IBM MaaS360 Email Access Gateway (EAG)

ActiveSync Reverse Proxy

Contents

Introduction	4
Version History	4
MaaS360 Email Access Gateway Deployment	5
Implementation Use-cases	6
Requirements and pre-requisites:	8
General Requirements	8
Requirements for EAG implementation scenarios:	9
Scenario #1: Any ActiveSync Client	9
Scenario #2: MaaS360 Secure Mail Only	9
Scenario #3: User Identification with LDAP Federation	9
Scenario #4: User Identification with Cloud Extender Identity Certificate	9
Scenario #5: Kerberos Constrained Delegation	. 10
Supported Corporate directories:	. 10
Deploying MaaS360 Email Access Gateway (EAG):	. 11
Step 1: Download Media from MaaS360 Portal	. 11
Step 2: Deploy Virtual Appliance	. 11
Step 3: Install Firmware	. 11
Step 4: Configure Virtual Appliance	. 12
Step 5: Login to Web Management Interface	. 17
Step 6: Configure Data Interface	. 18
Step 7: Activate Reverse Proxy	. 20
Step 8: Configure Runtime Component	. 22
Step 9: Set up Reverse Proxy	. 24
Step 10: Disable Basic Authentication	. 26
Step 11: Import SSL Certificates of Mail Server	. 27
Step 12: Create Junction	. 28
Step 13: Import SSL Certificate for Public Connection	. 31
Step 14: Validating Setup	. 34
Deployment Scenarios:	. 36
Scenario 1: Any ActiveSync Client	. 36
Use-case:	. 36
Workflow:	. 36
EAG Configuration:	. 36
MaaS360 Configuration:	. 39
Scenario 2: MaaS360 Secure Mail only	. 41

	Use-case:	. 41
	Workflow:	. 41
	EAG Configuration:	. 41
	MaaS360 Configuration:	. 44
S	cenario 3: User Identification with LDAP Federation	. 45
	Use-case:	. 45
	Workflow:	. 45
	EAG Configuration:	. 45
	Connecting to LDAP over SSL	. 51
	MaaS360 Configuration:	. 54
S	cenario 4: User Identification with Cloud Extender Identity Certificate	. 55
	Use-case:	. 55
	Workflow:	. 55
	MaaS360 Cloud Extender Configuration:	. 56
	EAG Configuration:	. 60
	EAG Federation Configuration:	. 65
	MaaS360 Configuration:	. 65
S	cenario 5: Kerberos Constrained Delegation	. 67
	Use-case:	. 67
	Workflow:	. 68
	EAG Configuration:	. 68
	MaaS360 Configuration:	. 76

Introduction

MaaS360 Email Access Gateway (EAG) is a secure, scalable and high-performance enterprise grade reverse proxy solution that controls the ActiveSync traffic flow to a corporate email environment. ActiveSync is a communication protocol developed by Microsoft that allows synchronization of data for emails, calendar, contacts, notes and tasks to and from a corporate messaging server for mobile devices. Most email clients use the ActiveSync protocol to synchronize data as does MaaS360 Secure Mail.

MaaS360 EAG helps organizations secure the email environments by leveraging enhanced access control mechanisms by means of allowing only authorized and compliant devices to connect and receive email. In case of on-premises email environments (email server within the corporate network), MaaS360 EAG enables end users to securely access emails on mobile devices without requiring the exposing of the mail environment to the internet.

The features of MaaS360 Email Access Gateway (EAG) are:

- reverse proxy for ActiveSync traffic for email environments
- security for both cloud and on-premises email environments
- ability to restrict access to specific email client (MaaS360 Secure Mail)
- ability to restrict access to only devices that are enrolled in MaaS360
- enhanced security schemes in addition to email authentication

<u>Note</u>:

MaaS360 Email Access Gateway (IBM Security Verify Access) can be used to only proxy connections from mobile devices managed by IBM MaaS360 to enterprise email servers

Microsoft Outlook is not supported

https://docs.microsoft.com/en-us/outlook/troubleshoot/profiles-and-accounts/outlook-cannot-use-activesync-connect-exchange

Version History

Version	Date	Comment
6.0	2018	Public release using ISAM 9.0.x
7.0	2022	Updated for ISVA 10.0.3

MaaS360 Email Access Gateway Deployment

MaaS360 Email Access Gateway (EAG) is a reverse proxy solution that is typically deployed in the DMZ. EAG exposes an external interface to the internet for all mobile device connections. This interface serves as the hostname for ActiveSync connections for email clients. EAG will proxy all ActiveSync traffic from mobile devices before the traffic is forwarded to corporate email servers.



- Mobile devices connect to the external hostname of EAG over SSL
- EAG terminates the SSL traffic and performs one of the following tasks depending on how EAG is configured:
 - Forward the traffic as is to corporate email server
 - Inspect headers and decide to allow or reject the traffic
 - o Identify user against corporate directory before forwarding traffic to corporate email server
- If EAG is configured to identify user (e.g. Simon), then user identification is first performed before allowing the traffic to pass to the email servers. The following security schemes are supported:
 - **Corporate credentials**: EAG connects to corporate directory server using LDAP to validate the user.
 - Identity certificates: EAG can be configured to identify user based on identity certificates that are provisioned to the user during MaaS360 enrollment. This requires MaaS360 Cloud Extender integration with Certificate Authority (CA) to deliver identity certificates to MaaS360 enrolled devices.
- The connection is forwarded to the email servers. In addition to user identification at the reverse proxy level, email servers will perform user authentication. Depending on the security scheme configured for email servers, EAG supports these modes:
 - **Corporate credential**: EAG presents the end user credentials to the email servers for authentication.
 - **Kerberos delegation**: EAG can attach Kerberos tickets for the email servers to avoid authentication. This method allows email servers to offload authentication to EAG.

Implementation Use-cases

MaaS360 Email Access Gateway (EAG) is configured depending on requirements for end user productivity and email security. The below table shows the different scenarios for EAG deployment:

#	Scenario	Description
1	Any ActiveSync Client	 Workflow: ActiveSync traffic from any email client is forwarded from EAG to corporate email servers EAG does not confirm identity of user before forwarding ActiveSync traffic Email servers will authenticate users Use-case: This option is to expose ActiveSync traffic while keeping email servers internal to the network. All traffic is forwarded to the corporate email servers.
2	MaaS360 Secure Mail Only	 Workflow: ActiveSync traffic originating from only MaaS360 Secure Mail client is forwarded to corporate email servers Traffic from any other email client (native email client on iOS / Android) is blocked by EAG EAG will only allow ActiveSync traffic based on email client type (MaaS360 Secure Mail) Email servers will authenticate users Use-case: This option is used to expose ActiveSync for only MaaS360 Secure Mail clients while keeping corporate email servers internal to the network.
3	User Identification LDAP Federation	 Workflow: ActiveSync traffic from any email client is only forwarded to corporate email servers once user identity has been confirmed via the federated LDAP connection The user identity is checked against corporate directory via LDAP federation on the EAG Email servers will authenticate the user Use-case: This option is used to expose ActiveSync traffic and confirm user identity before forwarding traffic to the corporate email servers, which remain internal to the network.
4	User Identification Cloud Extender Identity Certificate	 Workflow: ActiveSync traffic from any email client is only forwarded to corporate email servers once user identity has been confirmed using both the federated LDAP connection and identity certificate Identity certificate is used to confirm user identity with EAG and can be provisioned to email clients (MaaS360 Secure Mail or native email) during MaaS360 enrollment Email servers will authenticate the user Use-case: This option is used to expose ActiveSync traffic and confirm user identity before forwarding traffic to the corporate email servers, which remain internal to the network.

5	Kerberos Constrained	Workflow:
	Delegation	 ActiveSync traffic from any email client is only forwarded to corporate email servers once user identity has been confirmed using both the federated LDAP connection and identity certificate Userid or client identity certificate is used to confirm identity with EAG EAG attaches Kerberos tickets for corporate email servers along with the forwarded ActiveSync traffic Corporate email servers will validate the Kerberos tickets and not perform any secondary authentication. The authentication operations are delegated to FAG
		Use-case:
		This option is used to expose ActiveSync traffic and confirm user identity before forwarding traffic to the corporate email servers, which remains internal to corporate network. In this option, EAG performs user authentication and forwards authenticated ActiveSync traffic and Kerberos tokens to the corporate email servers, offloading authentication from the email servers.

Each of the scenarios can be layered on top of another. For example, scenario 1 can be implemented now, and scenarios 3 or 4 are configured later.

Requirements and pre-requisites:

This section covers the system requirements for basic EAG installation. Scenarios of basic email gateway and authorization of MaaS360 Secure Mail use-cases are accomplished with these requirements.

General Requirements

Туре	Minimum Requirement	
Virtualization Environments		
Supported environments	Refer to quick start guide for further information https://www.ibm.com/docs/en/sva/10.0.3?topic=virtual- appliance-quick-start-guide	
Hardware Requirements		
Disk Space	100 GB	
Memory	4GB	
Network Requirements		
Network interfaces for EAG appliance:	Public Interface for Reverse Proxy Traffic Private Interface for EAG Management Optionally an additional private interface to communicate to email	
Public Interface (Reverse Proxy Traffic)	Hostname IP Address Subnet Mask Default Gateway	
Private Interface (EAG Management)	Hostname IP Address Subnet Mask Default Gateway	
Email Server Connectivity	Access to corporate email server from EAG public interface. Firewalls rules may need to be opened to enable this connectivity Typically inbound port 443 needs to be opened on the firewall	
Certificate Requirements		
SSL Certificate for public interface	Publicly signed certificate for public hostname Private key of the public certificate	
SSL Signer Certificates (if SSL is used)	Signer Certificate of corporate mail servers Signer Certificate of issuing CA and intermediaries	

Requirements for EAG implementation scenarios:

This section provides additional requirements for other various implementation use-cases highlighted in the previous section. These requirements are in addition to the general requirements section above.

Scenario #1: Any ActiveSync Client

No additional requirements other than general requirements. Scenario #2: MaaS360 Secure Mail Only

No additional requirements other than general requirements.

Scenario #3: User Identification with LDAP Federation

Туре	Minimum Requirement	
Network Requirements		
LDAP Connectivity	Access to LDAP from EAG private (management) interface is required for LDAP federation Firewalls rules may need to be opened to enable this connectivity One of the following ports is required depending on how the LDAP integration is configured Port 389 for LDAP Port 636 for LDAP over SSL	
Certificate Requirements		
SSL Signer Certificates (If SSL is used)	Signer Certificate of LDAP server Signer Certificate of issuing CA and intermediaries of the LDAP server	
Accounts		
LDAP Bind Account	Basic LDAP user for directory bind	

Scenario #4: User Identification with Cloud Extender Identity Certificate

Туре	Minimum Requirement	
Network Requirements		
LDAP Connectivity	Access to LDAP from EAG private (management) interface is required for LDAP federation Firewalls rules may need to be opened to enable this connectivity One of the following ports is required depending on how the LDAP integration is configured Port 389 for LDAP Port 636 for LDAP over SSL	
Certificate Requirements		
SSL Signer Certificates (If SSL is used)	Signer Certificate of LDAP server Signer Certificate of issuing CA and intermediaries of the LDAP server	
Accounts		
LDAP Bind Account	Basic LDAP user for directory bind	

Scenario #5: Kerberos Constrained Delegation

Туре	Minimum Requirement	
Network Requirements		
LDAP Connectivity	Access to LDAP from EAG private (management) interface is required for LDAP federation Firewalls rules may need to be opened to enable this connectivity One of the following ports is required depending on how the LDAP integration is configured Port 389 for LDAP Port 636 for LDAP over SSL	
Key Distribution Centre (KDC) Connectivity	Access to KDC from EAG private (management) interface is required to obtain Kerberos tickets to forward to the email server Firewall rules may need to be opened to enable this connectivity KDC typically uses port 88	
Certificate Requirements		
SSL Signer Certificates (If SSL is used)	Signer Certificate of LDAP server Signer Certificate of issuing CA and intermediaries of the LDAP server	
Accounts		
LDAP Bind Account	Basic LDAP user for directory bind	
Kerberos Delegation User Account	Account used to impersonate and obtain service tickets from KDC for the email server Account used to impersonate and obtain service tickets from KDC for the email server	

Supported Corporate directories:

Type IBM Security Directory Server IBM Tivoli Directory Server for z/OS Microsoft AD LDS (Lightweight Directory Services) Microsoft Active Directory

For further information refer to https://www.ibm.com/docs/en/sva/10.0.3?topic=configurationsupported-registries

Deploying MaaS360 Email Access Gateway (EAG): Step 1: Download Media from MaaS360 Portal

MaaS360 EAG is delivered as a virtual appliance that is downloaded from the MaaS360 portal. The virtual appliance is an image file that is deployed on a supported hypervisor.

Steps to download EAG media:

- 1. Log on to MaaS360 Portal
- 2. Go to SETUP > Services menu and locate the Email Gateway service
- 3. Click on link to download EAG installation media

If the Email Gateway service is not enabled, then please contact MaaS360 Support

See Box link:

Step 2: Deploy Virtual Appliance

MaaS360 EAG needs to be deployed in the DMZ and is installed on supported virtualization platforms. Follow the quick start guide to build and configure the virtual machine from the supplied ISO file.

Useful links:

https://www.ibm.com/docs/en/sva/10.0.3?topic=virtual-appliance-quick-start-guide https://www.ibm.com/docs/en/sva/10.0.3?topic=started-virtual-appliance-tasks

Step 3: Install Firmware

The next step after virtual machine creation is to load the EAG virtual appliance firmware from the ISO media

Configuration	Screenshot
Power on the virtual machine	ISOLINUX 4.05 0x587a3765 ETCD Copyright (C) 1994-2011 H. Peter Anvin et al
After 10 seconds, the installation	Security Appliance Installer
will automatically start	Wait 10 seconds or press enter to boot the appliance installer.
	Type "boothdd" to boot from the hard drive, or "interactive" to boot the interactive appliance installer.
	boot: _
Power on and the installation will	The firmware image is about to be installed. This installation process will erase the hard disk and all existing data will be lost.
prompted enter yes to proceed	Enter 'yes' to proceed.
The appliance firmware is automatically installed to the virtual machine	The signature of the installation image has been verified. Partitioning the disk Formatting the boot partition on the disk Configuring the disk boot loader
Wait for the installation to	Formatting the partition
complete	Installing the firmware image
Remove installation media when prompted and reboot	The firmware image has been successfully installed.
	Unmount the installation media and then press the enter key to reboot the appliance.

Step 4: Configure Virtual Appliance

Configuration	Screenshot
A flashing cursor may be seen The following prompt will appear	unconfigured.appliance login:
Login to the console using the administrator user id admin and the default password of admin	unconfigured.appliance login: admin Password:
After the firmware has been loaded onto the appliance a wizard is automatically run Press Enter to continue	Welcome Welcome to the IBM Security Verify Access setup wizard. Using this setup wizard, you can: * View and accept the Software License Agreement * Set the appliance password * View and configure networking Press Enter to continue
Select option 1 to procced to agree	By choosing 'I agree,' you agree that (1) you have had the opportunity to review the terms of both the IBM and non-IBM licenses presented above and (2) such terms govern this transaction. If you do not agree, choose 'I do not agree'. 1: I agree 2: I do not agree Select option:
FIPS Mode can be enabled at this stage and once enabled it cannot be disabled FIPS cannot be enabled after setup and is not required for EAG Enter n to continue	FIPS 140-2 Mode Configuration You must enable FIPS mode in order to comply with FIPS 140-2 and NIST 800-131a. If you select to enable FIPS mode, appliance will be rebooted immediately to perform FIPS power-up integrity checks. Do not choose to enable FIPS mode without reading the FIPS section in the user guide. If you choose to enable FIPS mode now, you cannot disable it later without reinstalling the appliance. FIPS 140-2 Mode is not enabled. 1: Enable FIPS 140-2 Mode x: Exit p: Previous screen n: Next screen Select option: n
The next prompt is the option to change the appliance password This step can be skipped for now by entering n The passwords can be changed at the end of the installation	Appliance Password Password changes are applied immediately. Password has not been modified. 1: Change password x: Exit p: Previous screen n: Next screen Select option: n_
Entoy 1 to observe the bast years	Used Name Configuration
Enter 1 to change the host name	Host Name Configuration Host name: unconfigured.appliance 1: Change the host name x: Exit p: Previous screen n: Next screen Select option: 1

Configuration	Screenshot
Enter the hostname of the appliance This is any arbitrary hostname that is used to identify this appliance This hostname will correspond to the management interface of EAG Enter n to continue	Host Name Configuration Host name: eag.maas360swat.com 1: Change the host name x: Exit p: Previous screen n: Next screen Select option: n
Next step is to configure a management interface that is used to configure and manage EAG Enter 3 to configure an interface The reverse proxy interface is configured at a later point	Network Interface Settings 1: Display device settings 2: Display policy 3: Configure an interface 4: Create a VLAN interface 5: Delete a VLAN interface 6: Set IPv4 default gateway 7: Set IPv6 default gateway x: Exit p: Previous screen n: Next screen Select option: 3
Enter 1 to configure the 1.1 Interface Enter 1 to enable this interface	Configure an Interface Select the interface to configure:Enable this interface?1: 1.1 2: 1.2 3: loopback Enter index: 12: No Enter index: 1
A static IP address for the management interface is specified in this example Enter 2 for manual configuration	Select an IPv4 configuration mode: 1: Automatic 2: Manual 3: Automatic and Manual Enter index: 2_
Enter 2 to add a new IP address to the 1.1 interface	Configure Static IPv4 Addresses Select an action: 1: Show configured addresses 2: Add an address 3: Delete an address 4: Finish configuring addresses Enter index: 2
Enter management IP address and the subnet mask	Enter the IPv4 address: 10.0.1.5 Enter the IPv4 prefix or subnet mask: 255.255.255.0

Configuration	Screenshot
Enter 1 to specify this IP address as a management address	Enter the IPv4 address: 10.0.1.5 Enter the IPv4 prefix or subnet mask: 255.255.255.0 Use this IP address for management? 1: Yes 2: No Enter index: 1
Enter 1 to enable this IP	Enable this IP address? Configure Static IPv4 Addresses Select an action:
address Enter 4 to finish configuring	1: Yes1: Show configured addresses2: No2: Add an address3: Delete an address3: Delete an addresses4: Finish configuring addresses
addresses	Enter Index: 4_
Enter 1 to Automatic configure IPv6 address	Select an IPv6 configuration mode: 1: Automatic 2: Manual 3: Automatic and Manual Enter index: 1
Enter 2 to not use obtained IP	Configure Auto IPu6 Address
address for management	Use obtained IP address for management? 1: Yes 2: No Enter index: 2
Entor 6 to sot the IPv/ default	
gateway	Network Interface Settings 1: Display device settings 2: Display policy 3: Configure an interface 4: Create a VLAN interface 5: Delete a VLAN interface 6: Set IPv4 default gateway 7: Set IPv6 default gateway x: Exit p: Previous screen n: Next screen Select option: 6
Enter the default gateway address	Set IPv4 Default Gateway Enter gateway IP address: 10.0.1.1_

Configuration	Screenshot
Enter 1 to specify that the 1.1 interface should be used to reach the Default Gateway	Set IPv4 Default Gateway Enter gateway IP address: 10.0.1.1 Select interface: 1: 1.1 2: 1.2 3: loopback Enter index: 1
Networking configuration has been completed Enter n to proceed to the next screen	Network Interface Settings 1: Display device settings 2: Display policy 3: Configure an interface 4: Create a VLAN interface 5: Delete a VLAN interface 6: Set IPv4 default gateway 7: Set IPv6 default gateway x: Exit p: Previous screen n: Next screen Select option: n
Select option 1 to set DNS server 1	DNS Configuration DNS is obtained from DHCP on 1.1 1: Set DNS server 1 2: Set DNS server 2 3: Set DNS server 3 4: Obtain DNS servers from DHCP x: Exit p: Previous screen n: Next screen Select option: 1
Enter the IP address of the DNS server	Set DNS Server 1 Enter the DNS server IP address: 10.0.1.2

Configuration	Screenshot
Once the DNS configurations have been completed Enter n to continue to the next screen	DNS Configuration DNS server 1: 10.0.1.2 DNS server 2: DNS server 3: 1: Set DNS server 1 2: Set DNS server 2 3: Set DNS server 3 4: Obtain DNS servers from DHCP x: Exit p: Previous screen n: Next screen Select option: n
Enter 3 to change time zone if required, or enter n to continue Check the time and date displayed and modify if necessary Once the date, time and time zone are set correctly, enter n to continue	Time Configuration Time configuration changes are applied immediately. Time: 12:50:23 Date: 03/15/2022 Time Zone: America/New_York 1: Change the time 2: Change the date 3: Change the time zone x: Exit p: Previous screen n: Next screen Select option: n_
Check the data displayed in the Summary Enter 1 to accept and apply the specified configuration	Summary FIPS 140-2 Mode is not enabled. Password has not been modified. Host name: eag.maas360swat.com Interface: 1.1 Policy: IPv4 Mode: Manual IPv4 Manual Settings: IPv4 Address: 10.0.1.5/255.255.255.0 [Management] IPv6 Mode: Automatic IPv6 Mode: Automatic IPv6 Mode: Automatic IPv6 Automatic Settings: Interface: 1.2 Policy: Interface: loopback Policy: The IPv4 default gateway is 10.0.1.1 on interface 1.1. DNS server 1: 10.0.1.2 DNS server 3: Time: 12:50:42 Date: 03/15/2022 Time Zone: America/New_York 1: Accept the configuration 2: Cancel the configuration 3: Modify the configuration Select option: 1

Configuration	Screenshot
If prompted, press enter to reboot and continue	Applying policy changes. Policy changes could not be applied. System must be rebooted. Press enter to continue: _
Depending on changes restart may not be required	Applying policy changes. Policy changes were successfully applied. Local Management Interface has been restarted. Welcome to the IBM Security Verify Access appliance Enter "help" for a list of available commands

Step 5: Login to Web Management Interface

	Configuration
The appliance offers a brows In this example, the URL is h The default credentials to log	ser-based graphical user interface Ittps://eag.maas360swat.com g in to the local management interface are user admin password admin
	IBM® Security Verify Access
	Local Management Interface
	User name
	admin
	Password:
The password for the Local M	Aanagement Interface (LMI) can be configured via the UI
eag.n	naas360swat.com admin 🔗 💮 Language
	Set Password
	Logout
Set the new password if requ	uired
	Set Password ×
	Update the password for the authenticated user
	Current Password:
	New Password: ••••••
	Submit Cancel

Step 6: Configure Data Interface

		Config	uration		
From the top n	nenu, select System >	Network Settir	ngs > Interfaces		
	Monitor V Web V S	ystem \land			
	Updates and Licensing	Network Settings	System Settings	Secure Settings	
	Overview	General	Date/Time	SSL Certificates	
	Application Database Settings	DNS	Administrator Settings	File Downloads	
	Available Updates	Interfaces	Management Authentication	n Silent Configurat	ion
	Scheduled Security Updates	Interfaces Static Routes	Management Authorization		
Provide a Nam	e to the interface (Re	verse Proxy for	example)		
Networking Configur	DNS Interfaces Static Routes Test Con	nection	Edit Interface		
Interfaces:	June notice state notice rest con	lociton	General Config	uration IPv4 Setting	IPv6 Settings
+ New 🖉 Edit	Delete		Interface: 1.2	~	
Interface	Enabled Name	Address	Name: Reverse	Proxy]
1.1		10.0.1.5/255.255.255.0	[Management]	21	
JNECK ENADLED	Edit Interface	Interface			
Check Enabled	l option to enable the	interface			
	Lan Interface				
	General Configuration	IPv4 Settings IPv	6 Settings		
	Auto (DHCP)				
	Enabled				
	Management Ad	dress			
	Manual	Route			
	+ New 2 Edit	ū Delete			
	Address		Management Address	Enabled	
	10.0.1.6/24	ţ	No	Yes	
	Override the Ove	erlapping Subnet Valid	ation		
he option to o onfiguration o warning mes	override the overlappi of the network interfa isage is shown if this i	ng subnet valid ces s the case	ation may have to be	e selected depe	nding on the



Step 7: Activate Reverse Proxy

•	Config	guration	
System > Updates and Lice	ensing > Licensing and	Activation	
Monitor 🗸 🤍 We	b ∽ System ∧		
Updates and Licensin	g Network Settings	System Settings	Secure Settings
Overview	General	Date/Time	SSL Certificates
Application Database	Settings DNS	Administrator Settings	File Downloads
Available Updates	Interfaces	Management Authentication	Silent Configuration
Scheduled Security U	odates Static Routes	Management Authorization	
Update Servers	Test Connection	Management SSL Certificate	
Update History	Hosts File	Account Management	
Licensing and Activati	on Packet Tracing	Advanced Tuning Parameters	9
Licensir Firmware Settings	g and Activation Cluster Configuration	Snapshots	
Locate the license key file v	vith the EAG media that	has been downloaded	from the MaaS360 Portal
On the Licensing and Activa	ation page, click Select	License and locate the	license file to install
Select the license file and t	hen click Open		
Licensing and Activation	🔹 File Upload		×
Activated Modules	← → ∽ ↑ ↓ > This PC > Downloads	ب ت	Search Downloads
Import	Organize 🔻 New folder		i≡ - □ ?
Module	Name	^ Date modified	Type Size
	Desktop	3/15/2022 11:34 AM	Text Document 1 KB
Sunnort License	🕹 Downloads 🖈		
Select License	Documents *		
Select License	System32		
No licensed modules. Add	This PC		
	i Network		
	File name: License Key		✓ All Files ✓
			Open Cancel
Click Save Configuration			
Activ	ated Modules		
Impo	nt		
The lic	ense file upload process	s is pending:	
# Тур	e File Name		
1 TXT	License Key.txt		
Save	Configuration Cance	l	
Confirm license is enabled			

			Configura	ation					
		Activated Mod	lules				_		
		Import							
		Module							
		Name: IBM Securi Enabled: True Software License A	ity Verify Access Ba Agreement: <u>View</u>	ase Appliance Service Agree	<u>ment</u>				
Review a	and deploy of	changes							
	Pending	Chandes		Deploy Pendi	ng Changes			×	
	There is	currently one unde	eployed change.	Module Activation	Date Modified Mar 15, 2022,	11:36:54 A	м		
	Review F	Pending Changes				Cancel	Roll Back	Deploy	
The follo	wing messa the link in t	age is displayed	onnect to the m	anagement i	interface				
Poverse	Provy is no	 Sessi The p natur interf This a netwo The lo unava Click mana 	on Ended olicy was success e of the changes ace to restart. action does not co ork traffic. ocal management ailable until the r here to return to gement interfac	esfully applie required the lisrupt the fl at interface v estart finish the local e	ed but the e user ow of vill be es.				
Reverse	Proxy is no		eb menu						
		Web 🔨	IBM Security Verif	y System					
		Manage		Global Setting	gs				
		Runtime Co	omponent	URL Mapping					
		Reverse Pro	рху	Junction Map	ping				
		Authorizati	on Server	Client Certific	ate Mapping				

Step 8: Configure Runtime Component

		Config	guration		
b > Manage > F Runtime Com ck Configure	Runtime Compo ponent is not co	onent onfigured			
	Web ^	IBM Security V	erify Syste	m ~	
	Manage		Global Sett	ings	
	Runtime C	omponent	URL Mappir	ıg	
	Reverse Pr	oxy		apping	
	Authorizati	ion Server	Client Certi	ficate Mapping	
					_
IBM Security Ve	rify Access	Monitor ~	Web ∽ IBM	Security Verify	System 🗸
Runtime Compo	nent				
Status: Not confi	Unconfigure	Start Stop			
Status: Not confi Policy Server for the configure of the	S Unconfigure	Start Stop			
Status: Not confi Policy Server User Registry Runtime Environme Main Policy S	S Unconfigure	Start Stop			
Status: Not confi Policy Server User Registry Runtime Environme Main Policy S	S Unconfigure	Start Stop			
Status: Not confi Policy Server User Registry Runtime Environme Main Policy S	S Unconfigure	Start Stop			
Status: Not confi Policy Server User Registry Runtime Environme Main Policy S Local Remote Import	S Unconfigure	Start Stop			
Status: Not confi Policy Server User Registry Runtime Environme Main Policy S O Local C Remote Import	S Unconfigure	Start Stop			
Status: Not confi Policy Server User Registry Runtime Environme Main Policy S O Local C Remote C Import	S Unconfigure	Start Stop			
Status: Not confi Policy Server User Registry Runtime Environme Main Policy S O Local C Remote Import User Registry	S Unconfigure	Start Stop			
Status: Not confi Policy Server User Registry Runtime Environme Main Policy S O Local C Remote C Import User Registry	igured to Local to LOAP Local ent Configure erver LDAP	Start Stop			
Status: Not conf Policy Server User Registry Runtime Environme Main Policy S © Local © Local © Remote © Import User Registry © LDAP Remot © LDAP Remot	S Unconfigure	Start Stop			
Status: Not conf Policy Server User Registry Runtime Environme Main Policy S O Local C Remote Import User Registry C LDAP Remot LDAP Local	S Unconfigure	Start Stop		Previous	ext Finish Canc

Configuration	
Runtime Environment Configure ×	
Main Policy Server LDAP	
Administrator Password *	
••••••	
Confirm Administrator Password *	
SSL Server Certificate Lifetime (days) 1,460 🗘	
SSL Compliance *	
No additional compliance V	
Previous Next Finish Cancel	
Select LDAP and click Finish	
Runtime Environment Configure ×	
Main Policy Server LDAP	
Previous Next Finish Cancel	
Runtime Component status is now available	
Runtime Component	
🕲 Confidure 🔗 Unconfidure 🕒 Start 🔳 Stop 🕧 Restart 🖾 Replicate with Cluster 🗔 Manade 🖌	
Status: Available	
Mode: The environment is configured using a local policy server and a local user registry.	
Go to Application Log Files to view the Policy Server and User Registry log files.	

Step 9: Set up Reverse Proxy

		Configuration		
> Manage > Ro New	everse Proxy			
			Current and	
	web ^ IBM	i Security Verify	System V	
	Manage	Glo	bal Settings	
	Runtime Compo	nent URI	_ Mapping	
	Reverse Proxy	Jun	ction Mapping	
	Reverse Authorization Se	Proxy Trver Clie	nt Certificate Mapping	
Reverse Proxy				
+ New 2 Edit	Delete ► Start All ■ Stor	p All () Restart All C Ref	resh Manage V Troubleshooting V	Last Modified
	and the second se	State	changes are Active	Last Houmed
N N N	ter applied			
o item				o 48
0 item	name (e.g. mailproxy) lated automatically wi) ith the hostname o	10 25 50 10	o All
the Instance name is popul t the IP Addre ace New Reve Instance mailproxy	name (e.g. mailproxy) lated automatically wi ess for the Primary Int rse Proxy Instance IBM Security Verify Access) ith the hostname of terface to the add Transport	10 25 50 10 of the instance ress that was configured fo	o All
the Instance name is popul t the IP Addre ace New Reve Instance mailproxy	name (e.g. mailproxy) lated automatically wi ess for the Primary Int rse Proxy Instance IBM Security Verify Access) ith the hostname of terface to the add Transport	10 25 50 10	o I All
the Instance name is popul t the IP Addre ace New Reve Instance mailproxy Description Host name eag.maas	name (e.g. mailproxy) lated automatically wi ess for the Primary Int rse Proxy Instance IBM Security Verify Access on e * 360swat.com) ith the hostname of terface to the add Transport	10 25 50 10	o I All
the Instance name is popul t the IP Addre ace New Reve Instance mailproxy Description Host nam eag.maas	name (e.g. mailproxy) lated automatically wi ess for the Primary Int rse Proxy Instance IBM Security Verify Access n on e * 360swat.com) ith the hostname of terface to the add Transport	10 25 50 10	o I All
the Instance name is popul t the IP Addre ace New Reve Instance mailproxy Description Host nam eag.maas Listening 7234	name (e.g. mailproxy) lated automatically wi ess for the Primary Int rse Proxy Instance IBM Security Verify Access on e * 360swat.com Port *) ith the hostname of terface to the add Transport	10 25 50 10	o I All
the Instance name is popul t the IP Addro ace New Reve Instance mailproxy Description Host nam eag.maas Listening 7234	name (e.g. mailproxy) lated automatically wi ess for the Primary Int rse Proxy Instance IBM Security Verify Access n on e * 360swat.com Port *) ith the hostname of terface to the addu Transport	10 25 50 10	o I All
the Instance name is popul t the IP Addre ace New Reve Instance mailproxy Description Host nam eag.maas Listening 7234 IP Addres 10.0.1.6	name (e.g. mailproxy) lated automatically with rse Proxy Instance IBM Security Verify Access (*) ith the hostname of terface to the addu Transport	10 25 50 10	o I All

		Configuration	
	New Reverse Proxy Instance		
		-	
	Instance IBM Security Verity Access	Transport	
	Administrator Name *		
	sec_master		
	Administrator Password *		
	•••••		
	Domain *		
	Default		
C - I + T			Previous Next
Select Trans Enable HTT	sport PS Port 443		
	Instance IBM Security Verify Access	Transport	
	Enable HTTP		
	HTTP Port		
	HTTP Port Enable HTTPS		
	HTTP Port Enable HTTPS HTTPS Port		
	HTTP Port Enable HTTPS HTTPS Port 443		
	HTTP Port Enable HTTPS HTTPS Port 443	Pre	vious Next Finish
Click Finish	HTTP Port Enable HTTPS HTTPS Port 443	Pre	vious Next Finish
Click Finish The reverse	HTTP Port Enable HTTPS HTTPS Port 443 proxy instance is created	Pre	vious Next Finish
Click Finish The reverse	HTTP Port Enable HTTPS HTTPS Port 443 proxy instance is created Reverse Proxy	Pre	vious Next Finish
Click Finish The reverse	HTTP Port TTPS Port 443 Proxy instance is created Reverse Proxy New 2 Edit 2 Delete Start All =	Pret Stop All 🕐 Restart All 🕞 Refresh Manage 🕥	vious Next Finish
Click Finish The reverse	HTTP Port TTPS Port 443 proxy instance is created Reverse Proxy New 2 Edit 2 Delete Start All =	Stop All () Restart All () Refresh () Manage () State	vious Next Finish V Troubleshooting V Changes are Active
Click Finish The reverse	HTTP Port TTPS Port 443	Stop All 🕐 Restart All 🔯 Refresh Manage State	vious Next Finish Troubleshooting ~ Changes are Active

Step 10: Disable Basic Authentication

Select Re Click Edit				Configura	tion				
CIICK Edit	verse Proxy	instanc	e						
	Reverse Proxy Bas	ic Configurati	ion - mailproxy						
	Server SSL	Junction	Authentication	Session Response	SSO Log	gging Inter	faces		
	Client Connec	ction					Threa	ds and Connections	
	✓ HTTPS						Persist	ent Connection Timeout *	
	HTTPS Port *						0		
	443						Worke 300	r Threads *	
	🗌 НТТР								
	HTTP Port *								
	80								
Serve	r SSL	Junction	Authentication	Session Respons	se SSO	Logging	Inte	rfaces	
Ba	sic Authenticati	ion						Forms Authentication	
Da									
Trar	nsport							Transport	
Trar	nsport ne	~						Transport HTTPS	~
Trar Nor Review at	nsport ne nd deploy cl	hanges						Transport HTTPS	~
Trar Nor Review al	nsport ne nd deploy cl	hanges			Deploy Pen	ding Change	25	Transport HTTPS	×
Trar Nor Review at	nsport ne nd deploy cl Pending (There is c	hanges Changes	s one undep	loyed change.	Deploy Pen Module	ding Change Date Mo	es	Transport HTTPS	×
Review al	nsport ne Pending (There is c Review P	hanges Changes currently ending C	one undep Changes	loyed change.	Deploy Pen Module	ding Change Date Mo	es odified	Transport HTTPS	×
Review al	nsport ne nd deploy cl Pending (There is c Review Po	hanges Changes currently ending C	one undep Changes	loyed change.	Deploy Pen Module	ding Change Date Mo	es ⊳dified	Transport HTTPS Cancel Roll Back De	×
Review al ! Restart re Select the	nsport ne Pending (There is c Review P everse proxy e reverse proxy	hanges Changes currently ending C / instanc oxy insta	one undep changes ce if prompt	loyed change. ted	Deploy Pen Module	ding Change Date Mo	es dified	Transport HTTPS Cancel Roll Back De	×
Review al Review al Restart re Select the System We Successful	nsport ne nd deploy cl Pending (There is c Review Po everse proxy e reverse proxy e reverse proxy	hanges Changes currently ending C y instanc oxy insta Reverse Proxy + New 2 Edi	one undep changes ce if prompt ance and cli	loyed change. ted ick Restart	Deploy Pen Module	ding Change Date Mo	es	Transport HTTPS Cancel Roll Back De	× x
Review al Review al Restart re Select the System W Successful pending ch The followic The followic	nsport ne nd deploy cl Pending (There is c Review Pe everse proxy e reverse proxy e reverse proxy e reverse proxy e reverse proxy e reverse proxy	hanges Changes currently ending C y instanc oxy insta Reverse Proxy + New 2 Edi	cone undep changes ce if prompt ance and cli it @ Delete > Start Name	loyed change. ied ick Restart	Deploy Pen Module resh Manage ~ Tr Changes an	ding Change Date Mo oubleshooting ~	es odified	Transport HTTPS Cancel Roll Back De	× ×
eview al rea eview al estart re select the System Wa Successful pending du proxy insta be restart to take effit	nsport ne nd deploy cl Pending (There is c Review Pe everse proxy e reverse proxy e reverse proxy e reverse proxy ing reverse ing reverse	hanges Changes currently ending C y instance oxy instance reverse Proxy + New 2 Edi Instance / I instance / New No fi	one undep changes ce if prompt ance and cli it @ Delete ▶ Start Name	loyed change. ted ick Restart = Stop © Restart Q Ref State	Deploy Pen Module	ding Change Date Mo oubleshooting ~ e Active	es bdified	Transport HTTPS Cancel Roll Back De System Notification Successfully restarted the	× × ploy

Step 11: Import SSL Certificates of Mail Server

Typically, corporate email servers have an SSL certificate to secure ActiveSync traffic. EAG terminates SSL traffic from mobile devices and initiates a new SSL connection to the corporate email server.

In this step, the SSL certificate(s) for the email server are imported into EAG. To complete this step, the following pre-requisite steps should already have been performed:

- All certificates should be exported in x.509 DER encoded format
- If the above SSL certificate is issued from a private Certificate Authority (CA) or an Intermediate CA, EAG requires the entire SSL certificate chain
- Export the SSL certificate(s) of the issuing (and Intermediate if required) Certificate Authorities
- SSL certificates can be exported by using a browser connection to mail server and then by examining SSL connection (click on padlock in browser address bar). The certificates can be viewed and exported from here
- Complete the following section once the mail server certificates have been exported

Select pdsrv Click Manage > Edit SSL Certificate Database System Settings Date/Time Administrator Settings Management Authentication Click on Signer Certificates Select Manage > Import Edit SSL Certificate Database - pdsrv + New 2 Edit 1 Delete 2 Refresh Manage ∧ View Signer Certificates Personal Certificates Certificates 2 Label Issuer			n	
IBM Security Verify System ^ Sstem ^				
System Settings Secure Settings Date/Time SSL Certificates Administrator Settings Eile Downloade Management Authentication SSL Certificates Silent Configuration pdrv Click on Signer Certificates Select Manage > Import Edit SSL Certificate Database - pdsrv + New ∠ Edit Delete C Refresh Manage ^ Signer Certificates Personal Certificates Certificates Personal Certificates Iabel Issuer			SL Certificates	
Date/Time SSL Certificates Administrator Settings Eile Downloade Management Authentication SSL Certificates Silent Configuration downloade Certificates downloade Silent Configuration downloade Certificates downloade Silent Configuration downloade Certificates downloade Select Manage > Import Local Edit SSL Certificate Database - pdsrv	Edit SSL Certificate Datab Edit SSL Certificate Datab	LE Réplicate with cluster	No filter applied C Remean Last Replacate with Closer Last Replacate with Closer	_ Certificate Database perties
Administrator Settings Management Authentication Eile Downloads SSL Certificates Silent Configuration embedded_idap_keys tocal inj_trust_store tocal fin_trust_store tocal for for for for for for for fo	Last Mo Rename	Type Las	Certificate Database Name Type Last Mo Desc Rena	e
Management Authentication SSL Certificates Management Authentication SSL Certificates Silent Configuration pdrv Local Click on Signer Certificates Edit SSL Certificate Database - pdsrv Edit SSL Certificate Database - pdsrv + New Z Edit Delete Refresh Manage ^ View Signer Certificates View Signer Certificates	Mar 15, 2 Import Export	Local Mar	mbedded_ldap_keys Local Mar 15, 2 Impoi Expor	0-09 BM
Click on Signer Certificates Select Manage > Import Edit SSL Certificate Database - pdsrv + New	Mar 18, 2022, 12:18:33 PM	Local Mar	inguiss_skore tocal Mar 18, 2022, 1 idarv Local Mar 18, 2022, 1	18:33 PM
+ New ∠ Edit				
Label Issuer			esh Manage ^ View	
Export Export Extract	ct	Subject	Import Export Extract	
✓ … No filter applied Load			Load	

IBM MaaS360 Email Access Gateway

	Conf	iguration		
	Import Signer Certificato	2	×	
	Certificate File ~ mail-server-cert.cer			
	Browse			
	Certificate Label *			
	Mail Server			
		Import	ncel	
Sve	om Natification The manageme	ont SSL certificate w	as successfully up	lated
5y5	en Notification The manageme	III SSE CEITINCALE W	as successivily upo	lated.
croll to bottom and	confirm that both certificate tificate make sure the chair	s loaded success	sfully import any missi	ng certificates
cpending on the ce	intere, make sure the chain			ng ver uncates
	E 1 10 1 2E			
	5 10 25	50 100 All		
	5 10 25	50 100 All		
	5 10 25	50 100 Al l		
O Mail Serve	5 10 25 CN=MS-EX	CH2016	CN=MS-E)	(CH2016
O Mail Serve	5 10 25	CH2016	CN=MS-E)	KCH2016
O Mail Serve	5 10 25 CN=MS-EX	CH2016	CN=MS-E)	(CH2016
O Mail Serve Review and deploy c	CN=MS-EX	CH2016	CN=MS-E)	(CH2016
O Mail Serve	T CN=MS-EX	CH2016	CN=MS-E) ing Changes	<pre> KCH2016</pre>
O Mail Serve Review and deploy c	5 10 25	CH2016	CN=MS-E) ing Changes	(CH2016 ×
O Mail Serve Review and deploy c ! Pending There is c	T CN=MS-EX hanges Changes urrently one undeployed char	CH2016 Deploy Pendi nge. Module	CN=MS-E) ing Changes Date Modified	XCH2016 ×
O Mail Serve Review and deploy c Pending There is c	T CN=MS-EX	CH2016 Deploy Pendi nge. Module	CN=MS-E) ing Changes Date Modified	KCH2016 ×
O Mail Serve Review and deploy c ! Pending There is c Review P	T CN=MS-EX hanges Changes surrently one undeployed char ending Changes	CH2016 Deploy Pendi	CN=MS-E) ing Changes Date Modified	KCH2016 ×
O Mail Serve Review and deploy c Pending There is c Review P Review P	T CN=MS-EX hanges Changes urrently one undeployed chan ending Changes / instance if prompted	CH2016	CN=MS-E) ing Changes Date Modified	KCH2016 ×
O Mail Serve Review and deploy c Pending There is c Review P Restart reverse proxiselect the reverse proxise	5 10 25 r CN=MS-EX hanges Changes surrently one undeployed chan ending Changes / instance if prompted oxy instance and click Restan	CH2016 Deploy Pendi nge. Module	CN=MS-E) ing Changes Date Modified	KCH2016 ×
 Mail Serve Review and deploy c Pending There is c Review P Review P Restart reverse proximate 	thanges Changes C	CH2016 Deploy Pendi nge. Module rt	CN=MS-E) ing Changes Date Modified	KCH2016 ×
 Mail Serve Mail Serve Review and deploy c Pending there is c Review P Review P Restart reverse proxide the reverse	5 10 25 r CN=MS-EX hanges Changes currently one undeployed char ending Changes / instance if prompted oxy instance and click Restat Reverse Proxy + New 2 Edit ■ Delete > Start ■ Stop © Restat	CH2016 CH2016 Deploy Pendi nge. Module rt t Q Refresh Manage ~ Trock	CN=MS-E) ing Changes Date Modified Cance	KCH2016 ×
 Mail Serve Mail Serve Review and deploy c Pending there is a construction of the serve Review P Restart reverse proxide the reverse proxide construction of the serverse proximations need to be server as a server of the serverse proximation of the serve	5 10 25 r CN=MS-EX hanges Changes currently one undeployed charges currently one undeployed charges y instance if prompted oxy instance and click Restant Reverse Proxy + New & 2 Edit Delete > Start Instance Name Start	CH2016 CH	CN=MS-E) ing Changes Date Modified Cance bleshooting ~	CH2016 X Roll Back Deploy
 Mail Serve Mail Serve Review and deploy c Pending the serve Pending the serve Review P Restart reverse proximations need to be proximationed needs System Warning Successfully deployed all pending changes. The following reverse proximations need to be persented for updates to take effect: 	5 10 25 r CN=MS-EX hanges Changes currently one undeployed changes ending Changes / instance if prompted oxy instance and click Restant Reverse Proxy + New 2 Edit 10 Delete > Start = Stop 10 Restant Instance Name Stat Instance Name Stat V No filter applied	CH2016 Deploy Pendi nge. Module rt rt Changes are A	CN=MS-E) ing Changes Date Modified Cance bleebooting ~ Active System Succes	KCH2016 X Roll Back Deploy Notification stully restarted the started

Step 12: Create Junction

A junction allows communication to a backend server resource, in this case the corporate email environment.

Note:

In this example the junction server name is resolved using DNS. If a host entry is required, then this is entered using System > Network Settings > Hosts File

If an SSL error is encountered when creating the junction, this may be related to SSL/TLS configuration and is often be resolved by reviewing the reverse proxy instance configuration file and updating the following section:

Selectively disable SSL version support for junction connections

disable-ssl-v2 = yes disable-ssl-v3=yes disable-tls-v1 = no disable-tls-v11 = no disable-tls-v12 = yes

			<u> </u>						
	Reve	rse Proxy							
	+ Ne	w 🖉 Edi	it 🗍 Delete	► Start	Stop	() Restart	G Refresh	Manage ^	Troubleshooting \checkmark
	~	Instance N	Name			State		Configuration	1 •
	_							AAC and Fed	eration Configuration
	8.	. No fi	ilter applied					Junction Mar	nagement
								Renew Mana	gement Certificate
	~	mailproxy				🕑 Sta	rted	🕑 Tri	ue
Ju	nction	Manageme	ent - mailproxy	Create a Si	tandard Jui	nction			
Jui	nction	Manageme	ent - mailproxy Ū Delete	Create a St Junction	tandard Jui Servers	nction Basic Authent	ication Identit	y SSO and LTP,	A General
Jui Ne Sta Vir	ew ^ andard	Manageme	ent - mailproxy Delete t Name	Create a St Junction Creati	tandard Ju Servers on of a jun	Basic Authent	ication Identit	y SSO and LTP,	A General Junction Type
Jui Ne Sta	ew ^ andard tual Ju	Manageme	ent - mailproxy Delete	Create a St Junction Creati Junctio	Servers on of a jun	Basic Authent ction for an ir	ication Identit	y SSO and LTP,	A General Junction Type O TCP

All other required values are completed automatically

IBM MaaS360 Email Access Gateway

Configuration					
Add TCP or S	SL Servers		×		
Hostname * ms-exch2016	.maas360swat.com	Query Contents			
TCP or SSL Po 443	ort *	UUID of the Server			
Virtual Host		Distinguished Name(DN)			
Virtual Host F	Port 🐥	Uindows File System Support			
Local Address 10.0.1.6	\$	Treat URL as case insensitive			
		Save	el		
Confirm server added					
	+ New	ū Delete			
	Hostname				
	♡ No filter a	applied			
	O ms-exch2016.r	maas360swat.com			
Select Identity Change HTTP Basic Authen	tication Header to Ign	ore			
	Junction Servers E	Basic Authentication Identity			
	Supply identity information in HTTP headers				
	HTTP Basic Authentic	ation Header			
	Ignore Filter	^			
	Ignore				
Click Save The junction is created					

Junction Management - mailproxy	
System Notification Created junction at /mail ×	
New ✓ Z Edit Delete	
Junction Point Name Virtual or Standard	
\bigtriangledown No filter applied	
O /mail Standard Junction	
Click Edit and select Servers Confirm junction is running	
+ New 🖉 Edit 🛍 Delete	
Hostname Server State Server Operational S	State
♡ No filter applied	
O ms-exch2016.maas360swat.com running Online	

Step 13: Import SSL Certificate for Public Connection

This is the certificate of the hostname that mobile devices will connect to for SSL handshake

In this example, the SSL certificate is for the hostname: mail.maas360swat.com

- It is recommended to obtain an SSL certificate from a public CA for this purpose
- The certificate needs to be in a P12 format and protected with a password
- All certificates that are part of the chain should also be imported
- If required, a new CSR can be generated on the proxy using the proxy FQDN as the certificate request distinguished name (e.g. cn=mail.maas360swat.com)

Configuration						
System > Secure Settings > SSL Certificates Select pdsrv Click Manage > Edit SSL Certificate Database						
IBM Security Verify System ^		SSL Certificates	🖽 Replicate with	n Cluster		
System Settings	Secure Settings	☑ No filter applied		Edit SSL Certificate Database Edit Properties Details		
Date/Time	SSL Certificates	Certificate Database Name	* Type	Last Mo Describe Rename		
Administrator Settings	Eile Downloade	lmi_trust_store	Local	Export Mar 15, 2022, 1:30:08 PM		
Management Authentication	SSL Certificates Silent Configuration	pdsrv	Local	Mar 18, 2022, 12:18:33 PM		
Click on Personal Certificates Select Manage > Import						

		Configuration		
		Configuration		
	Edit SSL Certificat	e Database - pdsrv		
	+ New 🛛 🖉 Edit	Delete C Refresh	Manage ^	
	Signer Certificates	Personal Certificates Ce	view ertif Receive is	
	Label	Defau Issuer It	Import Export	
	♡ No filt	er applied	Load	
Import the SSL certifi Enter the password th Click Import Use a friendly Name f	cate for the data ir nat is used to prote ield when creating dron-down menu	iterface ct the certificate an SSL certificate as this options	s label is used display 1	the certificate
	Import Perso	onal Certificate	×	
	Type *			
	PKCS12			
	Certificate File	*		
	mail-server.pfx			
	Browse			
	Password			
		Impo	rt Cancel	
Confirm certificate wa Confirm certificate an	as imported Id associated signe	r certificates are present	t in the SSL store	
System No	otification The ma	anagement SSL certificate	was successfully upda	ited.
(B1) C E82 BEC 546	60BE23- .6-4A2E- .0-6C545B3 false .F4}	CN=R3,O=Let's Encrypt,C=US	CN=*.maas360swat.co	m
O R3-inte	er	CN=ISRG Root X1,O=Internet Security Research Group,C=US	CN=R3,O=Let's Encrypt,C	=US
O ISGR-r	oot	CN=ISRG Root X1,O=Internet Security Research Group,C=US	CN=ISRG Root X1,O=Inte Security Research Group,	rnet C=US

					Confi	guratio	on			
Re	view and	l deploy ch	anges							
							Deploy Pending	Changes	(< .
	•	Pending There is c	Changes currently one ur	ndeploy	ed cha	nge.	Modulo	Date Medified		
						-	Module	Date Mourred	11.08.04.48	
		Review Pe	ending Changes	5					Cancel Roll Back Deploy	<u> </u>
Re Se	start rev lect the r	erse proxy reverse pro	onstance if pro oxy instance ar	ompted nd click	Restar	t				
•	System Warnin Successfully de	ng × eployed all	Reverse Proxy + New & Edit Delete	► Start S	top U Restar	t 🛛 🕄 Refresh	Manage V Troublesh	nooting ~		
	pending chang The following r	jes. reverse	Instance Name		State	•	Changes are Active			
	proxy instance be restarted fo to take effect :	s need to or updates	♡ No filter applied					0	System Notification Successfully restarted the	×
	– mailproxy		✓ mailproxy		9	Started	🛦 False		proxy instance.	
Se Se Cli	lect the r ick Save	newly impo	orted certificat	е						
				Reverse Pr	oxy Basic C	onfiguratio	on - mailproxy			
				Server	SSL	Junction	Authentication			
				SSL						
				SSL Cer	tificate Key	File				
				pdsrv		~	Edit			
				Network	HSM Key F	ile				
						~	Edit			
				SSL Sen	ver Certifica	te	-			
				WebSE	AL-Test-Onl	3546F4} ^				
				{B160	BE23-E826-	4A2E-BEC0	-6C545B3546F4}			
		Donding	Chandaa				Deploy Pending	g Changes	×	1
	•	There is a	currently one u	ndeploy	/ed cha	nge.	Madula	Data Madified		
							Module	Date Mourieu	11.00.04.08	
		Review P	ending Change	S					Cancel Roll Back Deploy	
Re	start rev lect the r	erse proxy reverse pro	instance if pro	ompted	Restar	t				
	System Warni	ng ×	Reverse Proxy		neotai	<u> </u>				
	Successfully de pending chang	eployed all jes.	+ New 🖉 Edit 🕅 Delete	► Start S	top U Restar	t 🛛 🕄 Refresh	Manage ~ Troublesh	nooting 🛩		
	The following r proxy instance be restarted fo to take effect :	reverse is need to or updates	☐ Instance wante ∇ No filter applied		State		changes are Active	0	System Notification Successfully restarted the	×
	- mailproxy		mailproxy		Ø :	Started	🛕 False		proxy instance.	

Step 14: Validating Setup

Configuration
Browse to public interface (e.g. https://mail.maas360swat.com)
C A https://mail.maas360swat.com
Application Gateway Username Username Password Password Login
The SSL certificate being used can be verified
Page Info — https://mail.maas360swat.com/
Web Site Identity
Web site: mail.maas360swat.com
Owner: This web site does not supply ownership information.
Verified by: Let's Encrypt
Enter the Security Master credentials
Application Gateway Username: sec_master Password: Login
A successful logon will display the splash screen
C D C B https://mail.mass360swat.com IBM Security Verify Access

Page 34 of 76

Configuration					
Logout using the pkmslogin form (e.g. https://mail.maas360swat.com/pkmslogin.form)					
C A https://mail.maas360swat.com/pkmslogin.form					
Application Gateway					
pkmslogout logout the current user session (Not valid for clients who authenticate with Basic Authentication or SPNEGO. BA clients must exit their browser to properly terminate their session. SPNEGO clients must log off from their workstation) pkmspasswd change password for logged-in user					
Click logout and confirm user logged out					
Application Gateway User sec_master has logged out.					

Deployment Scenarios: Scenario 1: Any ActiveSync Client

Use-case:

This option is selected to expose ActiveSync traffic while keeping email servers internal to the network. EAG will forward the traffic from email clients to corporate email servers. EAG does not authenticate or authorize connections.

Workflow:

- ActiveSync traffic from any email client is forwarded from EAG to corporate email servers
- EAG does not authenticate any users before forwarding ActiveSync traffic
- Email servers will authenticate users

EAG Configuration:

	Configuratio	on
Web > Manage > Policy Administration Sign on with Security Master credent	on ials	
IBM Security Verify Access	Monitor V We	eb $ imes $ IBM Security Verify $$ System $ imes $
Policy Administration		
Task List		Security Verify Access Sign On
ACL > Create ACL ACL Name > mailproxy-unauthentica Description > allow unauthenticated Click Create	ted access to mail proxy	Secure Domain +User Id sec_master +Password ••••••••••••••••••••••••••••••••••••
Confirm ACL created		
Policy Administration		Create ACI
Task List User Group Object Space ACL Search ACLs Create ACL Import ACL Export All ACLs List Action Groups	Create ACL +ACL Name mailproxy-unauthenticated Description allow unauthenticated access to mail p Create Cancel	Proxy resou
ACL > Search ACL Click on the Search button Confirm new ACL is listed		
	Configuration	
---	---	
Policy Administration		
Task List	Search ACLs	
 User Group Object Space ACL Search ACLs Create ACL 	+ACL Name +Maximum Results + 100 Search 11 ACLs matched the search criteria Create Delete Export Options Filters	
Export All ACLs	Select ACL Name	
List Action Groups	default-comig	
▶ POP	default-gso	
▶ AuthzRule	default-management	
GSO Resource Secure Domain	default-management-proxy	
· Secure Domain	default-policy	
	default-replica	
	default-root	
	favicon	
	mailproxy-unauthenticated	
	Page 1 of 1 Total: 11	

Click on the link for the new ACL created

Under ACL Entries, click on Create Under Entry-Type, select Unauthenticated Check the Permissions T r x and click Apply Click Create Another Under Entry-Type, select Any-other Check the Permissions T r x and click Apply

Click Done

	ACL Properties							
	General Attach Extended Attributes							
	ACL Name mailproxy-unauthenticated							
	Description							
	allow unauthenticated access to mail proxy resou							
	ACL Entries							
	Create Delete							
	Select	Entry Name	Entry Type		Permissions			
		sec_master	User		Tc-mdbsvaB-RI			
			Any-other		Trx			
			Unauthenticat	ted	Тгх			
	Delete Clone	Export Cancel						
Object Space	> Browse Ob	ject Space						
Policy	Administration	1						
Task I	List			Browse Object Space				
▶ Use	r							
h Gro				Refresh Prune				
	oup			Deth ACI) ula		
♥ U0j	Jett Space			Faul ACL	FOF Autrize	uie		
DIC	awse Object Spa	auc Connon		+ / default-root				
Co	Dy/Paste Object	Space						

				Config	guration		
Evenend Object Cre							
Expand Object Spa	ice						
P	Rowse Ot	iect Sn	асе				
	101130 01	Jeer op	400				
	Refresh	Prune					
1			Path		ACL	POP	AuthzRule
6	= /				default-root		
	E N	lanagen	nent		default-management		
		/ebSEA	۸L		default-webseal		
		eag.n	naas360swa	at.com-mailpro	ху		
		벞	favicon.ic	0	favicon	favicor	1
			indov bt-	nl			
			mail				
		Å	nics				
			P.00				
			Pro Ob Ww De Ob C Ww Ob C Ww Ob C Ww Ob C Ww Ob C MW C C M C C C C C C C C C C C C C C	tected Object Pro ieneral Extende iject Name ebSEAL/eag.maas scription ject from host eag. Can Policy be a L Attached ilproxy-unauthentic P Attached thzRule Attached eate Child Object py Delete [erties d Attributes 360swat.com-mailproxy/mai maas360swat.com. ttached to this object ated Detach Attach t Export Cancel		
Browse Object Spa Confirm that the A Sign Off from Polic	ice and CL is as ly Admi	hit th socia nistra	e Refres ted to th tion	h button to e junction	refresh the ACL as	ssociat	tions to ju
	Refresh	Prune					
			Path		ACL default-root	POP	AuthzRule
	<u>н</u> м	anagem	ent		default-manadement		
	Ġ w	/ebSEAl	L		default-webseal		
	ė	eag.m	aas360swat	.com-mailproxy			
		Ē	favicon.ico		favicon	favicon	
		Ē	icons				
		Ш	index.html		and the second se		
			maii		maliproxy-unauthenticated		
		Ē	pics				

		Configuration	
If OWA is enabled, t unauthenticated AC	hen this is accessible wi L was added to the junc	ithout requiring entering credentials be tion	ecause the
Browse to the OWA	URL via EAG URL		
		(mail.maas360swat.com/mail/owa/auth/logon.aspx?replaceCurrent=18url=https%3a%: Domain/user name: Password:	

MaaS360 Configuration:

	Configuration						
To configure native	mail use the MaaS360 MDM policies						
Browse to Security Browse to Device S Configure the host Enable SSL The username and %email% etc. depe	> Policies on the MaaS360 portal and ed ettings > ActiveSync name to point to the data interface of EA email fields can be configured with wildo ending on the username format of email e	it the MDM Policy G (e.g. mail.maas360s card variables like %us environment	wat.com/mail) sername%,				
Save and publish th	Save and publish the policy						
	Configure ActiveSync Settings	v					
	Account Name for the ActiveSync Server End users will see the mailbox with this name.	MaaS360 EAG Email					
	Host Name of the ActiveSync Server mail.maas360swat.com/mail						
	Domain Name Leave this blank to use the enrollment information to populate the user's domain.						
	Account Username Leave this blank to use the enrollment information to populate the user's username. If Account Username is same as Email Address (such as Office365 or Traveler), use %email% as the variable.						
	Email Address Leave this blank to use the enrollment information to populate the user's email address						

Con	figuration
To configure MaaS360 Secure Mail use the MaaS	360 WorkPlace Persona policies
Browse to Security > Policies on the MaaS360 po Browse to Email > Configuration Configure the Mail Server to point to the data inte Enable SSL The username and email fields can be configured %email% etc. depending on the username formation	ortal and edit the WorkPlace Persona Policy erface of EAG (e.g. mail.maas360swat.com/mail) d with wildcard variables like %username%, at of email environment
Save and publish the policy	
Configure Secure Mail	
Mail Server	Exchange ~
Select the appropriate email server to ensure that the devices automatically. Auto Approval supported for Exchange, Office 3 IBM Connections Cloud.	get approved 65,IBM Traveler and
Hostname of the ActiveSync Server	mail.maas360swat.com/mail
Enter your Email Server URL.	
Use SSL	✓
Configure Secure Connection.	
Domain Name	
Leave this blank to use the user's domain name. If a usernam the field below and you need a domain name then enter that o %domain% to use user's domain.	e is being entered in Iomain name or
Email Address	
Leave this blank to use the user's email address.	
Account Username	
Leave this blank to use the username in this system. If Account as Email Address (such as Office365 or IBM Traveler) use %	nt Username is same mail% as the variable.
Once the policy has been pushed to the device the the connection to the email server (via the proxy	e email client will prompt for user credentials when) has been established

Scenario 2: MaaS360 Secure Mail only

Use-case:

This option is used if only the MaaS360 Secure Mail client is to be allowed while keeping corporate email servers internal to the network. Traffic from other email clients is blocked.

Workflow:

- ActiveSync traffic originating from only MaaS360 Secure Mail client is forwarded to corporate email servers
- Traffic from any other email client is blocked
- Email servers will authenticate users

EAG Configuration:

Configurat	ion
Complete all the steps for EAG configuration in Scenario) #1
Web > Manage > Reverse Proxy Select reverse proxy instance and click Manage > Config Search for text: [azn-decision-info] Copy this text: useragent = header:user-agent	guration > Edit Configuration File
Click Save	
Advanced Configuration File Editor - mailproxy	×
<pre>* mobileNumber = mobile * * * * * * * * * * * * *</pre>	nn which should when making van be obtained
Danding Changes	Deploy Pending Changes ×
There is currently one undeployed change.	Module Date Modified
Review Pending Changes	Cancel Roll Back Deploy
Restart reverse proxy instance if prompted Select the reverse proxy instance and click Restart	

			Confidurati	- n			
			Connguration	on			
		Reverse Proxy					
System Warning Successfully deployed	× ed all	+ New Z Edit Delete Start	Stop 🕐 Restart 🛱 Refresh	Manage V Troubleshooting V			
pending changes.		Instance Name	State	Changes are Active			
proxy instances need be restarted for under	e d to	∑ No filter applied			0	System Notification	×
to take effect :	ates		Startad	A Falco		Successfully restarted the proxy instance.	
– mailproxy		■ manproxy	Jailed	A Taise		proxy motaneor	
Web > Manage	e > Polic	y Administration					
Sign on with S	ecurity l	Master credentials	5				
	IB	M Security Verify Access	Monitor 🗸 🛛 We	eb 🗸 🛛 IBM Security V	erify	System ∽	
			I.				
	Pol	licy Administration					
	Tas	sk Liet		Security Verify Access	s Sian	On	
	105			Security verify Access	s sign	UII	
				Secure Domain			
				+User Id			
				sec_master			
				 Password 		_	
				•••••			
				Sign On			
!TRUE! Fail Reason: O)nlv Maa	S360 Mail Client A	llowed				
	Policy Admin	istration					
	Task List		Create AuthzRule				
	▶ User						
	 Group Object Spa 	200	 AuthzRule Name MaaS360-Mail-Only 				
	▹ ACL		Description				
	 POP AuthzRule 	•	Only Allow MaaS360	lail Client]	
	List Authz	Rules thzRule	 AuthzRule Text 				
	Import Aut	thzRule	<pre><xsl:if test='contain ITPUE!</pre></th><th>s(/XMLADI/useragent, "Ma</th><th>aaS36</th><th>0")'></xsl:if></pre>				
	 Export All GSO Resort 	authzKules					
	Secure Dor	main					
						li.	
			Fail Reason				
			Only MaaS360 Ma	I Client Allowed			
						1	
						////	
			Create Cancel				
Click Create							
Click Done							

	Conngui			
		 List of all Auth 	zRules	
1 The AuthzR	lule was created successfully	Create De	lete Export Opti	ions Filters
		Select	AuthzRule Na	ime
<u>Maass60-N</u>	<u>nali-Only</u>		laaS360-Mail-Only	
Create Anoth	ner			
Done		Page 1 of	1 Total 1	
wse Object Space and	locate the mail junction			
Policy Administration				
Task List	Browse Object Space			
User	Refresh Prune			
 Object Space 	P	ath	ACL	POP AuthzRule
Browse Object Space			default-root	
Create Object Space	H Management		default-management	
Import Object	WebSEAL	260owat com moilean	default-webseal	
ACL	eag.maas.	icon ico	favicon	favicon
▶ РОР		ons		
AuthzRule GSO Resource	in the second se	dex.html		
Secure Domain	🛨 ma	mail		
	+ pic	cs		
	Object Name	wat com-mailprov	w/mail	
	Description Object from host eag.maa Can Policy be attact ACL Attached mailproxy-unauthenticated	s360swat.com. hed to this objec	zi	
	Description Object from host eag.maa Can Policy be attack ACL Attached mailproxy-unauthenticated POP Attached AuthzRule Attached	s360swat.com. hed to this object Detach Attach	zi	
	Description Description Description Deject from host eag.maa Can Policy be attack ACL Attached mailproxy-unauthenticated POP Attached AuthzRule Attached MaaS360-Mail-Only Create Child Object	s360swat.com. hed to this object Detach Attach Detach		

	Browse Object Sp	ace				
	Refresh Prune					
		Path	ACL	POP	AuthzRule	-
	⊟ /		default-root			
	🕂 Manager	nent	default-management			
	WebSEA	AL.	default-webseal			
	😑 eag.r	naas360swat.com-mailproxy				
	(E)	favicon.ico	favicon	favicon		
	E E	icons				
		index.html				
	E	mail	mailproxy-unauthenticated		MaaS360-Mail-On	ly
	E E	pics				
estart the Runtime	Component					
Runtime Component	▶ Start Stop	rt 🛛 🖅 Replicate with Cluster 🗌 🛛	Manage 🗸		•	System Notification × Successfully restarted the runtime component.
Runtime Component	▶ Start ■ Stop 🕑 Restar	t 🗄 Replicate with Cluster 🗌	Manage 🗸		•	System Notification × Successfully restarted the runtime component.
Runtime Component	▶ Start Stop Restart ed using a local policy server an	t 🗄 Replicate with Cluster 🗌 1 d a local user registry.	Manage Y		•	Successfully restarted the runtime component.
Runtime Component	► Start Stop Or Restart red using a local policy server an	t EP Replicate with Cluster d a local user registry.	Manage Y		ľ	Successfully restarted the runtime component.
Runtime Component	Start Stop O Restart ■ Stop O Restart red using a local policy server and user Registr	t EP Replicate with Cluster d a local user registry. v.los.files.	Manage ~			Successfully restarted the runtime component.
Runtime Component	Start ■ Stop ⑦ Restarted using a local policy server and user Resistre e Mail Client i	t Replicate with Cluster 1 d a local user registry. vlog files. S allowed to cor	^{Manage} ∽ Inect via EAG F	Proxy		Successfully restarted the runtime component.

MaaS360 Configuration:

	Configuration		
To configure native	e mail use the MaaS360 MDM policies		
Browse to Security Browse to Device S Configure the host Enable SSL The username and %email% etc. dep Save and publish t	v > Policies on the MaaS360 portal and edi Settings > ActiveSync name to point to the data interface of EAC email fields can be configured with wildc ending on the username format of email e he policy	t the MDM Policy 6 (e.g. mail.maas360s ard variables like %us nvironment	wat.com/mail) ername%,
	Configure ActiveSync Settings	v	
	•		
	Account Name for the ActiveSync Server End users will see the mailbox with this name.	MaaS360 EAG Email	
	Host Name of the ActiveSync Server	mail.maas360swat.com/mail	
	Use SSL	✓	
	Domain Name Leave this blank to use the enrollment information to populate the user's domain.		
	Account Username Leave this blank to use the enrollment information to populate the user's username. If Account Username is same as Email Address (such as Office365 or Traveler), use %email% as the variable.		
	Email Address Leave this blank to use the enrollment information to populate the user's email address.		

Scenario 3: User Identification with LDAP Federation

Use-case:

This option is used to expose ActiveSync traffic and identify users before forwarding traffic to the corporate email servers, which remain internal to the corporate network.

EAG connects to corporate LDAP servers to identify users using corporate directory before allowing users to connect to mail servers.

Workflow:

- User identification takes place before traffic is forwarded to corporate email servers
- ActiveSync traffic from email client is forwarded to corporate email servers after successful user identification
- Email servers authenticate users

EAG Configuration:

To identify users against corporate credentials, the following set of tasks need to be completed on EAG:

- Configure LDAP Directory as EAG user registry
- Enable basic authentication for HTTPS junction
- Remove unauthenticated ACL

Configuration	
Complete all the steps for EAG configuration in Scenario #1 or #2	
Manage > Federate Directories	
Runtime Component © Configure © Unconfigure > Start = Stop © Restart = Replicate with Cluster = Status: Available Mode: The environment is configured using a local policy server and a local user registry. <u>Go to Application Log Files to view the Policy Server and User Registry log files.</u>	Manage Configuration Files Embedded LDAP Server Cleanup Federated Directories
Click New	
Federated Directories	
+ New 🖉 Edit 📋 Delete 🖉 SSL Settings 📿 Re	efresh
Name Suffix	

	Configuration
Enter details f	for the corporate directory server
Example Connect Name Hostname: ma Port: 389 Suffix: ou=ma Bind DN: cn=l	e: MaaS360 SWAT LDAP aas360swat.com aas360 users, dc=maas360swat, dc=com dapbinduser, cn=managed service accounts, dc=maas360swat, dc=com
Click Save	
	Name Mas360 SWAT LDAP Hostname * mas360wat.com Port * 389 Suffix * Cu=mas360wat,dc=com Bind DN unts_DC=mas360wat,DC=com Eind Password Eind Pas
/erify that the Click Close	e specific settings are correct
	Federated Directories X
	System Notification Successfully updated the directory X
	Name Suffix Server SSL V No filter applied Image: Suffix server ser
	MaaS360 SWAT LDAP ou=maas360 users maas360 swat,dc=com Bind DN: CN=LDAPBindUser,CN=Managed Service Accounts,DC=maas360ewat,DC=com
	1-1 of 1 item 10 25 50 100 All H < 1 → H

Configura	tion
Review and deploy changes	
Ponding Changes	Deploy Pending Changes ×
There is currently one undeployed change.	Module Date Modified
Review Pending Changes	Cancel Roll Back Deploy
Restart reverse proxy instance if prompted Select the reverse proxy instance and click Restart	
System Warning Successfully deployed all pending changes. × Reverse Proxy • New 2 Edit 10 Delete ► Start ■ Stop 10 Restart IC Ref	resh Manage ~ Troubleshooting ~
The following reverse proxy instances need to be restarted for updates to take effect : No filter applied	Changes are Active System Notification × Successfully restarted the
- mailproxy	▲ False proxy instance.
Manage >Configuration Files > ldap.conf	
Configuration Files pd.co Embedded LDAP ivrogradian Server Cleanup Idap. Federated Directories Tracin Search for basic-user-support and set value to yes # Basic user support enablement. Basic to # users without the need to import them to basic-user-support = yes	nf d.conf conf mg Configuration File user support allows the use of LDAP into IBM Security Verify Access.
Search for basic-user-principal-attribute = uid In this example, the corporate directory is Microsoft Ad mapped to userPrincipalName	ctive Directory, and the username attribute is
Copy this text and paste it at the bottom of the stanza Change this value from uid to userPrincipalName	under the suffix entry
[server:MaaS360 SWAT LDAP] host = maas360swat.com port = 389 bind-dn = CN=LDAPBindUser,CN=Managed Serv ssl-enabled = no suffix = ou=maas360 users ,dc=maas360swat	ice Accounts,DC=maas360swat,DC=com ,dc=com
<pre>basic-user-principal-attribute = userPrin Search for basic-user-no-duplicates attribute and set</pre>	cipalName /alue to no

	C	onfigurati	on			
<pre># If Ba: # dupli: # then # disab: # there # perfo: # the f: # optio: # to be # disab: # consi: basic-u:</pre>	sic user support is enabled, cate names are detected acro- the operation on the user wi- led, the server will not com are no duplicates. Disabli- rmance gains as the search a irst match user name is loca in is appropriate you must de unique, or whether security led then the basic-user-suff dered if duplicate user name ser-no-duplicates = no	this optio ss suffixes ll return a plete any c ng this opt cross each ted. To de termine whe requiremen ix-optimize s can be pr	n will contro . If a dupl: n error. If ross-suffix (ion allows f(suffix will : termine wheth ther user name ts allows for r enablement esent.	ol whether icate name this optio checks to e or signific stop immedi her disabli mes can be r duplicate must also	users with is detected, on is ensure that eant ately once ing this guaranteed es. If be	
Save Changes Review and deploy ch	nandes					
Dending (Changes		Deploy Pendin	g Changes		×
Pending There is c	currently one undeployed	change.	Module	Date Modified	1 11. Inc. Inc	
Review P	ending Changes				Cancel Roll Back Deplo	y
Restart reverse proxy Select the reverse pro	r instance if prompted bxy instance and click Re	start				
 System Warning Successfully deployed all pending changes. The following reverse proxy instances need to be restarted for updates 	Heverse Proxy + New ∠ Edit ① Delete > Start ■ Stop □ Instance Name ♡ No filter applied	() Restart C Refresh State	Manage V Troubles	ve	System Notification	×
to take effect : - mailproxy	✓ mailproxy	Started	▲ False		proxy instance.	
Web > Manage > Polic Sign on with Security	cy Administration Master credentials					
	IBM Security Verify Access Mo	onitor ~ We	eb ∽ IBM Seo	curity Verify	System \vee	
	Policy Administration		C	A		
	ask list	_	Secure Doma	Access Sign On	1	
]	
			+User Id		1	
			*Password			
			Size Or		J	
	Coorob		Sign On			
All directory users sh	ould show up in the list					
Policy Adm	inistration					
Task List		User Se	arch			
▼ User Search U	Isers	*User	ld *	Maximum F	Results	
Create U Import U	ser Jser	*	1	00	Search	
Show Gl Change I	obal User Policy My Password	75 use Create	rs matched th	ne search cr Or	riteria ptions Filters	

Configuration
Browse to public interface (e.g. https://mail.maas360swat.com)
Enter the UPN as a username to validate configuration Enter the password and click Login
Application Gateway
Username: swalker@maas360swat.com
Password:
Login
Enter the UPN as a username to validate configuration Enter the password and click Login Confirm login successful
Application Gateway
Your login was successful.
Logout using the pkmslogin form (e.g. <u>https://mail.maas360swat.com/pkmslogin.form</u>) Click logout and confirm user logged out
Application Gateway <u>pkmslogout</u> logout the current user session (Not valid for clients who authenticate with Basic Authentication or SPNEGO. BA clients must exit their browser to properly terminate
their session. SPNEGO clients must log off from their workstation) <u>pkmspasswd</u> change password for logged-in user User swalker@maas360swat.com has logged out.
Web > Manage > Policy Administration Sign on with Security Master credentials

			Con	figuration			
	IBM Security V	erify Ac	cess Monitor	r∨ Web	∨ IBM	Security Verify	System \checkmark
	Policy Administ	ration					
	Task List				Security Ve	rify Access Sigr	n On
					Secure Do	main	
					*User Id sec_maste	r	
					Passwore	••	
					Sign On		
					Sign On		
Browse Object	Space and lo	ocate	the mail junction	n			
Browse	e Object Space						
Refre	sh Prune						
Reine	F	Path		ACL		POP	AuthzRule
- /				default-root			
E E	Managemen	t		default-man	agement		
É	WebSEAL			default-web	seal		
	😑 eag.maa	s360sw	/at.com-mailproxy				
	÷ f	avicon.	ico	favicon		favicon	
	÷ i	cons					
	+ i	ndex.ht	ml				
		nail		mailproxy-u	nauthentic	ated	MaaS360-Mail-Only
	E p	ics					
Select mail and	d detach ACL	nding	00 1160 0360				
		ang	use case			_	
		Detacl	h ACL				
			Detach the 4	ACL from	the Ob	iect?	
		<u>_</u>	Detaen ine /				
			Detach				
			Cancel				
Refresh Object	Space and c	onfirn	n ACL removed				
	Refresh	Prune					
			Path	ACL default-root	POP	AuthzRule	
		/anageme	ent	default-manag	ement		
		VebSEAL	as360ewat.com maileron	default-websea	ıl		
			favicon.ico	favicon	favicor		
			icons				
		Ē	mail			MaaS360-Mail-O	Inly
		+	pics				

Configurat	ion
Web > Manage > Reverse Proxy Select instance and click Edit	
Reverse Proxy	
+ New 🖉 Edit 🗓 Delete	► Start Stop
Instance Name	
♡ No filter applied	
mailproxy	
Authentication > Basic Authentication > Transport > HT Click Save	TPS
Server SSL Junction Authentication Session	Response SSO Logging Interfaces
Basic Authentication	Forms Authentication
Transport HTTPS V	Transport HTTPS V
Review and deploy changes	
Deadlard Changes	Deploy Pending Changes ×
There is currently one undeployed change.	Module Date Modified
Review Pending Changes	Cancel Roll Back Deploy
Restart reverse proxy instance if prompted Select the reverse proxy instance and click Restart	
System Warning × Successfully deployed all pending changes. ×	sh Manage ~ Troubleshooting ~
The following reverse Instance Name State proxy instances need to be restarted for undates v No filter applied	Changes are Active System Notification ×
to take effect at a space of the space of t	▲ False proxy instance.

Connecting to LDAP over SSL

If SSL connection to LDAP is required, the SSL Certificate(s) associated to the LDAP server needs to be imported and the LDAP configuration needs to be setup to use SSL.

To complete this step, download and save the certificate(s) from the LDAP server:

The SSL certificate (public key) of the LDAP server will be known as *ldap-certificate.cer*

The SSL signer certificate of the issuing Certificate Authority (CA) will be known as *ldap-ca-certificate.cer*

	Config	uration		
ystem > Secure Setting	s > SSL Certificates			
elect pdsrv llick Manage > Edit SSL	Certificate Database			
IBM Security Verify	System ^	SSL Certificates		
	-,	+ New Delete SR	efresh 🗄 Replicate with Cluster 🔲 Manage ^ Edit SSL Cer	tificate Database
System Settings	Secure Settings	Certificate Database Name	Type Last Mo Describe	es
Date/Time	SSL Certificates	embedded_ldap_keys	Local Mar 15, 2 Import	
Administrator Setting	gs <u>File Downloade</u>	lmi_trust_store	Export Local Mar 15, 2022, 1:30:08	PM
Management Authen	tication Silent Configuration	n	Local Mar 18, 2022, 12:18:33	PM
lick on Signer Certificat	tes			
elect Manage > Import				
	Edit SSL Certificate Database	e - pdsrv		
	+ New / Edit III Dele	te D Refresh Man	ada 🛆	
		View	age	
	Signer Certificates Personal	Certificates Certif Rece	eive ¹⁴	
	Label	Issuer Expo	rt ort	
		Extra	act	
		1.030	4	
mport the signer certific	The interval of the LDAP server (Idd)	ıp-certificate.cer) a	and any relevant issuin	g CA
mport the signer certific igner certificate(s) lick Import and confirn	No filter applied cate of the LDAP server (Idd n certificate store updated Import Signer Certificate	ap-certificate.cer) a	and any relevant issuin	g CA
mport the signer certific igner certificate(s) lick Import and confirn	No filter applied Cate of the LDAP server (Idd n certificate store updated Import Signer Certificate Certificate File *	ap-certificate.cer) a	and any relevant issuin	g CA
mport the signer certific igner certificate(s) lick Import and confirn	No filter applied Cate of the LDAP server (Idd n certificate store updated Import Signer Certificate Certificate File * Idap-certificate.cer	up-certificate.cer) a	and any relevant issuin	g CA
mport the signer certific igner certificate(s) lick Import and confirn	No filter applied Cate of the LDAP server (Idd n certificate store updated Import Signer Certificate Certificate File * Idap-certificate.cer Browse	ap-certificate.cer) a	and any relevant issuin	g CA
mport the signer certific igner certificate(s) lick Import and confirn	No filter applied Cate of the LDAP server (Idde n certificate store updated Import Signer Certificate Certificate File * Idap-certificate.cer Browse Certificate Label *	ap-certificate.cer) a	and any relevant issuin	g CA
mport the signer certific igner certificate(s) lick Import and confirn	No filter applied Cate of the LDAP server (Idd n certificate store updated Import Signer Certificate Certificate File * Idap-certificate.cer Browse Certificate Label * LDAP	ap-certificate.cer) a	and any relevant issuin	g CA
mport the signer certific igner certificate(s) lick Import and confirn	No filter applied Cate of the LDAP server (Ida Import Signer Certificate Certificate File * Idap-certificate.cer Browse Certificate Label * LDAP	ap-certificate.cer) a	and any relevant issuin	gCA
mport the signer certific igner certificate(s) lick Import and confirn	No filter applied Cate of the LDAP server (Idd n certificate store updated Import Signer Certificate Certificate File * Idap-certificate.cer Browse Certificate Label * LDAP	ap-certificate.cer) a	and any relevant issuin	g CA
mport the signer certific igner certificate(s) click Import and confirm System Notific	No filter applied cate of the LDAP server (Idda n certificate store updated Import Signer Certificate Certificate File * Idap-certificate.cer Browse Certificate Label * LDAP	Import Cancel	as successfully update	gCA
mport the signer certific igner certificate(s) lick Import and confirm System Notific elect All option at the b	No filter applied Cate of the LDAP server (Idd n certificate store updated Import Signer Certificate Certificate File * Idap-certificate.cer Browse Certificate Label * LDAP ation The management bottom of the screen to view	Import Cancel SSL certificate wa	as successfully update	g CA
mport the signer certific igner certificate(s) lick Import and confirm System Notific elect All option at the b croll to bottom and con	No filter applied Cate of the LDAP server (Idd n certificate store updated Import Signer Certificate Certificate File * Idap-certificate.cer Browse Certificate Label * LDAP ation The management pottom of the screen to view firm that both certificates I cate, make sure the chain is	s present and impresent and im	as successfully update	g CA ed.
mport the signer certific igner certificate(s) lick Import and confirm System Notific elect All option at the b croll to bottom and con epending on the certific	No filter applied cate of the LDAP server (Ida n certificate store updated Import Signer Certificate Certificate File * Idap-certificate.cer Browse Certificate Label * LDAP ation The management oottom of the screen to view firm that both certificates I cate, make sure the chain is	Import Cancel SSL certificates oaded successfull s present and impo	and any relevant issuing as successfully update y ort any missing certifica	g CA ed.
mport the signer certific igner certificate(s) click Import and confirm System Notific elect All option at the b croll to bottom and con bepending on the certific	No filter applied cate of the LDAP server (Idal n certificate store updated Import Signer Certificate Certificate File * Idap-certificate.cer Browse Certificate Label * LDAP ation The management to view of the screen to extend the screen to view of the scree	Import Cancel SSL certificates oaded successfull s present and impo	and any relevant issuing as successfully update y ort any missing certifica	g CA ed. ates
mport the signer certific igner certificate(s) click Import and confirm System Notific elect All option at the b croll to bottom and con bepending on the certific	No filter applied cate of the LDAP server (Idal In certificate store updated Import Signer Certificate Certificate File * Idap-certificate.cer Browse Certificate Label * LDAP ation The management oottom of the screen to view firm that both certificates I cate, make sure the chain is 5 10 25 5	Import Cancel SSL certificate wa vall certificates oaded successfull s present and impo	and any relevant issuin as successfully update y ort any missing certifica	g CA ed. ates
mport the signer certific igner certificate(s) click Import and confirm System Notific elect All option at the b croll to bottom and con bepending on the certific	No filter applied cate of the LDAP server (Idal a certificate store updated Import Signer Certificate Certificate File * Idap-certificate.cer Browse Certificate Label * LDAP ation The management oview of the screen to view of the screen to the screen to view of the screen to view	Import Cancel SSL certificates SSL certificates Saded successfull s present and impo 50 100 All wat-MS-DC01- 60swat,DC=com	and any relevant issuing as successfully update y ort any missing certifica CN=maas360swat-MS- CA,DC=maas360swat.DS-	ed. ates
mport the signer certific igner certificate(s) click Import and confirm System Notific elect All option at the b croll to bottom and con bepending on the certific	No filter applied cate of the LDAP server (Idal a certificate store updated Import Signer Certificate Certificate File * Idap-certificate.cer Browse Certificate Label * LDAP ation The management option of the screen to view firm that both certificates I cate, make sure the chain is 5 10 25 10 25 10 25 CN=maas360s: CA,DC=maas360	Import Cancel SSL certificate wa vall certificates oaded successfull s present and import 50 100 All wat-MS-DC01- 60swat,DC=com	as successfully update yort any missing certifica CN=maas360swat-MS- CA,DC=maas360swat,D	ed. ates

			Configurat	ion			
				Deploy Pending Char	ndes	×	
	! Pending	Changes		bepies renaing ona			
	There is c	currently one und	eployed change.	Module Date	Modified	11.30.54.40	
	Review P	ending Changes					
De	etart roverse provi	v instance if prop	nted			Cancel Roll Back Deploy	
Se	lect the reverse prov	oxy instance and	click Restart				
	System Warning × Successfully deployed all	Reverse Proxy					
	pending changes.	+ New Z Edit I Delete	Start ■ Stop () Restart () Refre	sh Manage ∽ Troubleshooting ' Changes are Active	~		
	The following reverse proxy instances need to be restarted for undates	∑ No filter applied		•	0	System Notification	×
	to take effect :	✓ mailproxy	Started	🛕 False		proxy instance.	
w	eh > Manage > Run	time Component			-		
Ma	anage > Federated	Directories					
SS	L Settings > set ke	yfile > pdsrv					
Cl	ick Save						
			SSL Settings	×			
			directory is not configured to us	e SSL			
			Keyfile *				
			pdsrv 🔨	·			
-				Save Cancel			
Se	lect the federated	directory > Edit					
Cr	ange Port to 636						
Fr	iable 55L Iter hind nassword	> Save					
		Port *					
		636		Enable	le SSL		
Cl	ick Close						
Re	view and deploy cl	hanges					
				Deploy Pending Char	nges	×	
	Pending (Changes	anlowed change				
	There is c	urrently one und	eptoyed change.	Module Date	Modified	11.00.00.00	
	Deview D	anding Changes					
	Review P	ending Changes				Cancel Roll Back Deploy	
Re	estart reverse proxy	y instance if pron	npted				
Se	lect the reverse pr	oxy instance and	click Restart				
	System Warning × Successfully deployed all	+ New C Edit Delete	Start Stop (1) Destart S Defra		~		
	pending changes.	Instance Name	State	Changes are Active			
	The following reverse proxy instances need to be restarted for updates	₩ No filter applied			0	System Notification	×
	to take effect :	 mailproxy 	Started	▲ False		proxy instance.	

Configuration
Browse to public interface
(e.g. https://mail.maas360swat.com)
Enter the UPN as a username to validate configuration
Enter the password and click Login
Application Gateway
Username: swalker@maas360swat.com
Password:
Login
Enter the UPN as a username to validate configuration
Enter the password and click Login
Confirm login successful (splash screen displayed)
IRM Security Verify Access
IDM Security Verity Access
Logout using the pkmslogin form
(e.g. https://mail.maas360swat.com/pkmslogin.form)
Click logout and confirm user logged out
Application Gateway
Application Gateway
ptmslogout Nov valid for clents who authenticate with Basic Authentication or SPNEGO, BA clents exacted with the thermore to necessive torgenerate
their session. SPNEGO clients must log off from their workstation) User swalker@maas360swat.com has logged out.

MaaS360 Configuration:

Configuration

Same as scenario 2

Scenario 4: User Identification with Cloud Extender Identity Certificate Use-case:

This option is used to expose ActiveSync traffic and identify users using client identity certificates before forwarding traffic to the corporate email servers, which remains internal to the corporate network. EAG uses information in the certificate and validates against corporate directory before allowing users to connect to mail servers.

Mail servers will use the user corporate credentials to perform authentication.

MaaS360 Cloud Extenders should be implemented to integrate with corporate Certificate Authority (CA) using Direct CA integration to issue Identity Certificates to devices. This way, only MaaS360 enrolled devices access email. The email client can be native or MaaS360 Secure Mail client.

The client identity certificate is only used for identification against EAG. Directory credentials are used against the email server.

Workflow:

- User identification takes place before traffic is forwarded to corporate email servers
- Certificates are used to validate client identity and are provisioned to email clients (MaaS360 Secure Mail or native email) during MaaS360 enrollment
- ActiveSync traffic from email client is forwarded to corporate email servers after successful user identification



• Email servers authenticate users

To successfully identify users via certificates, EAG needs to be configured to communicate with the user registry (LDAP in this case).

EAG needs to be configured to extract the user information from the identity certificate and use this information to against the corporate directory.

This authentication mechanism is depicted in the workflow diagram below:

Identity Certificate Mapping in Email Gateway



MaaS360 Cloud Extender Configuration:

The first step is to setup the MaaS360 Cloud Extender to integrate with a Certificate authority to issue identity certificates to devices.

MaaS360 MDM or Persona policies need to be configured to use client identity certificate.

Setup MaaS360 Cloud Extender to integrate with a PKI.

In this step, it is important to configure the Subject Name of the certificate to contain the user Distinguished Name (DN) from the LDAP directory.

Detailed instructions on how to set this up is described in the IBM MaaS360's Knowledge Center page under <u>Certificate Integration Cloud Extender module.</u>

Configuration

From Cloud Extender select the Certificate Integration module.

		Confi	guratio	n					
		Certificate	e Integrat	ion					
		Securely deplo to mobile devi	oy identity ce ices	rtificates					
			~	:					
nce in the modu his action will o	ile, click "Add Ne pen the "Select y	ew Template". /our Enterprise C	Certific	ate Aut	hority ((CA)" p	anel belo	w.	
	Selec	t your Enterprise Cer	rtificate	Authorit	/ (CA)				
	O Micr	rosoft CA 🛛 🔿 Verizon		O Open Tr	ust				
	⊖ Sym	antec 🔿 Entrust		🔿 IDNomi	c - Mobile	Guard			
	⊖ Gen	eric 🔿 EST				3			
	Selec	t the purpose of issu	ing Ider	tity Cert	ificates				
	O Use Cre	r Authentication for Email, ates Device Identity Certif	Wi-Fi, VPN icates	, browser c	r reverse p	roxy.			
	. (Direct CA Certs Creates Device Identity	Certificate	s		.4			
		SCEP Creates Device Identity	Certificate	5					
	O S/M Cre	IIME encryption and digita ates User Identity Certifica	l signature ates	or user au	thenticatio	n.			
		-			Ne	xt			
lake the followi	ng selections on t	this panel and cl	ick "Ne	xt".	_	_			
Cloud Extender Configuration To	ol				_	п ×			
IOME IMPORT EXPORT P	Roxy settings help~			Eng	lish (United S	tates) v			
Certificate Integrati	on								
Securely deploy identity certificates	to mobile devices SCEP - Microsoft, Veriz	on. Open Trust server de	etails			U			
Start	Template Name	EAG Certificate Authentication	n				1		
	Hostname of SCEP server	http v host-1.maas360sw	at.com						
	SCEP Server challenge type	O Dynamic O Static O None							
2 SCEP Config	Challenge Username	maas360swat\mscepadmin							
	Challenge Password	•••••							
3 Cert Attributes									
4 Finish									
				Not	Savo	Cancal			

IE IMPORT EXPORT	PROXY SETTINGS HELP~		English (United Sta	tes) v	
ertificate Integra	tion			()	
	Certificate Properties				
Start	Subject Name 🕕	/CN=%dn%			
	Subject Alternate Name	UPN		~	
	Cache certs on Cloud Extender				
SCEP Config	Location of Certificate Cache	Choose a location to store cached certific		Browse	
4 Finish					
		Back	Next Save	Cancel	
ifigure the Su	ıbject Name of the c	ertificate to have the u	ser Distinguis	hed Nam	e (DN).

The Subject Name can be configured to contain any field. The Certificate Mapping rules in EAG needs to be modified accordingly.

In this example, we will use the user DN.

	Configuration	
	Certificate X	
	General Details Certification Path	
	Field Value ^	
	Serial number 15 00 00 02 6 1f 11 b9 db bf Signature algorithm sha256RSA	
	Signature hash algorithm sha256	
	Valid from Wednesday, November 23, 20	
	Valid to Thursday, November 23, 2017	
	CN = Test User 1,CN=Users,DC=maas360swat.com	
	Edit Properties Copy to File	
	OK	
The issued certificate will lo	ok like this.	<u> </u>
The Subject Name will have	the user DN	
<xmlumi></xmlumi>		
< Certificate Example A!>		
<stsuuser:stsunversaluser xr<br=""><stsuuser:principal></stsuuser:principal></stsuuser:stsunversaluser>	hins:stsuuser="urn:ibm:names:11F1M:1.0:stsuuser">	
	<stsuuser:attribute name="name"></stsuuser:attribute>	
<stsi< td=""><td>user:Value>CN=Test User 1CN\=UsersDC\=maas36</td><td>Oswat.com</td></stsi<>	user:Value>CN=Test User 1CN\=UsersDC\=maas36	Oswat.com
<td>ribute></td> <td></td>	ribute>	
<stsuuser:attributelist< td=""><td></td><td></td></stsuuser:attributelist<>		
<stsuuser:attr< td=""><td>ibute name="SubjectCN"</td><td></td></stsuuser:attr<>	ibute name="SubjectCN"	
type="urn:ibm:security:gskit">		
<stsi< td=""><td>iuser:Value> Test User 1CN\=UsersDC\=maas360sv</td><td>vat.com</td></stsi<>	iuser:Value> Test User 1CN\=UsersDC\=maas360sv	vat.com
<td>></td> <td></td>	>	
This certificate when presen	ted to EAG is represented in an XML format.	
The costion marked in blue :	a attribute that EAC people to extracted prese	dy formattad and compared
against the user	s attribute that EAG needs to extracted, proper	ty formatted and compared
Distinguished Name (DN) on	LDAP.	

EAG Configuration:

To configure EAG to use certificates the following steps needs to be completed:

- Enable Client Certificates
- Setup Certificate Mapping

Enable Client Certificates:

Configuration			
From IBM Security Verify Access Local Manageme	nt Interface		
Reverse Proxy Basic Configuration - mailproxy	Help ?	×	
Server SSL Junction Authentication Session Response SSO	Logging Interfaces		
Basic Authentication	Forms Authentication	·	
Transport	Transport		
HTTPS ~	HTTPS V		
Realm Name			
Token Authentication			
Transport			
None			
	Save	ət.	
Reverse Proxy Basic Configuration - mailproxy		×	
		Help ?	
Course COL Duration Automatication Courses COL	harden behaltere		
Client Certificates	Kerberos	^	
Accept Client Certificates	Transport None		
Forward and Ford	Kontak Ella		
0			
Certificate FAI URI	Use Domain Qualified Name		
Contribute and One			
	Kerberos Service Names		
Certificate Data			
+ New B Delete	+ New Delete T Default		
	Value	~	
		Save Cancel	
Browser to Web >Reverse Proxy			
Select the provy instance and click Edit			
Select the proxy instance and title Eult			
On Authentication, set Basic Authentication >> Tra	insport = HTTPS		
Set Client Certificates >> Accept Client Certificates	= Required		
Click Sava			
CIICK JAVE			

	Configuration
•	Pending Changes There is currently one undeployed change. Review Pending Changes
	System Notification × Successfully submitted changes to configuration.
	view Pending Changes to deploy changes.
	Deploy Pending Changes ×
	ModuleDate ModifiedReverse Proxy Configuration FileJul 12, 2022, 2:59:38 PM
	Cancel Roll Back Deploy
Deploy and	Restart the reverse proxy instance

Setup Certificate Mapping:

EAG needs to be configured with a transformation rule (XSL) that extracts the Subject Name from the Identity Certificate and compares that against the LDAP attribute of the user

This XSL rule is depicted here and the same is available as XSL-Template.txt in the EAG download media



```
<!-- XSL-Template.txt -->
 <xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:stsuuser="urn:ibm:names:ITFIM:1.0:stsuuser"
version="1.0">
          <xsl:output method="text" omit-xml-declaration="yes"
 encoding='UTF-8' indent="no"/>
          <xsl:template match="text()"/>
          <xsl:template
 match="/XMLUMI/stsuuser:STSUniversalUser/stsuuser:AttributeList">
                   <xsl:variable name="subjectCN">
                            <xsl:call-template name="tokenize">
                                          <xsl:with-param name="rawSubjectCN"
 select="stsuuser:Attribute[@name='SubjectCN']/stsuuser:Value"/>
                            </xsl:call-template>
                   </xsl:variable>
                    <xsl:choose>
                            <xsl:when test="starts-with($subjectCN,'CN=')">
                          !<xsl:value-of select="$subjectCN" />!
                            </xsl:when>
                             <xsl:otherwise>
                             <xsl:choose> <xsl:when test="contains($subjectCN,',')">
                                       <xsl:choose>
<xsl:when test="contains($subjectCN,'.com')"> !CN=<xsl:value-of select="substring- before($subjectCN,'.com')"/>,DC=com!
               </xsl:when>
                            <xsl:otherwise> !CN=<xsl:value-of select="$subjectCN" />!
                            </xsl:otherwise>
                                      </xsl:choose>
                                          </xsl:when>
                            <xsl:otherwise>
                               <xsl:choose>
                  <xsl:when test="contains($subjectCN,'.com')"> !<xsl:value-of select="$subjectCN" />!
               </xsl:when>
                             <xsl:otherwise> !CN=<xsl:value-of select="substring before($subjectCN,'.com')"/>.DC=com!
          </xsl:otherwise>
                                        </xsl:choose>
                                  </xsl:otherwise>
                             </xsl:choose>
                     </xsl:otherwise>
 </xsl:choose> </xsl:template>
          <xsl:template name="tokenize">
                   <!-- this template removes backslashes, might be
 not needed -->
                   <xsl:param name="rawSubjectCN" />
                   <xsl:variable name="first-item" select="normalize-
 space(substring-before(concat($rawSubjectCN, '\'), '\'))" />
                   <xsl:if test="$first-item">
                            <item>
                                             <xsl:value-of select="$first-item"
 />
                             </item>
                            <xsl:call-template name="tokenize">
                                          <xsl:with-param name="rawSubjectCN"
 select="substring-after($rawSubjectCN,'\')" />
                           </xsl:call-template>
                   </xsl:if>
         </xsl:template>
 </xsl:stylesheet>
 XSL Template can be modified from the IBM Security Verify Access management interface. See steps below.
```

	Global Settings	Global Keys	API Access Control		
Runtime Component	URL Mapping	SSO Keys	Resources		
Reverse Proxy	Junction Mapping	LTPA Keys	Policies		
uthorization Server	Client Certificate Mapping		CORS Policies		
)istributed Session Cad	he User Name Mapping				
olicy Administration	Password Strength				
	Forms Based Single Sign-on				
	HTTP Transformation				
	Kerberos Configuration				
	RSA SecurID Configuration				
	Rate Limiting				
	Redis Configuration				
+ New 2 Edit	🖻 Delete 😋 Refresh Ma	nage ~			
to access the XSL	Template				
Create Content: * Content: * Cont	Template - XLS-Template.txt> 1:stylesheet xmlns:xsl="http://www 1:output method="text" omit-xml-de oding='UTF-8' indent="no"/> 1:template match="text()"/> 1:template ch="xMLUMI/stsuuser:STSUniversalU 1:variable name="subjectCN"> 1:call-template name="tokenize"> 1:wariable name="subjectCN"> 1:wariable name="subjectCN"> 1:wariable name="subjectCN"> 1:wariable name="subjectCN"> 1:wariable name="subjectCN"> 1:wariable name="subjectCN">	1.w3.org/1999/XSL/ claration="yes" Jser/stsuuser:Attr: jectCN']/stsuuser	Transform" xmlns:stsu ibuteList"> :Value"/> <th></th> <th></th>		
Create Content: * Content: * Cont	Template - XLS-Template.txt> 1:stylesheet xmlns:xsl="http://www 1:output method="text" omit-xml-de oding='UTF-8' indent="no"/> 1:template match="text()"/> 1:template match="text()"/> 1:template name="subject(N"> 1:variable name="subject(N"> 1:variable name="subject(N"> 1:variable name="subject(N"> 1:variable name="subject(N"> 1:with-param name="rawSubject(N" ect="stsuuser:Attribute[@name='Sub sl:variable> <xs sl:value-of select="\$subject(N" /> sl:when> 3360DN</xs 	/.w3.org/1999/XSL/ claration="yes" lser/stsuuser:Attr: jectCN']/stsuuser :l:choose> <xs: !</xs: 	Transform" xmlns:stsi ibuteList"> :Value"/> 1:when test="starts-: >		
Create Content: * Cont	Template - XLS-Template.txt> 1:stylesheet xmlns:xsl="http://www 1:output method="text" omit-xml-de oding='UTF-8' indent="no"/> 1:template match="text()"/> 1:template catch="text()"/> 1:template name="subjectCN"> 1:call-template name="tokenize"> 1:wariable name="subjectCN"> 1:wariable name="subjectCN"> 1:wariable name="subjectCN"> 1:wariable name="subjectCN"> 1:wariable name="subjectCN"> 1:wariable name="subjectCN"> 1:wariable name="subjectCN"> 1:wariable name="subjectCN"> 1:wariable name="subjectCN"> 1:wariable> 	/.w3.org/1999/XSL/ claration="yes" /ser/stsuuser:Attr: /jectCN']/stsuuser il:choose> <xs: !</xs: 	<pre>Iransform" xmlns:stsu ibuteList"></pre>		
o access the XSL Create Content: * (1- (xs) enc (xs) (xs) enc (xs) (xs) (xs) (xs) (xs) (xs) (xs) (xs)	Template - XLS-Template.txt> 1:stylesheet xmlns:xsl="http://www 1:output method="text" omit-xml-de oding='UTF-8' indent="no"/> 1:template match="text()"/> 1:template ch="/XMLUMI/stsuuser:STSUniversalU 1:variable name="subjectCN"> 1:variable>	<pre>r.w3.org/1999/XSL/ claration="yes" lser/stsuuser:Attr: ijectCN']/stsuuser il:choose> <xs: !</xs: </pre>	Transform" xmlns:sts: ibuteList"> :Value"/> 1:when test="starts-: > OK Cance		
o access the XSL Create Content: * Content:	Template - XLS-Template.txt> 1:stylesheet xmlns:xsl="http://www 1:output method="text" omit-xml-de oding='UTF-8' indent="no"/> 1:template match="text()"/> 1:template match="text()"/> 1:template name="subjectCN"> 1:call-template name="subjectCN"> 1:with-param name="subjectCN"> 1:when> 1:when> 1:when> 1:Not not not not not not not not not not n	/.w3.org/1999/XSL/ claration="yes" Jser/stsuuser:Attr: jectCN']/stsuuser :1:choose> .1: clear the cou	Transform" xmlns:sts: ibuteList"> :Value"/> 1:when test="starts-: 	een and paste	e the c



EAG Federation Configuration:

In this step, EAG needs to be configured to integrate with a corporate directory

Follow the steps in Scenario 3 to connect EAG to LDAP

MaaS360 Configuration:

# Configuration	Screenshot	
 If native email needs to be configured on end user devices, MaaS360 MDM policies need to be configured. Browse to Security >> Policies on the MaaS360 portal. On iOS, Android or Windows MDM policy, browse to Device Settings >> ActiveSync 		
point to the data interface of	Configure ActiveSync Settings	Yes
EAG	Ξ	
(mail.maas360swat.com)	Account Name for the ActiveSync Server End users will see the mailbox with this name.	MaaS360 EAG Email
• Enable SSL	Host Name of the ActiveSync Server	mail.maas360swat.com
• The username and email	Use SSL	Yes
fields can be configured with wildcard variables. Use	Domain Name Leave this blank to use the enrollment information to populate the user's domain.	
%email% or %upn% for both Username and Email Address field since this user	Account Username Leave this blank to use the enrollment information to populate the user's username. If Account Username is same as Email Address (such as Office365 or Traveler), use %email% as the variable.	%email%
authentication is now configured to use UPN	Email Address Leave this blank to use the enrollment information to populate the user's email address.	%email%
 Leave Domain Name as blank. 	Synchronize Emails for the Selected Date Range	
• Save and Publish the policy	Identity Certificate	EAG Certificate Authentication
If MaaS360 Secure Mail needs to be configured on end user devices, MaaS360 Persona policies need to be configured. Browse to <i>Security >> Policies</i> on the MaaS360 portal. • On persona policy, browse to <i>Email >> Configuration</i>		
Configure the hostname to point	Configure Secure Mail	
to the data interface of EAG	Mail Server Select the appropriate email server to ensure that the devices get approved automatically. Auto Approval supported for Exchange, Office	Exchange
(maii.maas360swai.com)	Hostname of the ActiveSync Server	mail.maas360swat.com/mail
• The username and email	Enter your Email Server URL.	Yes
fields can be configured with	Configure Secure Connection.	
wildcard . Use %email% or	Domain Name Leave this blank to use the user's domain name. If a username is being entered in the field below and you need a domain name then enter that domain name or %domain% to use user's domain.	
and Email	Account Username Leave this blank to use the username in this system. If Account Username is same as Email Address (such as Office365 or IBM Traveler) use %emal% as the variable.	%email%
Address field since this user	Email Address Leave this blank to use the user's email address.	%email%
to use UPN	Authentication Type	Certificate
• Leave Domain Name as blank.	Identity Certificate	EAG Certificate Authentication

 Set Authentication Type to Password. Save and Publish the policy 		



Scenario 5: Kerberos Constrained Delegation

Use-case:

This option is used if to expose ActiveSync traffic and identify users before forwarding traffic to the corporate email servers, which remains internal to corporate network. In this option, EAG performs user identification and once successful attaches a Kerberos Token to the ActiveSync traffic that gets forwarded to the email servers.

The email servers will use the Kerberos token that it receives along with the ActiveSync traffic to authenticate the users.

MaaS360 Cloud Extenders should be implemented to integrate with a corporate Certificate Authority (CA) to issue Identity Certificates to devices. This way, only MaaS360 enrolled devices access email if email is configured via MaaS360 policies. The email client can be native or MaaS360 Secure Mail client.

The client identity certificate is only used for identification. Directory credentials are used against the email server. The client identity certificate used will not be passed onto the email server.

Workflow:

- User identification takes place before traffic is forwarded to corporate email servers
- Certificates are used to validate client identity and are provisioned to email clients (MaaS360 Secure Mail or native email) during MaaS360 enrollment
- EAG attaches Kerberos tickets for corporate email servers along with the forwarded ActiveSync traffic
- ActiveSync traffic from email client is forwarded to corporate email servers after successful user identification
- Corporate email servers will validate the Kerberos tickets and not perform any secondary authentication. The authentication operations are delegated to EAG for optimized corporate directory performance

EAG Configuration:

To configure EAG to use Client Identity Certificates the following steps needs to be completed:

- 1. Setup Cloud Extender for Direct Certificate Authority Integration
- 2. Setup Certificate Mapping
- 3. Configure Kerberos Constrained Delegation
- 4. Enable Kerberos SSO for HTTPS junction

#	Configuration	Screenshot			
	Complete all the steps for EAG configuration in Scenario #4. This covers Steps 1 – 3 above.				
	Ensure that ActiveSync application on the server is configured for Kerberos authentication.	€ € • • Host-2 • Sit File View Help	es → Default Web Site → Microso	ft-Server-ActiveSyr	nc 🕨
	In Microsoft IIS, set the permission on MS-Server-ActiveSync site to have	Connections S	Authentication		
Wi	Windows Authentication enabled	> 1-2 (MAAS360SWAT\ad_admin) > Application Pools Sites Image: Site particular spectrum > Image: Site particula	Name Anonymous Authentication ASP.NET Impersonation Basic Authentication Digest Authentication Forms Authentication Windows Authentication	Status Disabled Disabled Disabled Disabled Disabled Enabled	Response Type HTTP 401 Challenge HTTP 401 Challenge HTTP 302 Login/Redirect HTTP 401 Challenge

Ensure that Negotiate:Kerberos is listed as an available provider for				
Windows Authentication.	Group by: No Grouping			Alerts Click here to learn how to configure Extended Protection.
	Name Anonymous Authentication ASP.NET Impersonation	Status Disabled Disabled	Response Type Providers ? ×	Actions Disable
If it is not listed, add	Basic Authentication Digest Authentication Forms Authentication	Enabled Disabled Disabled	Enabled Providers: Move Up	Advanced Settings Providers
Negotiate:Kerberos provider to the list.	Windows Authentication	Enabled	Maye Down Remove	
Restart IIS after the changes are made			Select a provider from the list of available providers and click Add to add it to the enabled providers. Available Providers:	
			Negotiste/Korberos v Add	

Identify a domain user that can be	
used as a service account in EAG to	
used as a service account in EAG to request Kerberos service tickets	Published Certificates Member Of Password Replication Dial-in Object Security Environment Sessions Remote control Remote Desktop Services Profile COM+ Attribute Editor General Address Account Profile Telephones Organization Image: EAG Bind User Initials: Image: Image
	OK Cancel Apply Help
Before generating the Kerberos keytab file, review the chosen account for any existing service principal names (SPN). The expected result is that no existing SPN is found.	C:\>setspn -L eag-binduser Registered ServicePrincipalNames for CN=eag-binduser C:\>_
Command : setspn -L eag-binduser	



Add another SPN of the service account user: HTTP/eag- binduser@maas360swat.com@MA AS360SWAT.COM setspn -S HTTP/eag- binduser@maas360swat.com@MA AS360SWAT.COM maas360swat\eag-binduser	C:\Windows\system32>set Checking domain DC=maas Registering ServicePrin C=com HTTP/eag-bindus Updated object C:\Windows\system32>	Administrator: Command spn -S HTTP/eag-binduser@ 369swat,DC=com cipalNames for CN=EAG Bind er@MAAS360SWAT.COM	Prompt 19A83608WAT.Com User,CN=Users	eag-binduser
Review the configured service principal names (SPN). Command: setspn -L eag-binduser	Ca. Microsoft Windows [Uer (c) 2013 Microsoft Cor C:\Windows\system32>se Registered ServicePrin =con: HITP/eag-bindu HITP/ag-bindu C:\Windows\system32>	Administrator: Command sion 6.3.96001 poration. All rights resen tspn -L eag-binduser tipalNames for CN=EAG Bind ser@maas360swat.com@MAAS36 ser	d Prompt rved. d User,CN=User: GØSWAT.COM	■ □ × = s,DC=maas360swat,DC
Configure Kerberos Realm: Browse to Web > Global Settings >> Kerberos Configuration.	Web ^ IBM Security Ver Manage Runtime Component Reverse Proxy Authorization Server Distributed Session Cache Policy Administration	ify System ✓ Global Settings URL Mapping Junction Mapping Client Certificate Mapping User Name Mapping Password Strength Forms Based Single Sign-on HTTP Transformation HTTP Transformation RSA SecurID Configuration RSA SecurID Configuration Rate Limiting Redis Configuration	Global Keys SSO Keys LTPA Keys	API Access Control Resources Policies CORS Policies

Click Realm , select New >> Realm Enter the Kerberos realm, this value can be the directory domain name. Do not use spaces in the Realm Name	Kerberos Configuration Defaults Realms Domains CA Paths Keyfiles New ~	
Hit Save	Create New Realm ×	
Deploy pending changes and restart reverse proxy for changes to take effect.	Realm * maas360swat.com Save Cancel	
Select the new realm and look for the "New" pulldown just above the name.		
	Kerberos Configuration Defaults Realms Domains CA Paths Keyfiles New ~	
	🖻 maas360swat.com	
Click <i>New > Property</i>		
	Kerberos Configuration	
	Defaults Realms Domains CA Paths Keyfiles	
	New 🔨 🖉 Edit 🗇 Delete 😰 Test 😒 Refresh	
	Subsection Property	
In the Create New Proper select kdc Enter the Directory KDC add Value field. The Directory KI is the name of the domain of For example, <machine>.<domain>, click Note that using port 88 is of Active Directory as this is de value Depending on the configura the domain name may be a preferred option instead of only a single directory server. In this example, the maas360swat.com Deploy changes.</domain></machine>	rty window, Iress in the DC address ontroller. a Save btional for efault tion, using more linking to setting is :	Create New Property Pre-Defined Names admin_server auth_to_local default_domain kdc kpasswd_server master_kdc v4_realm Name * kdc Value * host-1.maas360swat.com:88 Save
---	--	--
The following realm is now	created	Kerberos Configuration Defaults Realms Domains CA Paths Keyfiles New C Edit Delete Test Refresh maas360swat.com kdc = host-1.maas360swat.com:88
On Keytiles , click on the Im button to import the keytab was generated for the EAG account user	p ort file that service	Kerberos Configuration Defaults Realms Domains CA Paths Keyfiles + Import Import Delete Import Combine Refresh Name Import keytab file X Modified Import keytab file X Select the keytab file to import * 0 item eag-binduset.keytab Select Files Import Import Cancel Import Cancel

Deploy the pending changes.	Deploy Pending Changes × Module Date Modified Kerberos Keytab File Jul 12, 2022, 5:23:21 PM Cancel Roll Back Deploy System Notification × Successfully imported the keytab File
On Defaults, select the default_realm item, Edit and set the value to the newly created Kerberos realm on the pull down.	Kerberos Configuration Defaults Realms Domains CA Paths Keyfiles Mame Value Value </td
Deploy the pending changes and restart the reverse proxy instance	
Select Keyfiles , select the keytab file and test authentication with the recently configured SPN: <u>HTTP/eag-</u> <u>binduser@MAAS360SWAT.COM</u>	Kerberos Configuration Defaults Realms Domains CA Paths Keyfiles + Import Delete Combine Test Refresh Name Last Modified V No filter applied Test keytab authentication
If the setup is correct, a successful	eag-binduser.keytab Principal Name *

HTTP/eag-binduser@MAAS360.(

Test Cancel

1 - 1 of 1 item

test action notification is shown

IBM MaaS360 Email Access Gateway

Confirm Kerberos authentication is working as expected for any user Select the newly configured Realm from Realms and click Test Enter the valid credentials for a user in the corporate directory in the format <u>user@DOMAIN.NAME</u> Confirm test is successful.	Kerberos Configuration Defaults Realms Domains CA Paths Keyfiles New C Edit Image: Delete Image: Test Refresh Image: mass360swat.com Test Kerberos Authentication X Username * anyuser01@MAAS360SWAT.CoN Password * Image: Delete Password *
	Test Cancel
Browser to Web > Manage > Reverse Proxy	Advanced Configuration File Editor - mailproxy ×
Select the reverse proxy instance.	# We only want to listen on our management interfaces.
Click Manage >> Configuration >> Edit Configuration File.	# JUNCTION # JUNCTION # Location of the Junction to Request Mapping Table (JMT)
Locate the [junction] stanza.	<pre># This path is relative to the server-root value in the [server] stanza # The following files are currently available for this configuration entry: # - jmt.conf </pre>
	Save Revert Cancel
Update the following properties:	
kerberos-sso-enable = true	Advanced Configuration File Editor - mailproxy X
	<pre># '(jct-id)' refers to the junction point for a standard junction (include the # leading '/'), or the virtual host label for a virtual host junction. kerberos-sso-enable = true</pre>
kerberos-keytab-file = eag- binduser.keytab	<pre># The name of the Kerberos key table file for the WebSEAL server. This stanza # entry is required when Kerberos SSO authentication for junctions is enabled. # The keytab file must contain the key for the service-principal-name (SPN) # used for Kerberos authentication.</pre>
	<pre># The following files are currently available for this configuration entry: # - eag-binduser.keytab</pre>
	kerberos-keytab-file = eag-binduser.keytab # The Kerberos SPN. used as the impersonating user when creating the token. The
	Save Revert Cancel

Update the following properties: kerberos-principal-name = <u>HTTP/eag-</u> <u>binduser@MAAS360SWAT.COM</u> kerberos-service-name = <u>HTTP/host-</u> <u>2.maas360swat.com@MAAS360SW</u> <u>AT.COM</u> Note that these values are replaced with those specific to the current implementation		Advanced Configuration File Editor - mailproxy # The Kerberos SPN, used as the impersonating user when creating the token. The # service principal name can be determined by executing the Microsoft utility # secount). # format is: Kerberos-principal-name = HTTP/ <username>@<realm> # This stanza entry is required when Kerberos SSO authentication for junctions # is enabled. Advanced Configuration File Editor - mailproxy Metros-principal-name = HTTP/eag-binduser@MAAS3605NAT.COM Advanced Configuration file Editor - mailproxy Metros-principal-name = HTTP/eag-binduser@MAAS3605NAT.COM Metros-principal-name = HTTP/eag-binduser@MAAS3605NAT.Com # The Kerberos SSN for the back-end Web server. The service principal name can # be determined by executing the Microsoft utility setspn (that is, setspn -1: user, where user is the identity of the back-end Web server's account). # This configuration item may be customized for a particular junction by adding the adjusted configuration item to a [junction](jci_j]) starg, where # '(jct-id)' refers to the junction point for a standard junction (include the leading '/); or the virtual host label for a virtual host junction # Kerberos-service-name = HTTP/cusername>@crealm> # the starge service-name = HTTP/cusername>@crealm> # the adjusted configuration item to a [junction](jci_j]) starg, where # '(jct-id)' refers to the junction point for a standard junction (include the leading '/); or the virtual host label for a virtual host junction # This starge entry is required when Kerberos SSO authentication for junctions # kerberos-service-name = HTTP/cusername>@crealm> # This starge entry is required when Kerberos SSO authentication for junctions # is enabled.</realm></username>
Deploy changes and restart the reverse proxy instance	Test authentication with MaaS360 Secure Mail. Authentication should succeed with certificates and the end user should not be prompted for a password.	

MaaS360 Configuration:

MaaS360 configuration remains the same as Scenario #4	