



10 QUICK WINS IN HYBRID IDENTITY

Brian Desmond

www.ravenswoodtechnology.com

bdesmond@ravenswoodtechnology.com

Ravenswood Technology Group, LLC

Max Fritz

Technology Solutions Professional

Microsoft

max.fritz@microsoft.com



10 QUICK WINS IN HYBRID IDENTITY

Brian Desmond

www.ravenswoodtechnology.com

bdesmond@ravenswoodtechnology.com

Ravenswood Technology Group, LLC

Max Fritz

Technology Solutions Professional

Microsoft

max.fritz@microsoft.com



ABOUT ME – BRIAN DESMOND



@brdesmond



<https://www.linkedin.com/in/briandesmond/>



<https://www.ravenswoodtechnology.com>



ABOUT ME – MAX FRITZ



Microsoft



@theCloudSherpa



<https://www.linkedin.com/in/maxafritz/>



<https://www.maxafritz.com>

SECURE INFRASTRUCTURE FOR HYBRID IDENTITY



On-premises infrastructure is where it all begins



Accurate, timely, reliable identities are crucial



Your house needs to be in order, but it shouldn't block cloud adoption

QUICK WINS: THE EASY STUFF



Momentum is critical



Show clear business value



Build foundations

SELF-SERVICE PASSWORD RESET

1

- ▶ Analysts make a lot of money selling data on password reset costs
- ▶ You can solve for this cost quickly and easily
- ▶ SSPR is relatively useless without behavior changes:
 - ▶ Everyone must be forced to register
 - ▶ The service desk must refuse to do password resets and account unlocks
- ▶ With the converged MFA/SSPR experience, only one enrollment is necessary



SSPR Demo

APP SINGLE SIGN-ON

2

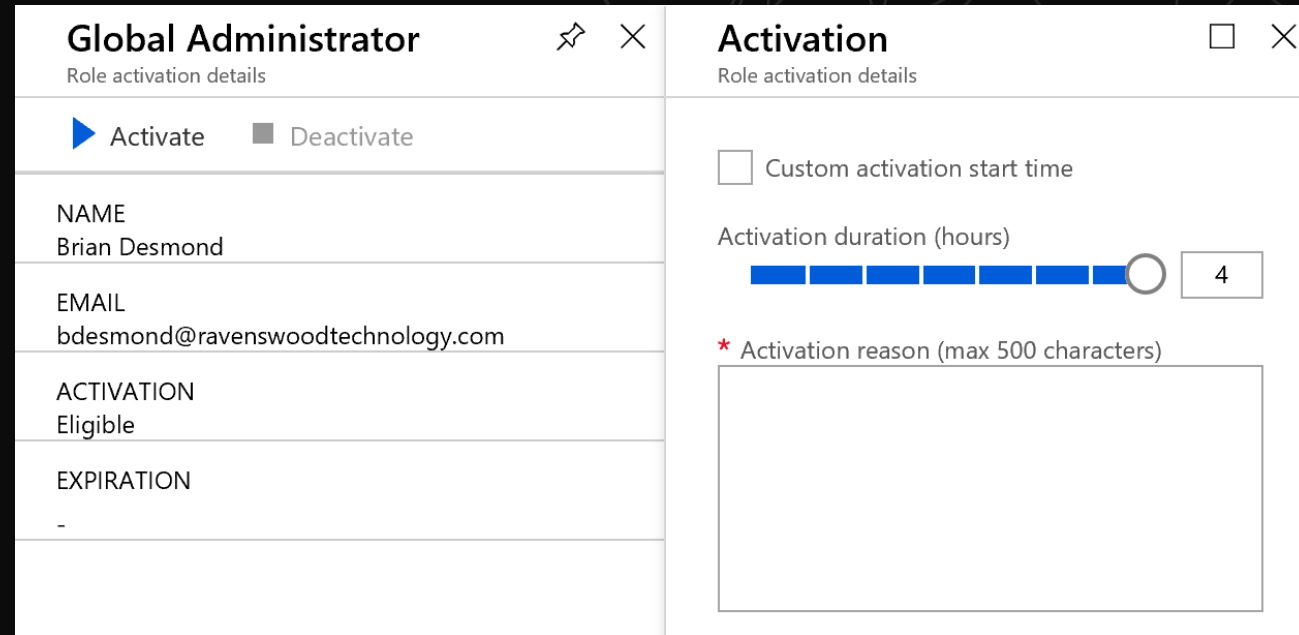
- ▶ Nobody likes a collection of passwords
- ▶ Federation platforms are complicated and expensive
- ▶ Start with high volume and high-risk apps
- ▶ You'll hit apps with requirements you can't meet, but that's OK
- ▶ App vendors will be an inhibitor
- ▶ Fiddler is your friend



PRIVILEGED IDENTITY MANAGEMENT

3

- ▶ AAD PIM is quick and easy governance and security
- ▶ Move quickly to make all your role members "eligible"
- ▶ Use role activation data to identify unnecessary role members
- ▶ AAD P2 licenses are only required for covered administrators



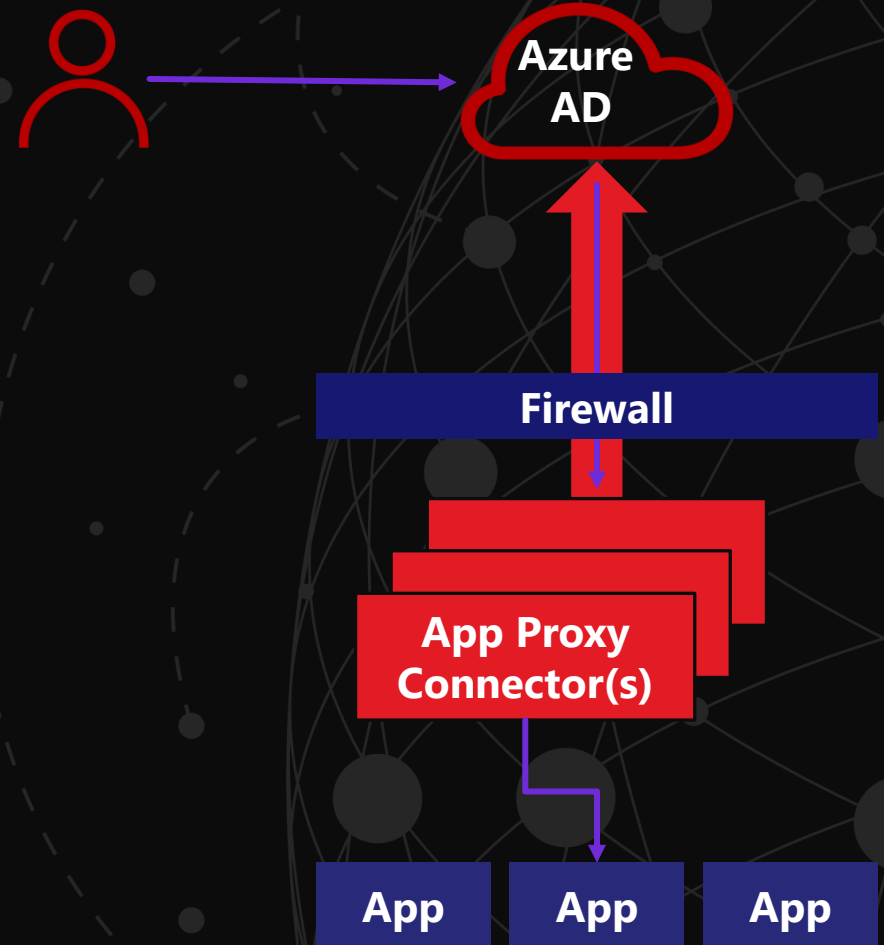
Global Administrator	
Role activation details	
<input type="button" value="Activate"/> <input type="button" value="Deactivate"/>	
NAME	Brian Desmond
EMAIL	bdesmond@ravenswoodtechnology.com
ACTIVATION	Eligible
EXPIRATION	-

Activation	
Role activation details	
<input type="checkbox"/> Custom activation start time	
Activation duration (hours)	<input type="text" value="4"/>
* Activation reason (max 500 characters)	
<input type="text"/>	

AZURE APPLICATION PROXY

4

- ▶ This is one of my favorite features
- ▶ Make Intranet apps accessible without a VPN
- ▶ Use conditional access to enforce rules on app access
- ▶ Three tools to solve app proxy problems:
 1. Kerberos delegation know-how
 2. Netmon/Wireshark
 3. Fiddler



UBER FAST SECURITY – CONDITIONAL ACCESS

5

- ▶ CA policies will let you wrap MFA and controls over all your apps
 - ▶ Cloud
 - ▶ On-Premises
- ▶ Go from *wide open* access to *protected* with minutes of work

Conditional Access Controls

- ▶ Multi-factor authentication
- ▶ Device type/OS
- ▶ Known device
- ▶ Compliant/healthy device
- ▶ Location
- ▶ Sign-in risk
- ▶ App enforced control



Conditional Access Policies

PASSWORD HASH SYNC

6

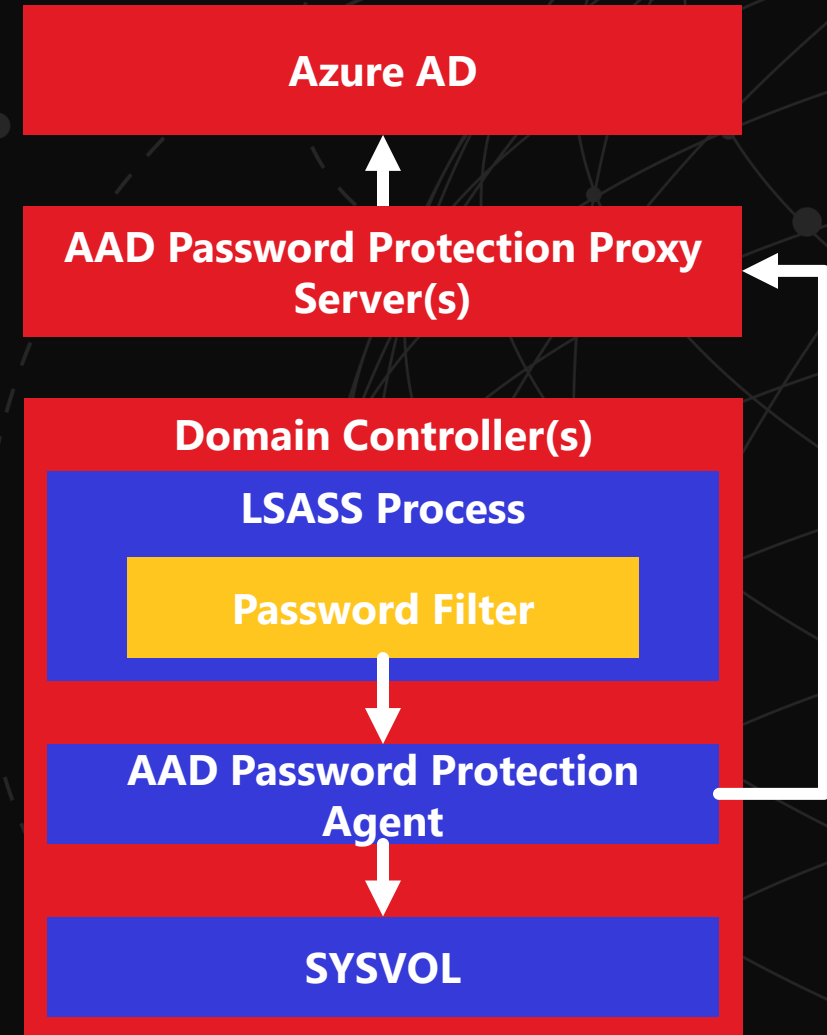
- ▶ You should enable password hash sync in all cases
- ▶ Federation will continue to work, if you use it
- ▶ Password hash sync enables the leaked credentials report
- ▶ You also gain a free DR plan for federation

RISK LEVEL	DETECTION TYPE	RISK EVENT TYPE	RISK EVENTS CLOSED	LAST UPDATED (UTC)
High	Offline	Users with leaked credentials ⓘ	44 of 45	12/7/2016 1:04 AM
Medium	Real-time	Sign-ins from anonymous IP addresses ⓘ	76 of 78	1/17/2017 2:44 PM
Medium	Offline	Impossible travels to atypical locations ⓘ	11 of 14	1/17/2017 2:44 PM
Medium	Real-time	Sign-in from unfamiliar location ⓘ	0 of 1	11/15/2016 7:18 PM
Low	Offline	Sign-ins from infected devices ⓘ	76 of 78	1/17/2017 2:44 PM

AZURE AD PASSWORD PROTECTION

7

- ▶ Traditional password policies breed bad behavior
- ▶ Azure AD Password Protection extends a banned password list to on-premises AD passwords
- ▶ Dynamically updated list of known-bad passwords/keywords
- ▶ Augment the list with keywords that you want to ban in your organization





Password Protection Demo

SIMPLIFY AND PROTECT: MFA ON-PREMISES

8

- ▶ MFA sprawl creates end-user and support pain
- ▶ 3rd party MFA solutions cost a lot of money
- ▶ NPS extension gives you Azure MFA for RADIUS clients
- ▶ Now you have Azure MFA for VPN, Citrix, RD Gateways, etc.
- ▶ Troubleshooting is not the easiest, but it generally works



STEPPING UP TO IDENTITY PROTECTION

9

- ▶ Unlocking identity protection unlocks a mountain of data
- ▶ It also brings you risk based conditional access
- ▶ Unlock the trial and try it on your data



OUTBOUND PROVISIONING

10

- ▶ IAM and governance in SaaS applications is hard
- ▶ Outbound provisioning lets you master SaaS identities with on-premises data
- ▶ Leverage security groups to map roles and access to SaaS apps
- ▶ In addition to out-of-box apps, any SCIM endpoint can be provisioned to
- ▶ Performance challenges with this feature have been significantly improved

TEN QUICK WINS

1. Self-Service Password Reset
2. Privileged Identity Mgmt.
3. App Single Sign-On
4. Azure Application Proxy
5. Conditional Access
6. Password Hash Sync
7. Azure AD Password Protection
8. MFA for On-Premises Services
9. Identity Protection
10. Outbound Provisioning

Extended Q&A



