

Hybrid Secure Access with Azure Active Directory and F5 BIG-IP

Azure Active Directory and F5 BIG-IP Access Policy Manager (APM) integration allows seamless access to legacy applications hosted in the cloud or on-premises. The integrated solution takes advantages of all the modern capabilities of Azure Active Directory like [Azure AD conditional access](#), [Azure AD Identity Protection](#) and [Azure AD Identity Governance](#) for legacy applications access without app modifications or agents installation.

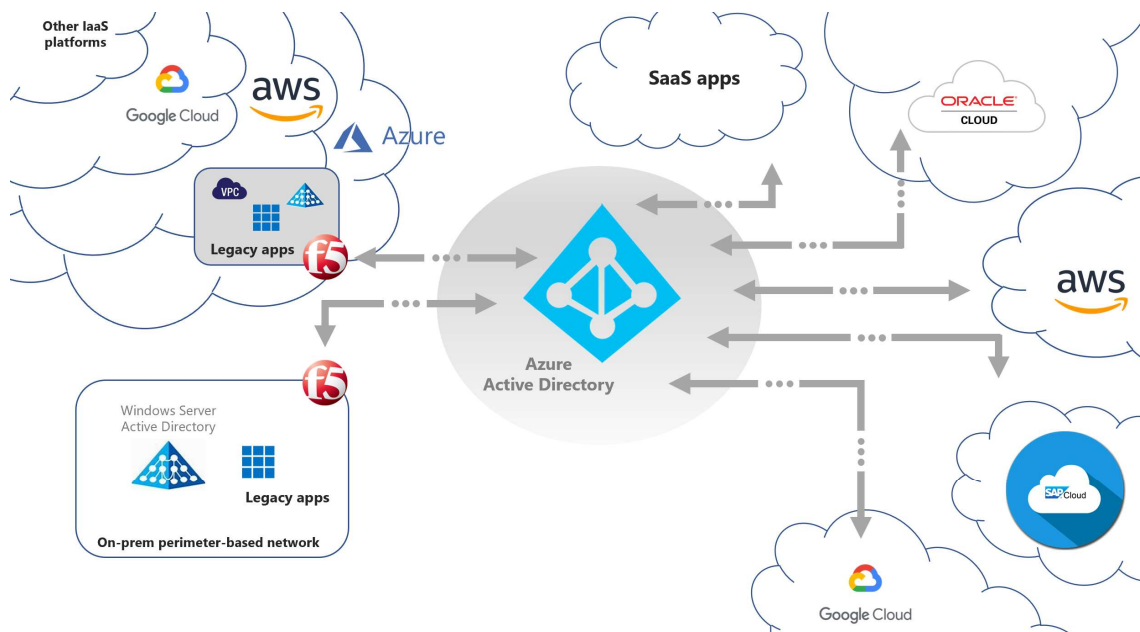


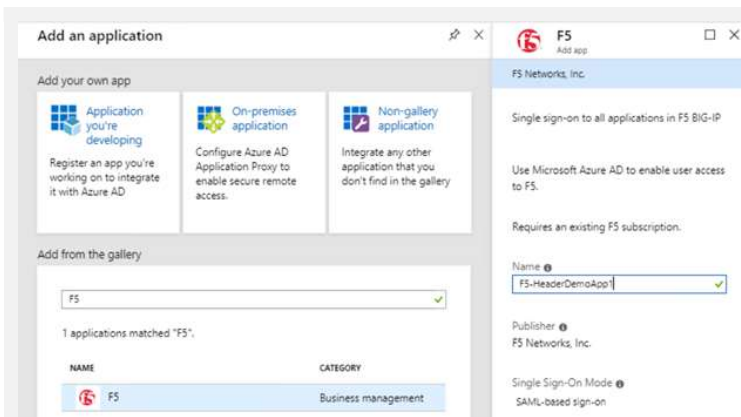
Figure 1 – Where F5 fits into the broader Hybrid Secure Access scenario

Key Authentication Scenarios

Apart from Azure Active Directory native integration support for modern authentication protocols like Open ID Connect, SAML and WS-Fed, F5 extends secure access for legacy-based authentication apps for both internal and external access with Azure AD, enabling modern scenarios (e.g. password-less access) to these applications. This include:

- ❖ Header-based authentication apps
- ❖ Kerberos authentication apps
- ❖ Anonymous auth or no inbuilt authentication apps
- ❖ NTLM authentication apps (protection with dual prompts for the user)
- ❖ Forms Based Application (protection with dual prompts for the user)

Solution Highlights



Add an application

Add your own app

- Application you're developing
- On-premises application
- Non-gallery application

Add from the gallery

1 applications matched "F5".

NAME	CATEGORY
F5	Business management

F5

Single sign-on to all applications in F5 BIG-IP

Use Microsoft Azure AD to enable user access to F5.

Requires an existing F5 subscription.

Name: F5-HeaderDemoApp1

Publisher: F5 Networks, Inc.

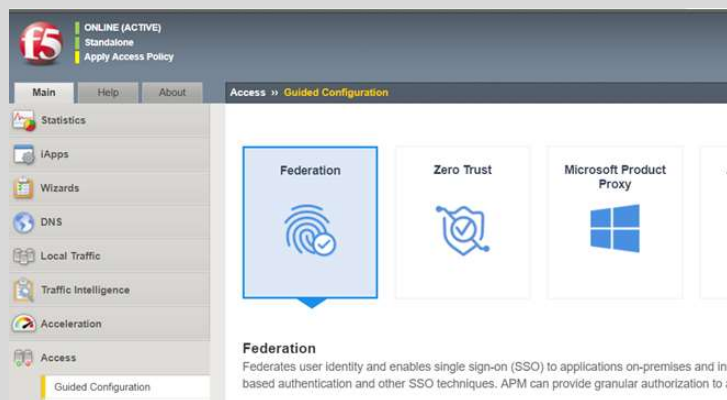
Single Sign-On Mode: SAML-based sign-on

Pre-Integrated App

F5 BIG-IP is a pre-integrated app in Azure AD with configuration in place that simplifies integration

Guided Configuration Wizard

Full support for the new guided configuration experience on F5 BIG-IP in addition to flexible advanced configuration support



ONLINE (ACTIVE)

Standalone

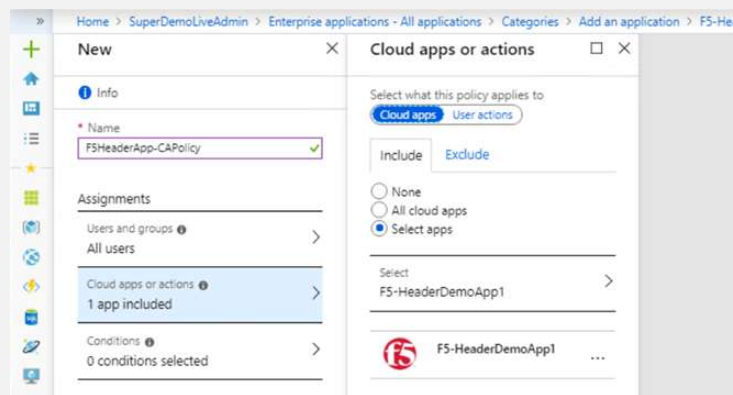
Apply Access Policy

Main Help About

Access > Guided Configuration

Federation

Federates user identity and enables single sign-on (SSO) to applications on-premises and in the cloud. APM can provide granular authorization to applications.



Home > SuperDemoLiveAdmin > Enterprise applications - All applications > Categories > Add an application > F5-HeaderApp-CAPolicy

New

Info

Name: F5-HeaderApp-CAPolicy

Assignments

- Users and groups: All users
- Cloud apps or actions: 1 app included
- Conditions: 0 conditions selected

Cloud apps or actions

Select what this policy applies to

Cloud apps User actions

Include Exclude

None All cloud apps Select apps

Select: F5-HeaderDemoApp1

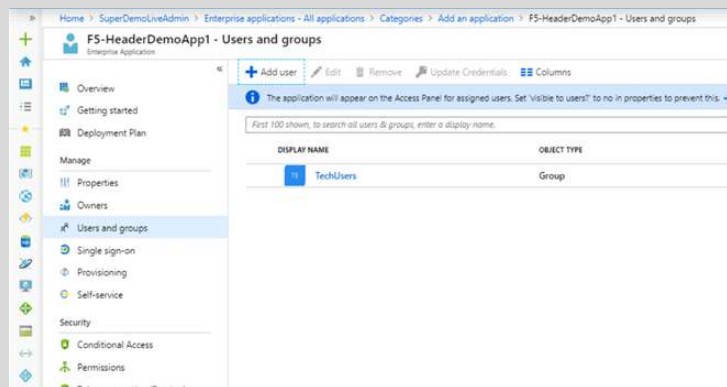
F5-HeaderDemoApp1

Conditional Access

Protection of legacy apps with the power of Azure Active Directory controls including conditional access, identity protection and governance

Centralized Authorization

Control authorization to both cloud and on-premises apps using a single control plane



Home > SuperDemoLiveAdmin > Enterprise applications - All applications > Categories > Add an application > F5-HeaderDemoApp1 - Users and groups

F5-HeaderDemoApp1 - Users and groups

Enterprise Application

Overview Getting started Deployment Plan Manage Properties Owners Users and groups Single sign-on Provisioning Self-service Security Conditional Access Permissions Token Authentication (Preview)

Users and groups

The application will appear on the Access Panel for assigned users. Set 'Visible to users?' to no in properties to prevent this.

First 100 shown, to search all users & groups, enter a display name.

DISPLAY NAME	OBJECT TYPE
TechUsers	Group

Microsoft

Apps

Add-in

FS-HeaderDemoApp1

Forms

Planner

Stream

Yammer

Dynamics 365

FS-KerberosApp1

HRWEB

Power BI

Sway

Expense

Flow

Kaizala

PowerApps

Teams

Groups

SharePoint

End-user Experience

Users can leverage the familiar MyApps portal to access on-premises and cloud legacy applications

Risk Reporting

Get centralized visibility into access risk via risk reporting and mitigate risk using Identity Protection to legacy applications running on-premises or in the cloud

GENERAL

Overview

Getting started

INVESTIGATE

Risky users (Users flagged for ri...

Risky sign-ins (Preview)

Risk Detections (Risk events)

Vulnerabilities

CONFIGURE

MFA registration

User risk policy

Sign-in risk policy

SETTINGS

This view will soon be replaced by Azure AD Identity Protection's advanced 'Overview'. Try it out.

Users flagged for risk

2

At r... 2

Sec... 0

Risk events

0

1

0

0

High Medium Low Closed

Windows Hello

Microsoft Authenticator

FIDO2 Security Keys

Passwordless support

Enable passwordless access for your legacy applications on-premises or in the cloud