Solution Brief

Symantec VIP Native Integration to Microsoft Azure Active Directory

Enabling the Cloud Generation

The promise of increased productivity with cloud applications has paid off and the traditional corporate network perimeter is quickly becoming a thing of the past. Today's corporate user demands frictionless access to their favorite productivity applications while keeping their identity and personal information secure. The proliferation of cloud applications has caused user identity and access management, which used to be purely in-premise provisioning and management concepts, to become border-less and be maintained with multiple solutions. User identities are either locked down in-premise with federation services layered on top (such as ADFS) or duplicated and synchronized with third party Identity-as-a-Service (IDaaS) solutions. On their cloud journey, organizations of all sizes are quickly realizing that simplifying identity solution deployments while keeping user access secure is mission critical to their success.

Cutting out the 'Middle Man'

On-premise identity federation services are not only difficult to deploy and manage but create heavy IT burden. Eliminating the need for this 'middle-man' identity provider by moving to a cloud native identity platform is the leading industry trend. Microsoft Azure AD has created a seamless and standards-based identity eco-system and provided organizations a smooth ramp from their on-premise directory solution to the cloud. Most notibly, turn-key integration with Office 365 has fueled tremendous growth of this platform. As a result, establishing a native integration with Azure AD and authenticating directly to Azure applications has become a key requirement to cloud migration. We are excited to offer Symantec VIP as the preferred authentication provider directly through Microsoft Azure Conditional Access.

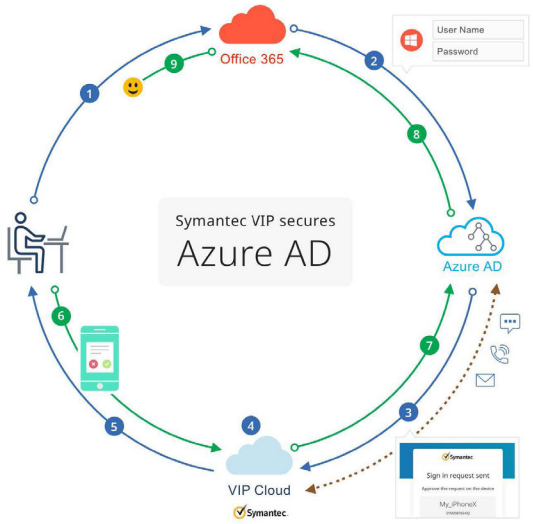
Configuring VIP for Azure

VIP now natively integrates with Microsoft Azure AD to allow for easy authentication into Microsoft applications such as Office 365. An enterprise administrator will need to first configure their Microsoft Azure AD tenant as an authorized application within the VIP administrative portal. Once complete, they can follow our documentation to easily setup Symantec VIP as the preferred two-step verification provider via Conditional Access for Microsoft's cloud application ecosystem such as Office 365.

How it works:

1. User accesses Microsoft Online/O365 or any other Azure AD client application.
2. User submits 'Username' and 'Password' to Azure AD.
3. Azure AD validates credentials and passes control to VIP via Conditional Access.
4. VIP prompts user to verify their identity.
5. User gets a VIP Push notification on their mobile phone to prove their identity.
6. User approves VIP Push from their mobile phone.
7. VIP relays the successful authentication to Azure AD.
8. Azure AD grants the user access to the application based on access control policies.
9. User is successfully logged in.

Figure 1: Strong Authentication for Azure AD with VIP



Key Benefits

Securing Cloud Migration

Customers who are migrating to cloud workloads now have a authentication solution that protects access to sensitive cloud applications both in and out of the Azure ecosystem. Whether it is adopting Azure AD, Office 365 or a 3rd party cloud application, VIP helps secure that cloud journey by preventing unauthorized user and device access.

Cloud applications allow users access from anywhere and any device which enable productivity and as a result: remote workers and users on BYO devices are now able to work securely with the promise of the cloud. Securing access from remote users and BYO devices are a growing administrative concern that VIP helps alleviate.

Enabling the Entire Microsoft Journey

Symantec VIP not only protects access to your Micrsoft Azure applications, we protect the entire Microsoft suite. From the time and end user logs into their computer to when an end user onboards their BYO device, VIP is there to protect against all malicious and unauthorized attempts. Secure onboarding of end users is part of the VIP self service capabilities that are built into the native Azure AD integration. Logging in to Windows computers can be protected with multi-factor authentication as well, regardless of the user being domain joined or not. Computer logins can even be protected if the end user is completely off-line. Symantec VIP ensures that the entire Microsoft stack - from their hardware machines to their browsers to their cloud applications are all protected with strong authentication.

Reducing Total Cost of Ownership (TCO)

VIP's integration with Azure AD allows organizations to take advantage of the full Microsoft cloud identity and authentication platform. By moving to the cloud, organizations can eliminate time and money spent managing on-premises components such as directories and federation and authentication servers. All of the reduced administrative costs and end user friction means reduction in total cost of ownership (TCO).

Deployment Considerations

Conditional access with third-party MFA custom controls requires an Azure Active Directory Premium P1 subscription. Review Microsoft's Azure conditional access documentation before configuring VIP.

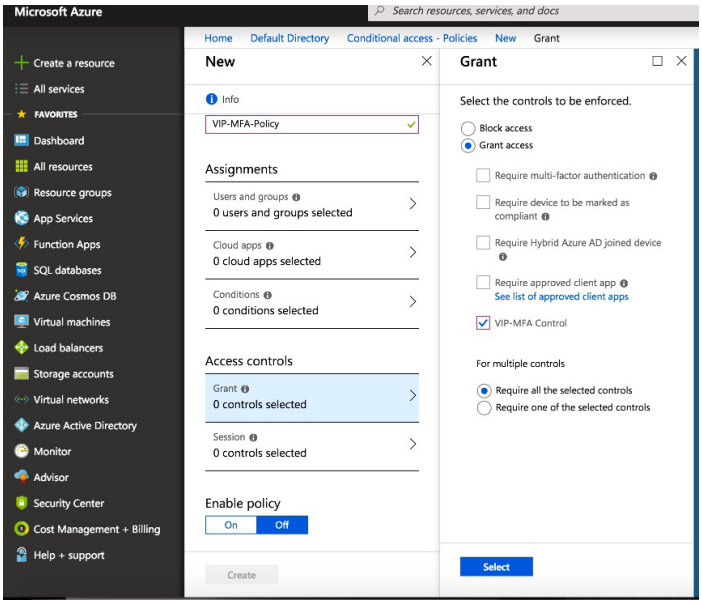
Note that Azure Active Directory conditional access protects cloud applications only when the user access originates from the following client applications:

- Web browsers
- Mobile and Desktop clients that support Microsoftmodern authentication (such as Office 2016applications).

Conditional access currently cannot enforce access controls in older Office clients such as Office 2010.

Contact your account representative for further information on deployment options.

Figure 2: Configuring a Conditional Access Policy



Symantec
A Division of Broadcom

For product information and a complete list of distributors, visit our website at: broadcom.com

Copyright © 2020 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries. Broadcom, the pulse logo, Connecting everything, and Symantec are among the trademarks of Broadcom.
SED-VIP-Azure-SB100 May 6, 2020