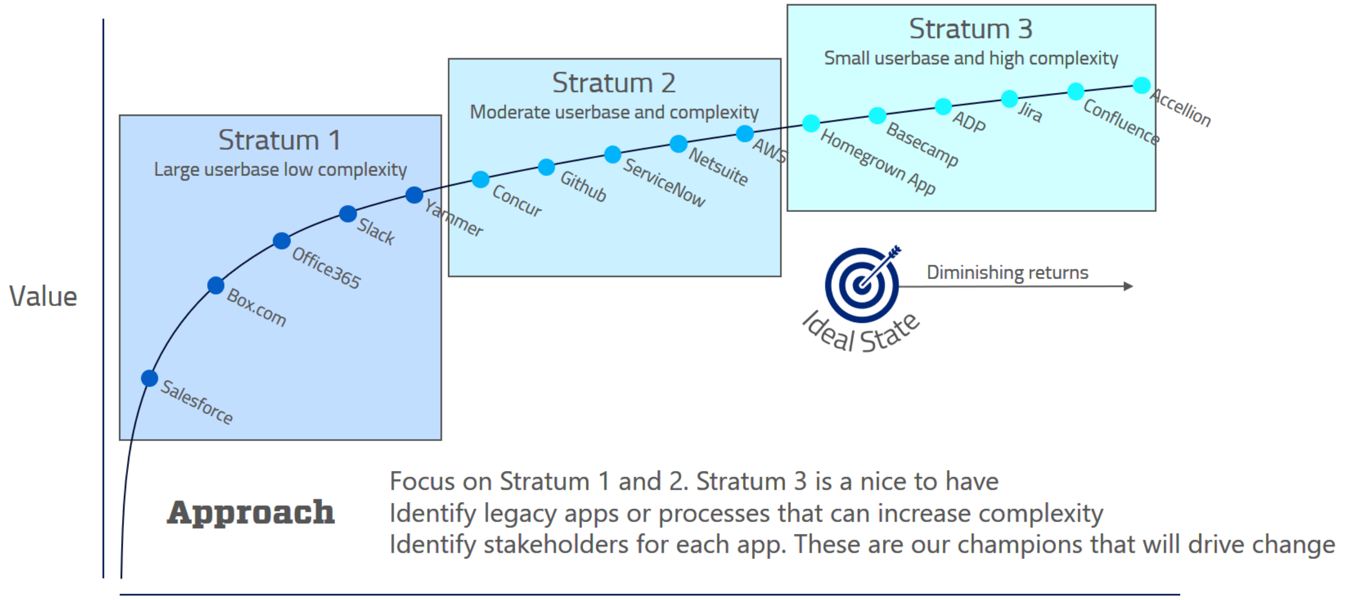
Getting Started

Okta Cloud Connect (OCC) is a product that allows for usage of the Okta platform for free for one application. Many organization have partnered with Tevora to enable fully automated Office 365 management through this free Okta product.

Okta Cloud Connect Product Page:
https://www.okta.com/partners/okta-cloud-connect/

Going Further

Users of Okta Cloud Connect for Office 365 are well positioned to extend the use of Okta to other enterprise applications. The Tevora approach of planning and execution of Okta expansion is built on a value and risk-based approach to identifying application owners, provisioning workflows, authentication options, and Okta migration feasibility. We then stratify the target applications and establish an implementation roadmap. In practice not all applications are good targets for Okta integration but there is always a targeted Ideal State for all Okta implementations beyond which there are diminishing returns for further application integration.



Focus on Stratum 1 and 2. Stratum 3 is a nice to have
Identify legacy apps or processes that can increase complexity
Identify stakeholders for each app. These are our champions that will drive change

Figure 2 - Integration Value Curve

About Tevora

Tevora is the nation's premier management consulting firm specializing in information assurance, governance and compliance services, and solutions. We work with some of the world's leading companies, institutions, and governments to ensure the safety of their information and their compliance with applicable regulations. Our main offices are located in Lake Forest, California.

Philosophy

As security professionals, we believe in using technology to lead the way rather than following the pack. We not only believe in servicing our clients' immediate needs, but also partnering with them long term. We recommend proactive initiatives rather than passive protection and we are committed to developing strategic solutions that meet our client's needs.

Consulting Team

Tevora is led by people with years of experience in business and technology. We understand business issues and we're best positioned to help companies transform security from a cost of doing business to a way to do more business. We believe that an MBA is just as important as a CISSP. We only hire credentialed, business-focused senior consultants.

Technology

While we are credentialed, experienced, and do considerable work with all of the industry's top security software vendors, we are beholden to none. Tevora is completely vendor agnostic, which allows us to utilize best-of-breed security software products based solely on our clients' needs. We offer the most strategic solutions to the companies we work with.

References

Figures

Sources

Goosen, C. (2016). *Using Powershell to Automate Office 365 License Assignment*. Retrieved from Chris's Blog: http://www.cgoosen.com/2016/03/using-powershell-to-automate-office-365-license-assignment/

Microsoft. (2016). *Understanding Office 365 identity and Azure Active Directory*. Retrieved from Microsoft Office Support: https://support.office.com/en-us/article/Understanding-Office-365-identity-and-Azure-Active-Directory-06a189e7-5ec6-4af2-94bf-a22ea225a7a9?ui=en-US&rs=en-US&ad=US