Forcepoint DLP and Azure Active Directory secure hybrid access

Integration Guide

Forcepoint

Integration Guide

Michael Nevin 14 September 2020 Public

Table of Contents

2
3
9
15
19
27
30

Version	Date	Author	Notes
0.1	15 April 2020	Michael Nevin	First draft
0.2	05 May 2020	Neelima Rai	Updated and added Troubleshooting chapter
0.3	05 May 2020	Mattia Maggioli	Review
0.4	19 June 2020	Jonathan Knepher	Review
0.5	14 September 2020	Mattia Maggioli	Minor updates

Summary

This guide provides step by step instructions to set up an integration between **Azure Active Directory secure hybrid access** and **Forcepoint DLP**.

The integration enables access and authentication to Forcepoint Security Manager with selected Azure AD users and to expose the Forcepoint Security Manager as an Azure app for remote management.

The code and instructions provided, enable system administrators to

- → Automatically deploy Azure AD Domain Services with LDAPs
- → Configure Azure AD as an external LDAPs source into Forcepoint Security Manager
- → Deploy and configure the App Proxy component of Azure to expose Forcepoint Security Manager as an Azure App

A description of the workflow between the components involved in this POC is depicted in this diagram:



Caveats

The integration described in this document was developed and tested with the following products:

- → Forcepoint DLP version 8.7.0.360
- → Azure Active Directory

This interoperability uses:

- → Deployment Service: a service that deploys Azure AD Domain Services template
- → Azure AD Domain Services: an extension to Azure Active Directory to enable LDAPs connectivity to Azure AD
- → Azure App Proxy: a component provided by Microsoft Azure to expose on-premises web applications

Implementation options

Two implementation options are provided in this document

- 1. Docker leverages docker images where the integration component is already installed with all necessary dependencies: the user only has to edit one docker-compose environment variable file and run containers on an existing docker setup.
- 2. Traditional requires the manual deployment of the integration component inside a clean Centos 7 host-machine.

The docker images for this integration have been tested working with:

- → Docker 19.03.6
- → Docker-compose 1.25.4

while the traditional version of this integration has been tested working with the following requirements

→ Centos 7.3

In this document we assume only Azure Active Directory is already in use. If **Azure AD Domain Services** with LDAPs is in use as well, then skip the **Implementation** chapter (either **Traditional** or **Docker**) and start directly from the **Forcepoint DLP – Configure Azure AD as external identity source** chapter.

Implementation – Docker

The solution described in this chapter requires a Linux machine (Centos 7.3 recommended) within the same network of Forcepoint Security Manager host machine. This machine will be referenced in the rest of this document as the **Docker-host** machine.

The following components must be installed on the Docker-host machine:

- → Docker Engine: if Docker Engine is not installed visit <u>docker-installation-docs</u> to install Docker Engine on Docker-host
- → Docker Compose: if Docker Compose is not installed on the Docker-host machine visit <u>docker-compose-installation</u> to install Docker, Compose on Docker-host
- → The file **fp-dlp-azure-ad-ds-deployment-docker.tar.gz** available at the link <u>https://frcpnt.com/dlp-deploy-azure-ad-docker-latest</u>

The archive fp-dlp-azure-ad-ds-deployment-docker.tar.gz contains the following files:

- → docker-compose-deployment.yml: docker-compose deployment file which will be used for deploying Azure templates into Azure, create an external Active Directory authentication server and external user domain in Forcepoint Security Manager.
- \rightarrow .env: the environment variables files for docker-compose.

Step 1: Login to Docker Registry

Use the following command and credentials to login into the Docker registry hosting the containers needed for this integration

```
root@linux:~# docker login docker.frcpnt.com
Username: fp-integrations
Password: t1knmAkn19s
```

Step 2: Modify .env file

Decompress fp-dlp-azure-ad-ds-deployment-docker.tar.gz and change your directory to fp-dlp-azure-ad-ds-deploymentdocker

```
tar -zxvf fp-dlp-azure-ad-ds-deployment-docker.tar.gz
cd fp-dlp-azure-ad-ds-deployment-docker
```

Open .env file with a text editor such as vi

vi .env

Update the following variables:

- 1. **AZURE_ADMIN_LOGIN_NAME:** is your Azure administrator login name. This administrator must have a **Global Administrator** role within Azure AD
- 2. AZURE_DOMAIN_NAME: is your Azure domain name
- 3. AZURE_LOCATION: is the Azure location where all resource will be created in Azure
- 4. **AZURE_RESOURCE_GROUP_NAME:** a name for Azure resource groups, if this resource group is not existing, the deployment process will create it.
- 5. DOCKER_HOST_PUBLIC_IP_ADDRESS: is the public IP address for the Docker-host machine
- 6. **PFX_CERTIFICATE_EXPIRY_DAYS:** the duration in days of the PFX certificate, after this the certificate will expire
- 7. PFX_CERTIFICATE_PASSWORD: a password that will be used for the PFX certificate

Once all variables are edited, save the .env file and move to the next step based on your existing Active Directory setup:

- → If you already have Azure AD Domain Services with LDAPs configured, move to Step 8
- → If you already have Azure AD Domain Services without LDAPs, move to Step 5
- → If you don't have Azure AD Domain Services, continue to Step 3

Step 3: Create PFX certificate Base64 for secure LDAP

1. Run the deployment container:

docker-compose up -d

2. Generate the PFX base64 certificate:

docker-compose exec deployment /app/deployment generate-ssl-cert

3. The output of the above command is the Base65 string of the generated PFX certificate. Copy this output.

4. Stop and remove the deployment container:

docker-compose down

5. Insert the copied Base64 string as a value for PFX_CERTIFICATE_BASE64 variable in .env files variable. For example,

PFX_CERTIFICATE_BASE64=MIIQRQIBAzCCD9cGDSqGSId3DUEHSAAaCCD8gEgg/EMIIPwDCCBf.....

Step 4: Deploy Azure AD DS template

1. Run the deployment container:

docker-compose up -d

1. Interact with deployment container:

docker-compose exec deployment /bin/bash

2. Execute the following command to deploy the Azure AD DS, the application provisioning template and to create Azure groups for Forcepoint Security Manager roles:

./deployment deploy-azure

3. Enter your password for the administrator login name, then the deployment monitoring progress will start. Wait until the progress bar is completed. Provisioning of all resources inside Azure can take up to 55 minutes.

INFO[0043] Preparing for deployment	
INFO[0073] Starting Deployment	
INFO[0113] Starting Deployment Monitoring	
INFO[2347] The Template Deployment process is finished.	
INFO[2347] The Deployment for azure AD DS(corkbizdev.onmicrosoft.com) is started this process can take up to 30 minutes.	
You can u <u>s</u> e azure portal to monitor this process	
bash-5.0#	

Once finished, Azure will start configuring Azure AD DS and this deployment will take up to 30 minutes and can only be monitored through Azure Portal.

4. To monitor the ongoing deployment login to the Azure portal, search for **Azure AD Domain Services**, click on your **Azure AD Domain Services**

Home > Azure AD Domain Services	
Azure AD Domain Services	
+ Add 🚳 Manage view 🗸 🖒 Refresh 🞍 Export to CSV 🛛 🖉 Assign tags 🗍 🗢 Feedb	oack
Filter by name Subscription == all Resource group == all Location =	= all 🔕 (+ ₇ Add filter
Showing 1 to 1 of 1 records.	
Name ↑↓	Type \uparrow_{\downarrow}
A corkbizdev.onmicrosoft.com	Azure AD Domain Services

The status of the Domain Services will be Deploying

🛕 The mana	1 The managed domain is being provisioned. This operation will take a while.			
	corkbizdev.onmicrosoft.com	O Deploying View health		

Wait until the status of the Domain Services changes to Running, this can take up to 30 minutes



Once the new service is Running move to step 5.

Step 5: Enable LDAPs on existing Azure AD DS.

In this section we assume you already have an existing Azure AD Domain Service in your Azure Active Directory: the following steps show how to enable LDAPs.

Create a certificate for secure LDAP

- 1. Open a terminal
- 2. Create a private key with this command:

openssl genrsa 4096 > private.pem

3. Create a public key. Execute this command after replacing YOUR_AZURE_DOMAIN_NAME with your Azure domain name:

openssl req -x509 -days 365 -new -key private.pem -out public.pem -addext extendedKeyUsage=serverAuth,clientAuth - subj "/CN=*YOUR_AZURE_DOMAIN_NAME"

4. Create a PFX certificate. Execute this command after replacing PASSWORD with a password for FPX certificate, and store the password in a secure location as it will be used again in the next steps:

openssl pkcs12 -export -in public.pem -inkey private.pem -out azure_cert.pfx -password pass: PASSWORD

This will generate a PFX certificate named azure_cert.pfx in your current directory. This certificate will be deployed to Azure AD DS in the next steps.

Enable secure LDAP

- 1. Login to Azure portal, search for Azure AD Domain Services.
- 2. Click on your Azure AD Domain Service.
- 3. Select Secure LDAP
- 4. By default, secure LDAP access to your managed domain is disabled: toggle Secure LDAP to Enable.
- 5. Secure LDAP access to your managed domain over the internet is disabled by default. Toggle Allow secure LDAP access over the internet to Enable
- 6. Select the folder icon next to **.PFX file with secure LDAP certificate**. Browse to the path of the a**zure_cert.pfx** file, then select the certificate a**zure_cert.pfx** .
- 7. Enter the password to decrypt .PFX file: this is the password that is used when azure_cert.pfx is created.
- 8. Select Save to enable secure LDAP.



A notification is displayed that secure LDAP is being configured for the managed domain. You can't modify other settings for the managed domain until this operation is complete.

It takes a few minutes to enable secure LDAP for your managed domain.

Lockdown secure LDAP access over the internet

- 1. Click Properties, then select your network security group
- 2. On the left-hand side of the network security group pane, choose Settings > Inbound security rules
- Click Add, then create a rule to allow TCP port 636: For improved security, choose the source as IP Addresses and then specify your Docker-host machine public IP address. This is necessary to enable network connectivity to the Forcepoint SCIM service hosted on premises.

Home > Resource groups > myResource	eGroup > aadds-n	sg - Inbound security rules	Add inbound security rule ×
aadds-nsg - Inbound sec Network security group	urity rules		/ Basic
,O Search (Ctrl+/) «	+ Add 🔌	Default rules	
Overview	Priority	Name	Source * ()
Activity log	101	AllowSyncWithAzureAF	1 P AQUIDAD V
Access control (IAM)	201	AllowRD	Source IP addresses/CIDR ranges * () 131.777.787.187.1929
Tags	301	AllowPSRemoting	Saura part manar 10
Diagnose and solve problems	65000	AllowVnetinBound	*
Cattings	65001	AllowAzureLoadBalano	Destination * ()
* Johnund security rules	65500	DenyAllinBound	Any V
Outbound security rules			Destination port ranges * ①
Network interfaces			636 🗸
() Subnets			Protocol *
Properties			Any TCP UDP ICMP
A Locks			Action *
Export template			Allow Deny
Manifester			Priority * 0
			401 V
Ulagnostic settings			Name *
T NG flow loor			Any mapping V
Noo now logs			Description
Support + troubleshooting			
Effective security rules			
Rew support request			
			Add

4. Click Add to save and apply the rule.

Step 6: Enable Azure AD Domain Services password hash synchronization

When Azure AD Domain Service is deployed for the first time, it does not contain any password hash for the existing users within Azure AD, therefore users intended to be used for Forcepoint Security Manager authentication must have their password changed before authentication in Forcepoint Security Manager will work.

The password change process will store password hashes inside Azure AD Domain Services so that users authenticating through LDAPs from Forcepoint Security Manager and other applications will be verified in a secure way. The preferred method to have password changes is left to the Azure AD administrator implementing this integration: for example, manually expiring the passwords of all users who will use the Forcepoint Security Manager integration (this will force a password change upon a new sign-in attempt) or instructing users to manually change their password at their preferred schedule.

Manually password changing:

- 1. Go to the Azure AD Access Panel page at https://myapps.microsoft.com
- 2. In the top-right corner click on your name then choose **Profile** from the drop-down menu.

Microsoft	Dee Dee Dee Dee Dee Dee Default Directory
Apps	Dee Riley driley@contoso.onmicrosoft.com
	Apps
	Groups
	Profile
	ORGANIZATIONS ද
	Default Directory
	Sign out

- 3. On the Profile page, select Change password.
- 4. On the Change password page enter your existing (old) password, then enter and confirm a new password.
- 5. Select Submit.

Wait 10 minutes after the password change has been completed (including the password of the user with Global Administrator role within Azure AD) then proceed to the next step (Forcepoint DLP – Configure Azure AD as external identity source).

Implementation - Traditional

The solution described in this chapter requires

- → A Centos 7.3 machine able to reach the Forcepoint Security Manager host machine over the network. This will be referenced in the rest of this document with the name **host-machine**.
- → The source files for this implementation, contained in the archive fp-dlp-azure-ad-ds-deployment.tar.gz available at the link <u>http://frcpnt.com/dlp-deploy-azure-ad-latest</u>

The archive fp-dlp-azure-ad-ds-deployment.tar.gz contains the following files and folders:

- → **deployment**: the deployment application for deploying templates to Azure, creating external Active Directory authentication server and external users' domain in Forcepoint Security Manager.
- → deployment.yml: the configuration file for the deployment application.
- → installation_script.sh: a bash script to install all required dependencies.

Step 1: Modify configuration files

Inside the **host-machine** unpack the **fp-dlp-azure-ad-ds-deployment.tar.gz** archive and change your directory to **fp-dlp-azure-ad-ds-deployment**

tar -zxvf fp-dlp-azure-ad-ds-deployment.tar.gz

cd fp-dlp-azure-ad-ds-deployment

Modify deployment.yml file

The contents of **deployment.yml** file are as follows:

AZURE_ADMIN_LOGIN_NAME: INSERT_YOUR_AZURE_ADMINISTRATOR_LOGIN_NAME_HERE
DOMAIN_NAME: INSERT_YOUR_AZURE_DOMAIN_NAME_HERE
LOCATION: INSERT_AZURE_LOCATION_HERE
DOMAIN_SERVICES_VNET_NAME: domain-services-vnet
DOMAIN_SERVICES_VNET_ADDRESS_PREFIX: 10.0.0.0/16
DOMAIN_SERVICES_SUBNET_NAME: domain-services-subnet
DOMAIN_SERVICES_SUBNET_ADDRESS_PREFIX: 10.0.0.0/24
NGINX_PUBLIC_IP_ADDRESS: INSERT_YOUR_HOST_MACHINE_PUBLIC_IP_ADDRESS
LOGGER_JSON_FORMAT: false
RESOURCE_GROUP: INSERT_AZURE_RESOURCE_GROUP_NAME_HERE
<pre>DEPLOYMENT_TEMPLATE: /root/fp-dlp-azure-ad-ds-deployment/azure_smc_template.json</pre>
PFX_CERTIFICATE_EXPIRY_DAYS: INSERT_NUMBER_OF_DAYS_FOR_PFX_CERTIFICATE_EXPIRATION_HERE
PFX_CERTIFICATE_PASSWORD: INSERT_A_PASSWORD_FOR_PFX_CERTIFICATE_HERE
PFX_CERTIFICATE_BASE64: PFX_BASE64_WILL_BE_INSERTED_HERE

Open deployment.yml file with a text editor such as vi and do the following steps.

- 1. Replace **INSERT_YOUR_AZURE_ADMINISTRATOR_LOGIN_NAME_HERE** with your Azure Administrator login name, this administrator most have **Global administrator** role.
- 2. Replace INSERT_YOUR_AZURE_DOMAIN_NAME_HERE with your Azure Domain Name
- 3. Replace INSERT_AZURE_LOCATION_HERE with an Azure region. All Azure resources will be created in this location
- 4. Replace INSERT_YOUR_HOST_MACHINE_PUBLIC_IP_ADDRESS with the public address of the host-machine.
- Replace INSERT_AZURE_RESOURCE_GROUP_NAME_HERE with your Azure resource group name, if the resource group name does not exist it will be created.
- 6. Replace INSERT_NUMBER_OF_DAYS_FOR_PFX_CERTIFICATE_EXPIRATION_HERE with the number of days for PFX certificate to be expired
- 7. Replace **INSERT_A_PASSWORD_FOR_PFX_CERTIFICATE_HERE** with a password that will be used as a password for the PFX certificate.

Save the deployment.yml file, and move to the next step

Step 2: Install dependencies

Execute the following command to make installation_script.sh executable

chmod +x installation_script.sh

installation_script.sh will install the following packages:

- → Python3
- → Golang 1.14
- \rightarrow Azure CLI
- \rightarrow OpenSSL (upgrade to the latest version)

Execute installation_script.sh

sudo ./installation_script.sh

The installation takes about 30 minutes.

Step 3: Create PFX certificate Base64 for secure LDAP

Skip this step if you have Azure AD Domain Services already deployed in your Azure Active Directory.

- 1. Make sure you are inside **fp-dlp-azure-ad-ds-deployment** directory.
- 2. Run the following command which will generate a Base64 string of PFX certificate.

./deployment generate-ssl-cert --config ./deployment.yml

3. Copy the output of the above command and use it to replace the placeholder PFX_BASE64_WILL_BE_INSERTED_HERE in the deployment.yml file

Step 4: Deploy Azure AD DS template

If Azure AD Domain Services is already deployed in Azure Active Directory, skip this step and move to step 5.

1. Execute the following command to deploy the Azure AD DS:

./deployment deploy-azure --config ./deployment.yml

- 2. Enter your password for the administrator login name displayed on screen:
- 3. The deployment monitoring progress will start, wait until the progress bar is completed: this can take up to 55 minutes.
- 4. Once the above template deployment has finished, Azure will start deploying Azure AD DS and this deployment will take up to 30 minutes and can only be monitored through Azure Portal.
- 5. Login to the Azure portal, search for Azure AD Domain Services.
- 6. Click on your Azure AD Domain Services

Home > Azure AD Domain Services	
Azure AD Domain Services	
🕂 Add 🛞 Manage view 🗸 🖒 Refresh 🞍 Export to CSV 🛛 🖉 Assign tags 🗠	\heartsuit Feedback \rightleftharpoons Leave preview
Filter by name Subscription == all Resource group == all	ocation == all 💿 (+ Add filter)
Showing 1 to 1 of 1 records.	
Name ↑↓	Type ↑↓
A corkhizdev anmicrosoft com	Azure AD Domain Services

The initial status of the Domain Services will be Deploying

🛕 The mana	aged domain is being provisioned. This operation will take a while.	
	corkbizdev.onmicrosoft.com	Deploying View health

Wait until the status of the Domain Services changes to Running, then move to step 6.



Step 5: Enable LDAPs on existing Azure AD DS.

In this section we assume you already have an existing Azure AD Domain Service in your Azure Active Directory: the following steps show how to enable LDAPs.

Create a certificate for secure LDAP

- 1. Open a terminal
- 2. Create a private key with this command:

openssl genrsa 4096 > private.pem

3. Create a public key. Execute this command after replacing YOUR_AZURE_DOMAIN_NAME with your Azure domain name.

openssl req -x509 -days 365 -new -key private.pem -out public.pem -addext extendedKeyUsage=serverAuth,clientAuth - subj "/CN=*YOUR_AZURE_DOMAIN_NAME"

4. Create a PFX certificate. Execute this command after replacing PASSWORD with a password for FPX certificate, and store the password in a secure location as it will be used again in the next steps

openssl pkcs12 -export -in public.pem -inkey private.pem -out azure_cert.pfx -password pass: PASSWORD

This will generate a PFX certificate named **azure_cert.pfx** in your current directory. This certificate will be deployed to Azure AD DS in the next steps.

Enable secure LDAP

- 1. Login to Azure portal, search for Azure AD Domain Services.
- 2. Click on your Azure AD Domain Service.
- 3. Select Secure LDAP
- 4. By default, secure LDAP access to your managed domain is disabled: toggle Secure LDAP to Enable.
- 5. Secure LDAP access to your managed domain over the internet is disabled by default. Toggle Allow secure LDAP access over the internet to Enable
- 6. Select the folder icon next to **.PFX file with secure LDAP certificate**. Browse to the path of the a**zure_cert.pfx** file, then select the certificate **azure_cert.pfx** .
- 7. Enter the password to decrypt .PFX file: this is the password that is used when **azure_cert.pfx** is created.
- 8. Select Save to enable secure LDAP.

aaddscontoso.com Secure LDAP				
	🗟 Save 🗙 Discard 🖉 Change Certificate			
Overview Control (IAM)	Secure LDAP Disabled Thumbprint Not available	Allow secure LDAP access over the internet Disabled Certificate expires Not available		
Settings	a	~	_	
Properties	Secure LDAP O			
Secure LDAP	Allow secure LDAP access over the internet ① Disable Enable			
Synchronization				
⊗ Health	Upload a .PFX file containing the certificate to be used for secure LDAP access to this managed domain			
Q Notification settings	DEV file with conurs I DAD contificate X			
(§) SKU	"azure-ad-ds.pfx"			
Monitoring	Password to decrypt .PFX file * ①			
Diagnostic settings	·······			
😭 Logs				
Workbooks	Your subnet is protected by network securit configured with proper IP ranges on the network	y group aadds-nsg. To give user access to secure LDAP endpoint, please ensure "Allow" rule on port 636 is twork security group.		
Support + troubleshooting				

A notification is displayed that secure LDAP is being configured for the managed domain. You can't modify other settings for the managed domain until this operation is complete.

It takes a few minutes to enable secure LDAP for your managed domain.

Lockdown secure LDAP access over the internet

- 1. Click **Properties**, then select your network security group.
- 2. On the left-hand side of the network security group pane, choose Settings > Inbound security rules.
- Click Add, then create a rule to allow TCP port 636: for improved security, choose the source as IP Addresses and then specify your Docker-host machine public IP address. This is necessary to enable network connectivity to the Forcepoint SCIM service hosted on premises.

Home > Resource groups > myResource	eGroup > aadds-ns	sg - Inbound security rules	Add inbound security rule ×
aadds-nsg - Inbound sec	urity rules		> asols-rog
P Search (Ctrl+/)	+ Add 🔌	Default rules	¢ 1001
			Source * ①
💎 Overview	Priority	Name	IP Addresses 🗸 🗸
Activity log	101	AllowSyncWithAzureAE	Source IP addresses/CIDR ranges * 🛈
R Access control (IAM)	201	AllowRD	131:11.00.000
🔷 Tags	301	AllowPSRemoting	Source port ranges * 🕢
Diagnose and solve problems	65000	AllowVnetin8ound	*
Settings	65001	AllowAzureLoadBalance	Destination * 🕢
📩 Inbound security rules	65500	DenyAllinBound	Any 🗸
- Outbound security rules			Destination port ranges * 🛈
Network interfaces			636
 Subnets 			Protocol *
Properties			Any COP COP
🔒 Locks			Action *
Export template			Priority # ()
Monitoring			401
Diagnostic settings			Name *
👷 Logs			AllowLDAPS 🗸
NSG flow logs			Description
Support + troubleshooting			
Effective security rules			
📯 New support request			
			Add

4. Click Add to save and apply the rule

Step 6: Enable Azure AD Domain Services password hash synchronization

When Azure AD Domain Service is deployed for the first time, it does not contain any password hash for the existing users within Azure AD, therefore users intended to be used for Forcepoint Security Manager authentication must have their password changed before authentication in Forcepoint Security Manager will work.

The password change process will store password hashes inside Azure AD Domain Services so that users authenticating through LDAPs from Forcepoint Security Manager and other applications will be verified in a secure way. The preferred method to have password changes is left to the Azure AD administrator implementing this integration: for example manually expiring the passwords of all users who will use the Forcepoint Security Manager integration (this will force a password change upon a new sign-in attempt) or instructing users to manually change their password at their preferred schedule.

Manually password changing:

- 1. Go to the Azure AD Access Panel page at https://myapps.microsoft.com
- 2. In the top-right corner, select your name, then choose Profile from the drop-down menu.

Microsoft	Dee Dee Default Directory
Apps Azure portal	Apps Groups Profile
	ORGANIZATIONS 🔅 Default Directory Sign out

- 3. On the Profile page, select Change password.
- 4. On the Change password page, enter your existing (old) password, then enter and confirm a new password.
- 5. Select Submit.

Wait 10 minutes after the password change has been completed (including the password of the user with Global Administrator role within Azure AD) then proceed to the next step.

Forcepoint DLP – Configure Azure AD as external identity source

In order to configure Azure AD as an external source do as follows:

1. Log into your local Forcepoint Security Manager using your local admin credentials.

	33346	
		Same to
	FORCEPOINT Security Manager	
	Version 8.5	
	admin	
	A	
	Forgot my password	Log On

2. Click the gear in the top right corner to access the settings page.

DATA				*	۰	0
			Role: Super Administrator	Ĭ	Г	Deploy
Main ^	Dashboard					
~						æ Re
Status	Health Alert Summary	Business Value - Data collected o	ver the last 24 hours (approximate)			
ຟ Reporting ₩ ↓	Your subscription is valid 4 data loss prevention and mobile policies are configured	Inspected Web traffic: Inspected email messages: Messages delivered to mobile devices:	0 (0 MB) 0 (0 MB) 0 (0 MB)			
Policy Management	No discovery, policies are configured Imissing essential configurations	Endpoints: Synchronized mobile devices:	0 (0 мв) 0 of 0 are enabled (08 Apr. 2020, 11:56 AM) 0			
Logs	Data Loss Prevention - Incidents collected over the last 24 hours					
Settings ^	Incidents by Severity	Top 5 Policies				
Çeneral	No Data Found		No Data Found			

3. Move your mouse over the General tab and reveal the roll over menu, click User Directory tab

SETTING	s 🗸	
Global	My Account	
Settings A	View your privileg	es or update your password.
۰.	My Account	
General	User Directory	
	Administrators	admin
		admin@go4labs.net
	Notifications	Global Security Administrator
	Two-Factor Auth	
	Audit Log	sword
	For a strong pas	sword, enter more than 8 characters with one or more capital letter, lower case letter, spe

- 4. Fill in the details to connect to the Azure Active Directory as follows:
 - User directory server: Set this to Active Directory
 - **IP address or hostname**: The public IP address or FQDN of your Azure AD, this can be found in the **Properties** section of **Azure AD Domain Services**.
 - **User distinguished name**: This should be the distinguished name of an account with admin access to the Azure AD. Format for this field is similar to:

CN=test.dlp@corkbizdev.onmicrosoft.com,OU=AADDC Users,DC=corkbizdev,DC=onmicrosoft,DC=com

For more information on distinguished name refer to: https://docs.microsoft.com/en-us/previous-versions/windows/desktop/ldap/distinguished-names

- o Password: the password of the account that has admin access to the Azure AD
- Use SSL encryption: make sure this is ticked for Azure Active Directory

SETTING	S Role:
Global	User Directory
ettings ^	Configure the LDAP user directory to use when adding and authenticating Security Manager administrators with network accounts.
	The user directory used for defining end users is configured within each Security Manager module.
ral	User directory server:
	IP address or hostname: Port 636
	User distinguished name: CN=test.dlp@corkbizdev.onmicr
	Example: domain\username
	Password: Test Connection
	Root naming context:
	This field is optional. Example: OU=Department, DC=DomainComponent, DC=Com
	Perform additional nested group search
	V Use SSL encryption
	Do you want to follow referrals returned by the directory service?
	Follow referrals

Click **OK** when you are done.

5. After you have successfully added the Active Directory mouse over **General** and select **Administrators** from the roll over menu



6. From here select Add Network Account in the bottom right.

Global Adn	ministrators					
otobat	initiation and a second s					
Settings ^						a Refresh
General Add	or delete Security Manager administrators and assign them permi	ssions.				
	User Name	Туре	Email Address	Role		
	admin	Local	admin@go4labs.net	Global Security Adn	ninistrator	
	DLP Administrator	Network		Global Security Adn	ninistrator	
	a Operator	Network		Global Security Adn	ninistrator	
				Add Local Account	Add Network Account	Delete

7. From here you can search for the Azure AD user or groups you want to assign permissions to on the Forcepoint Security Manager. Once you have selected the users or groups, use the arrow icon to add it to the selected accounts box.

F SETTING	55 👻					# ¢	0	
					Role: Global S	curity Admin	nistrator	
Global	Administrators > Add Network Account							
Settings 🔨	Add one or more administrators from the LDAP user d	irectory defined on the User Directory the users to add	page.					^
General	Users must have an email address in the directory to b	be found.						
	Directory Search							
	Search: dlp X Q Refine se	arch						
	Search results: 1 accounts found for 'dlp'			Selected accounts:				
-	Display Name	DLP Administrator	Email Address	Display Name				4
	Global Security Administrator	a configuration and account administr	ation (Sunor Administrator) sottings for a	Security Manager modules				
	 Notify administrator of the new account via email. Email notifications are not sent to members of netw 	ork group accounts.	auon (Super Hummistrator) settings for a	Security manager modules.				
	A SMTP server configuration is missing, cannot send	l email						
	Module Access Permissions							
	Assign permissions to this administrator. Global Sec by assigning administrators to a role, or granting th	curity Administrators have Super Admin em module-specific permissions,	nistrator access to all Security Manager r	odules. To limit access, select an access level for each mod	ule listed. Super Administrators can fine-tune priv	ileges withir	a modul	e 🖕
	, , , , , , , , , , , , , , , , , , , ,					ок	Ca	ncel

Click **OK** at the bottom right of the screen.

Forcepoint DLP – Configure Azure Application proxy

Azure Application proxy is the component provided by Azure to expose your local web application through Azure. To register Forcepoint DLP into Application proxy follow these steps:

1. From the Azure portal navigate to the Azure Active Directory

≡	Microsoft Azure		𝒫 azure act			\times	⊵	Ģ	D ©
	Azu	ire ser	Services	See all	Marketplace				
			Azure Active Directory		Azure Active Directory B2C				
		+	🧭 Azure Cosmos DB		🖄 Azure Active Directory		SQL		\rightarrow
	c	Create a	Azure Database for MySQL servers		Kelverion Runbook Studio for Azure Automation v3.4		. datab	ases	More servic
	n	resource	Activity log		Documentation See a	ai -			
			🛤 Azure Arc		Create an Azure Active Directory tenant Microsoft Docs				
	Rec	ont ro	寒 Azure Databricks		Azure Enterprise enrollment invoices Microsoft Docs				
	Rec	entre	Azure AD B2C		RelvingParty - Azure Active Directory B2C Microsoft Docs				
	Name	e	Azure AD Security		What is Azure Application Gateway Microsoft Docs	a	st Viev	ved	
	[i] fo	forcepoir	🖬 Azure NetApp Files		D	r	ninute	s ago	
	🎈 d	domain-s	🔶 Azure AD Authentication methods		No results were found.	v	veek a	go	
	(e) c	corkbizde	Resources			v	veeks a	ago	
	[9] N	Network\	No results were found.			v	veeks a	ago	
			Searching all subscriptions. Change					-	

2. In the left pane select Application proxy



3. Click Download connector service and install it on the Forcepoint Security Manager machine.

sctory	-	
(Ctrl+/) «	Solution	
v started	Application proxy provides single sign-on (SSO) and secure remote acceleration proxy	ess fo
e and solve problems	Connectors	
-	Connectors establish a secure communication channel between your on-pren	nise
	$+$ New Connector Group \downarrow Download connector service	
	Groups IP	,
itional relationships	▲ ∨Default	

4. Then click Accept Terms & Download.

	Application Proxy Connector Download
	Azure Active Directory Inside your network and the Application moxy, only
	one installation is necessary to service all your
Disable application proxy + Configure an app	published applications; a second connector can be installed for high availability purposes.
• Application provider single sign on (SSO) and secure remote access for web application	System Requirements
Learn more about Application Proxy	
	Operating Systems Windows Server 2012 R2
· · · · · · · · · · · · · · · · · · ·	 Windows Server 2012 K2 Windows Server 2016
onnectors	 Make sure the network is configured correctly
onnectors establish a secure communication channel between your on-premises network and A	for the connector. Learn about the requirements
+ New Connector Group 🛓 Download connector service	 The connector must have access to all on premises applications that you intend to
Groups IP	publish.
	Installation Instructions
V Verault	To install the Application Proxy connector, download
fsm	the connector installation package and install it on a
▲ ∨dlp	local, designated machine. For more information on the Application Proxy connector, see our online content.
	By downloading the connector, you accept our
	Terms of Service.
	Accept terms & Download

5. After the installation is completed you should see the IP address of the registered machine in the list of **Connectors** of the **Application proxy**:

🚫 Disable application proxy	+ Configure an app		
Application proxy provide Learn more about Application	es single sign-on (SSO) and ation Proxy	secure remote access for web appli	ications hosted on-premises.
Connectors Connectors establish a secure of + New Connector Group	communication channel be	tween your on-premises network ar service	nd Azure.
Groups		IP	Status
❶ ✓ Default			
fsm		94,25,168,168	Active

This shows that the **Application proxy** installed in the Forcepoint Security Manager machine has successfully connected to the Azure.

Next step is configuring the **Application proxy** hosted on the Forcepoint Security Manager machine to connect locally to Forcepoint Security Manager. The Application proxy **can only connect to local applications using an FQDN:** if your Forcepoint Security Manager is installed with the service binded to the IP address of the hosting machine, see the **Appendix** for two ways to address this.

Once the Forcepoint Security Manager is reachable using a FQDN, proceed with the following steps.

6. Back on the Application proxy page on Azure click Configure an app

New Connector Group	eq Download connector service		
connectors connectors establish a secure	communication channel between y	your on-premises netwo	ork and Azure.
Application proxy provic Learn more about Applic	les single sign-on (SSO) and secure ation Proxy	remote access for web	applications hosted on-premises.
, chable application provi			

7. Configure the **Basic Settings** and **Advanced Settings** as follows

- Name: name the app being configured with the Application proxy
- o Internal URL: enter the FQDN of the Forcepoint Security Manager including the port
- External URL: use https and define part of the FQDN, the last part of the URL will be the Azure AD name
- Set Pre-Authentication as Passthrough
- Connector group: this is the group your connector is in, by default is Default
- Backend Application Timeout: leave this Default
- o Translate URLs In
 - Headers: No
- Leave everything else default

$+$ Add \times Discard
Application proxy provides single sign-on (SSO) and secure remote access for web applications hosted on-premises. Learn more about Application Proxy
Basic Settings
Name * 🗊 DLP Application Proxy 🗸
Internal Url * (i) https://fsm.local:9443/
https:// V dlpapplicationproxy / -corkbizdev.msappproxy.net/ V
External Url 🕦 https://dlpapplicationproxy-corkbizdev.msappproxy.net/
Pre Authentication
Connector Group () Default
Additional Settings
Backend Application Timeout ① Default ~
Use HTTP-Only Cookie 🔞 Yes No
Use Secure Cookie 🗊 Yes No
Use Persistent Cookie 🗊 Yes No
Translate URLs In
Headers ① Yes No
Application Body () Yes No

8. Click Add in the top left corner.

After the page has been created you will be directed to a page **App name | Overview** (in the example above, the app name is DLP Application Proxy).

9. Go to Application Proxy under Manage on the left. Click Test Application and Open Application to verify all settings work correctly: you will be able to reach the Forcepoint Security Manager application from the public FQDN provided by Azure.

Provisioning access to on-premise Forcepoint Security Manager via Azure application

Users assigned to your Forcepoint Security Manager Azure app can use your Azure to access Forcepoint Security Manager on-promise with the following steps:

1. From the Microsoft Azure portal search for Enterprise applications

	𝒫 enterp		×	\sum	Ŗ	1
Azuro sor	Services	Marketplace	See all			
/ Eure ser	Enterprise applications	👛 VIDIZMO EnterpriseTube				
	Security Center	🖄 MessageSolution EnterpriseEmailArchive				
Create a	🚀 Quickstart Center	Conductor4SQL		Storage		м
resource	Bing Maps API for Enterprise	🚊 E-mail Converter		accounts		
	Managed applications center (preview)	Documentation				
Recent re	L. Integration accounts	Cannot connect with RDP to a Windows VM in Azure				
Name	Resources	Resource Groups		ast Viewer	J	
() forcepoir	No results were found.	No results were found.		days ago	1	
() forcepoir	Searching all subscriptions. Change	resource group	U	days ago		

2. Select the name of the application you created in previous steps of this guide (in the example below, the app name is **DLP Application Proxy**)

+ New application ≡≡ Colur	nns	
Try out the new Enterprise Apps :	earch preview! Click to enable the preview	$a \rightarrow$
Application Type Enterprise Applications	Applications status Any	Application visibility Any
First 50 shown, to search all of your	applications, enter a display name or t	he application ID.
Name	Homepage URL	
Azure DevOps	http://azure.com	ı/devops
😙 azure-fba	_	
DLP Application Proxy	https://dlpapplic	ationproxy-corkbizdev.msappproxy.net/
Forcepoint Graph API Inte	gration	

3. From this page select 1. Assign users and groups.





4. Select Add user

- 5. From this page you can select groups of users or individual users. Shown below is the same group we added to the Forcepoint Security Manager. All users belonging to this group will have access to this application.

Home > Enterprise applications All applications > DLP Application Proxy Users and groups > Add Assignment	Users and groups $ imes$
Add Assignment Forcepoint	۸ dlp (×
Users and groups > None Selected	DLP Administrator Selected
Select Role > User	dlp test test.dlp@corkbizdev.onmicrosoft.com
	Selected items DA DLP Administrator
Assign	Select

6. Finally click Assign.

ome $>$ Enterprise applications All applications $>$ DLP Application Proxy Users and group	ps 🗧 Add Assignment
Add Assignment	
Users and groups 1 group selected.	>
Select Role	>



Access via My Azure Applications

- 1. Login to <u>https://myapplications.microsoft.com/</u> with a user assigned or belonging to a group that was assigned to the Forcepoint Security Manager application.
- 2. Find your Azure app and click on it. This will redirect your web browser to Forcepoint Security Manager on-premise.

3. Enter your Azure credentials: the username is the part before the @ symbol in your Azure email address

Example

If your username is test.dlp@myazuredirectory.com then the username is test.dlp

FC Sec	RCEPOINT urity Manager	
/ersi	on 8.5	
2	test.dlp	
•	Password	

Troubleshooting

Follow these steps to identify issues impacting the normal operation of the integration described in this document.

Docker Implementation

Validate the prerequisites

Make sure the prerequisites described in the Summary chapter are all satisfied:

→ Check the version of Forcepoint DLP in use is listed as compatible

Forcepoint DLP version 8.7.0.360

- → Docker images for this integration have been tested with
 - Docker 19.03.6

Docker-compose 1.25.4

- → The docker implementation has been tested on a Centos 7.3 machine
- → User needs sudo permissions in the docker host machine
- \rightarrow Check the user can download the file with the below command:

wget --content-disposition https://frcpnt.com/dlp-deploy-azure-ad-docker-latest

Check network connectivity

Make sure firewalls or other security appliances are not impacting the network connectivity necessary for the operation of all components involved into this integration:

→ Check the docker host machine can be accessed via its public IP address or its public DNS name: execute the following command on any machine:

ping -c 2 YOUR_DOCKER_HOST_PUBLIC_IP_ADDRESS

replacing YOUR_DOCKER_PUBLIC_IP_ADDRESS with the public IP of the docker host machine. Once done check the result is similar to below:

```
PING YOUR_DOCKER_HOST_PUBLIC_IP_ADDRESS.url (10.10.120.12) 56(84) bytes of data.
64 bytes from 10.10.120.12 (10.10.120.12): icmp_seq=1 ttl=128 time=179 ms
64 bytes from 10.10.120.12 (10.10.120.12): icmp_seq=1 ttl=128 time=181 ms
```

→ Check the docker host machine has connectivity to Forcepoint Security Manager: execute the following command on docker host machine:

ping -c 2 FSM_PRIVATE_IP_ADDRESS

replacing the FSM_PRIVATE_IP_ADDRESS with your Forcepoint Security Manager private IP address or the hostname. Once done check the result is similar to below:

PING FSM_PRIVATE_IP_ADDRESS.url (10.10.120.12) 56(84) bytes of data. 64 bytes from 10.10.120.12 (10.10.120.12): icmp_seq=1 ttl=128 time=179 ms 64 bytes from 10.10.120.12 (10.10.120.12): icmp_seq=1 ttl=128 time=181 ms

Check dependencies are installed

Make sure the software dependencies needed by the components involved into this integration are installed:

→ Check all dependencies are installed: execute the following command on docker host machine to check dockercompose is installed: docker-compose --version

Check the output presents a version of 1.25.4 or higher (example below):

docker-compose version 1.25.4, build 8d51620a

 \rightarrow Check the host machine has docker installed: Execute the following command on the host machine:

docker info

Check the first few lines of the output are similar to below:

Client: Debug Mode: false

Server: Containers: 3 Running: 2 Paused: 0 Stopped: 1 Images: 3 Server Version: 19.03.8

Check all components are configured and running properly

Make sure the products and services involved into this integration are configured as expected and they are running:

 \rightarrow Check the domain service is successfully running in Azure



Traditional Implementation

Validate the prerequisites

Make sure the prerequisites described in the **Summary** chapter are all satisfied:

→ Check the version of Forcepoint DLP in use is listed as compatible

Forcepoint DLP version 8.7.0.360

- \rightarrow This integration requires to be run on a CentOS 7.3 machine
- → User needs sudo permissions for installing necessary certificates and keys
- → Check the user can download the file with the below command:

wget --content-disposition http://frcpnt.com/dlp-deploy-azure-ad-latest

Check network connectivity

Make sure firewalls or other security appliances are not impacting the network connectivity necessary for the operation of all components involved into this integration:

→ Check the host machine can be accessed via its public IP address or its public DNS name: execute the following command on any machine:

ping -c 2 YOUR_HOST_MACHINE_PUBLIC_IP_ADDRESS

replacing the YOUR_HOST_MACHINE_PUBLIC_IP_ADDRESS with the public IP of the host machine. Once done check the result is similar to below:

```
PING YOUR_ HOST_MACHINE_PUBLIC_IP_ADDRESS.url (10.10.120.12) 56(84) bytes of data.
64 bytes from 10.10.120.12 (10.10.120.12): icmp_seq=1 ttl=128 time=179 ms
64 bytes from 10.10.120.12 (10.10.120.12): icmp_seq=1 ttl=128 time=181 ms
```

→ Check the Centos 7.3 host machine can reach the Forcepoint Security Manager host machine over the network: execute the following command on host machine:

ping -c 2 FSM_PRIVATE_IP_ADDRESS

replacing the FSM_PRIVATE_IP_ADDRESS with your Forcepoint Security Manager private IP address or the hostname. Once done check the result is similar to below:

PING FSM_PRIVATE_IP_ADDRESS.url (10.10.120.12) 56(84) bytes of data. 64 bytes from 10.10.120.12 (10.10.120.12): icmp_seq=1 ttl=128 time=179 ms 64 bytes from 10.10.120.12 (10.10.120.12): icmp_seq=1 ttl=128 time=181 ms

Check dependencies are installed

Make sure the software dependencies needed by the components involved into this integration are installed:

 \rightarrow Check all dependencies are installed: execute the following command on host machine to check go is installed:

go version

Check the output is similar to below:

go version go1.14.1 linux/amd64

→ Check Azure CLI is installed: Execute following command on host machine:

az version

Check the output is similar to below:

```
{

"Azure-cli": "2.3.1",

"Azure-cli-command-modules-nspkg": "2.0.3",

"Azure-cli-core": "2.3.1",

"Azure-cli-nspkg": "3.0.4",

"Azure-cli-telemetry": "1.0.4",

"extensions": {}
```

→ Check openssl is installed: Execute following command on host machine:

openssl version

Check the output is similar to below:

OpenSSL 1.0.2k-fips 26 Jan 2017

→ Check python3.6 is installed: Execute following command on host machine:

python3 --version

Check the output is similar to below:

Python 3.6.8

Check all components are configured and running properly

Make sure the products and services involved into this integration are configured as expected and they are running:

Check the domain service is successfully running in Azure

corkbizdev.onmicrosoft.com

Running

View health

Appendix – Mapping an IP address to an FQDN

If the Forcepoint Security Manager was installed binding the service to the IP address of the machine rather to the hostname, one extra step is necessary in order to configure the **Application proxy** with the Forcepoint Security Manager. This can be accomplished by either

→ Adding a static entry to the end of the hosts file located in C:\Windows\System32\drivers\etc so the Application proxy can locally resolve the hostname of Forcepoint Security Manager to the IP (private IP address) of the Forcepoint Security Manager machine. As highlighted in the screenshot below:



→ If a local DNS server is available, adding a proper entry in the DNS server for the Forcepoint Security Manager machine which resolves to the private IP of the Forcepoint Security Manager machine itself

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint is the global human-centric cybersecurity company transforming the digital enterprise by continuously adapting security response to the dynamic risk posed by individual users and machines. The Forcepoint human point system delivers risk-adaptive protection to continuously ensure trusted use of data and systems. Based in Austin, Texas, Forcepoint protects the human point for thousands of enterprise and government customers in more than 150 countries.

© 2020 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. All other trademarks used in this document are the property of their respective owners.