Boosting productivity for SAP users with Azure ADS Single Sign-On

Holger Bruchelt
June 7th, 2018
SAP and Microsoft partnership—the next chapter

The trusted, optimized, seamless enterprise-ready cloud partnership

**Trusted**

20+ year alliance partnering together for the benefit of our mutual customers

85% of Fortune 500 have SAP and Microsoft Cloud

**Optimized**

Unique capabilities, roadmap, and experience to support SAP HANA & enterprise workloads from *on-premises* and Azure

**Seamless**

Co-located engineering resources & aligned sales and marketing teams provide a seamless customer experience

“We are taking our partnership to the next level... Together, we will help companies win the customer-driven growth revolution...”

—Bill McDermott, CEO of SAP

“Building on our longtime partnership, Microsoft and SAP are harnessing each other’s products to not only power our own organizations, but to empower our enterprise customers to run their most mission-critical applications and workloads with SAP S/4HANA on Azure.”

—Satya Nadella, CEO of Microsoft
Azure Active Directory across Microsoft & SAP

On-premises

Microsoft Azure

Active Directory

Azure AD Connect

Employees (Intranet)

Employees (Mobile)

Partners

Azure Active Directory B2B

SAP HANA
HANA Enterprise Cloud
SAP Cloud Platform
S/4HANA Cloud

Azure Active Directory across Microsoft & SAP

Office 365
Microsoft Dynamics 365
Power BI
Microsoft Intune

SAP Ariba
Concur
SAP Fieldglass
SAP BusinessObjects

© Microsoft Corporation
Announcing Single Sign-On Support when connecting to data sources from the Power BI Service

- Possibility to use Single Sign-On, leveraging Kerberos, when connecting to certain data sources using DirectQuery mode from Power BI.

Power BI Service:
1. For each interactive query by a Power BI AAD user, and each per-user dashboard tile update (background refresh) to on-premises DirectQuery sources configured for SSO, PBI Service passes along UPN string: “firstName.lastName@contoso.com”

On-premises Data Gateway with SSO:
2. If AAD DirSync/Connect configured: UPN string maps to AD user account
   Alternatively, autom. UPN mapping through AD lookup by gateway:
   • Find Active Directory to search (automatic, or configurable)
   • Lookup e.g. Email attribute of AD Person based on incoming UPN string (“firstName.lastName@contoso.com”) from Power BI Service.
   • If the AD Lookup fails, attempts to use the passed-along UPN string
   • If AD Lookup succeeds, retrieves UserPrincipalName of that AD Person.
3. Gateway resolves on-premise user principal name, performs Kerberos protocol auth transition, and opens data connection as that Windows identity, e.g. “Alias@corp.on-prem.contoso”
Single Sign-On for SAP GUI (using Kerberos)

- The SAP Single Sign-On product offers support for Kerberos/SPNEGO
- Using Kerberos technology via SNC or SPNEGO, a trust relationship is established between the user's front end (SAP GUI for Windows or a web browser, for example) and the back-end Application Server ABAP or Java

Single Sign-On Based on Kerberos / SPNEGO
Single Sign-On to SAP Fiori (running on SAP NetWeaver)

- Simple wizard based setup both on Azure Active Directory and SAP NetWeaver Side
- Maintain and control users on Azure Active Directory
Single Sign-On to SAP Cloud Platform

SAP Cloud Platform with Azure AD

• Control in Azure AD who has access to SAP Cloud Platform.
• Enable your users to automatically get signed-on to SAP Cloud Platform (Single Sign-On) with their Azure AD accounts.
• Manage your accounts in one central location - the Azure portal.
Use Azure AD authentication for Linux VMs to centrally control and enforce policies that allow or deny access to the VMs.

Log in to a Linux virtual machine in Azure using Azure Active Directory authentication (Preview)

To improve the security of Linux virtual machines (VMs) in Azure, you can integrate with Azure Active Directory (AD) authentication. When you use Azure AD authentication for Linux VMs, you centrally control and enforce policies that allow or deny access to the VMs. This article shows you how to create and configure a Linux VM to use Azure AD authentication.

⚠️ Note
This feature is in preview and is not recommended for use with production virtual machines or workloads. Use this feature on a test virtual machine that you expect to discard after testing.

There are many benefits of using Azure AD authentication to log in to Linux VMs in Azure, including:

- **Improved security:**
  - You can use your corporate AD credentials to log in to Azure Linux VMs. There is no need to create local administrator accounts and manage credential lifetime.
  - By reducing your reliance on local administrator accounts, you do not need to worry about credential loss/theft, users configuring weak credentials etc.
  - The password complexity and password lifetime policies configured for your Azure AD directory help secure Linux VMs as well.
  - To further secure login to Azure virtual machines, you can configure multi-factor authentication.
  - The ability to log in to Linux VMs with Azure Active Directory also works for customers that use Federation Services.
Single Sign-On to SAP HANA
Live Demos

- Configuration NetWeaver
- Configuration SAP Cloud Platform
- Configuration Azure