

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
Scenario 3: User Identification with LDAP Federation.....	45
Use-case:.....	45
Workflow:	45
EAG Configuration:	45
Connecting to LDAP over SSL.....	51
MaaS360 Configuration:	54
Scenario 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
Scenario 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

Note:

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

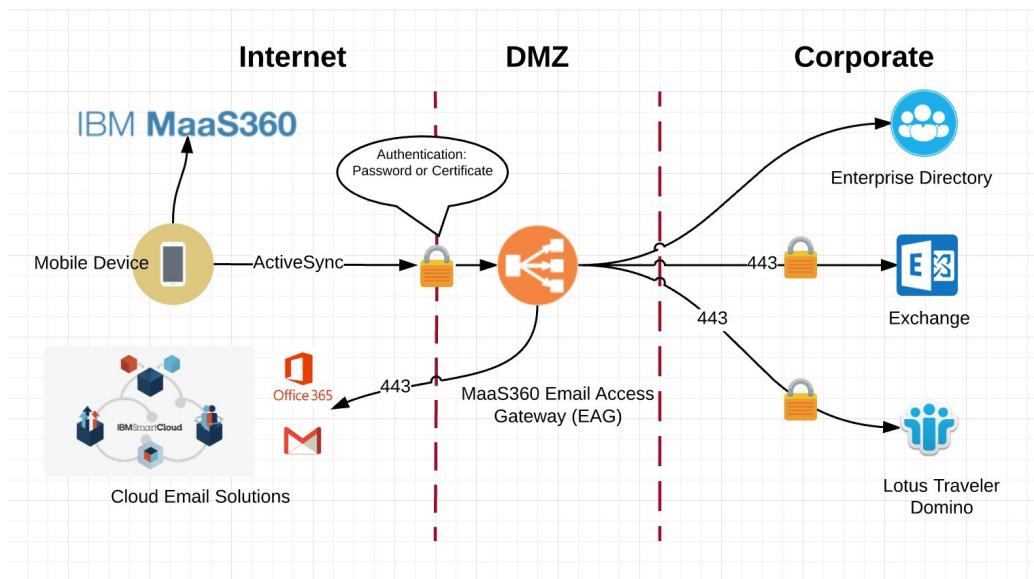
<https://docs.microsoft.com/en-us/outlook/troubleshoot/profiles-and-accounts/outlook-cannot-use-activesync-connect-exchange>

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
 - 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	<p>Workflow:</p> <ul style="list-style-type: none"> 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 <p>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.</p>
2	MaaS360 Secure Mail Only	<p>Workflow:</p> <ul style="list-style-type: none"> 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 <p>Use-case: This option is used to expose ActiveSync for only MaaS360 Secure Mail clients while keeping corporate email servers internal to the network.</p>
3	User Identification LDAP Federation	<p>Workflow:</p> <ul style="list-style-type: none"> 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 <p>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.</p>
4	User Identification Cloud Extender Identity Certificate	<p>Workflow:</p> <ul style="list-style-type: none"> 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 <p>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.</p>

5 Kerberos Constrained Delegation

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
- 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 EAG

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

Type	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

Type	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

Type	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

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

Step 4: Configure Virtual Appliance

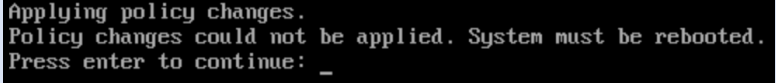
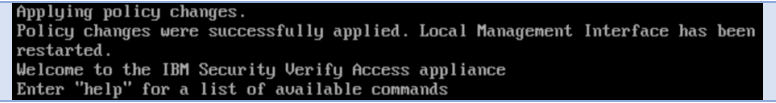
Configuration	Screenshot
<p>A flashing cursor may be seen</p> <p>The following prompt will appear</p>	
<p>Login to the console using the administrator user id admin and the default password of admin</p> <p>After the firmware has been loaded onto the appliance a wizard is automatically run</p> <p>Press Enter to continue</p>	
<p>Select option 1 to proceed to agree</p>	
<p>FIPS Mode can be enabled at this stage and once enabled it cannot be disabled</p> <p>FIPS cannot be enabled after setup and is not required for EAG</p> <p>Enter n to continue</p>	
<p>The next prompt is the option to change the appliance password</p> <p>This step can be skipped for now by entering n</p> <p>The passwords can be changed at the end of the installation</p>	
<p>Enter 1 to change the host name</p>	

Configuration	Screenshot	
<p>Enter the hostname of the appliance</p> <p>This is any arbitrary hostname that is used to identify this appliance</p> <p>This hostname will correspond to the management interface of EAG Enter n to continue</p>	<pre>Host Name Configuration Host name: eag.maas360swat.com 1: Change the host name x: Exit p: Previous screen n: Next screen Select option: n</pre>	
<p>Next step is to configure a management interface that is used to configure and manage EAG</p> <p>Enter 3 to configure an interface</p> <p>The reverse proxy interface is configured at a later point</p>	<pre>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</pre>	
<p>Enter 1 to configure the 1.1 Interface</p> <p>Enter 1 to enable this interface</p>	<pre>Configure an Interface Select the interface to configure: 1: 1.1 2: 1.2 3: loopback Enter index: 1</pre>	<pre>Enable this interface? 1: Yes 2: No Enter index: 1</pre>
<p>A static IP address for the management interface is specified in this example</p> <p>Enter 2 for manual configuration</p>	<pre>Select an IPv4 configuration mode: 1: Automatic 2: Manual 3: Automatic and Manual Enter index: 2_</pre>	
<p>Enter 2 to add a new IP address to the 1.1 interface</p>	<pre>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</pre>	
<p>Enter management IP address and the subnet mask</p>	<pre>Enter the IPv4 address: 10.0.1.5 Enter the IPv4 prefix or subnet mask: 255.255.255.0</pre>	

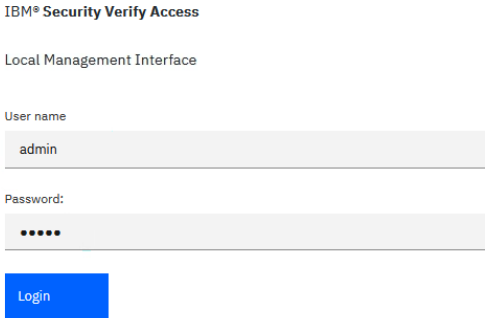
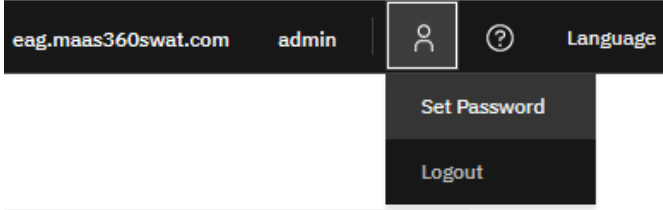
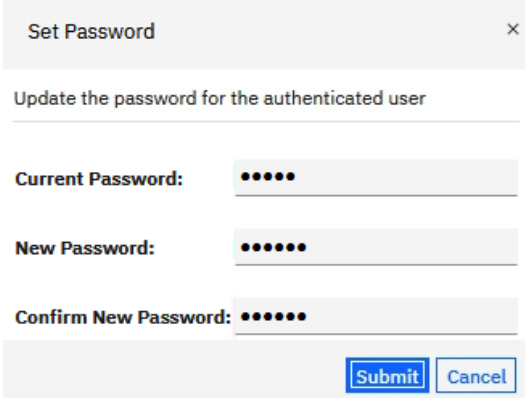
Configuration	Screenshot
<p>Enter 1 to specify this IP address as a management address</p>	<pre>Enter the IPv4 address: 10.0.1.5 Enter the IPv4 prefix or subnet mask: 255.255.255.0 Use this IP address for management? 1: Yes 2: No Enter index: 1</pre>
<p>Enter 1 to enable this IP address</p> <p>Enter 4 to finish configuring addresses</p>	<pre>Enable this IP address? 1: Yes 2: No Enter index: 1</pre> <pre>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: 4_</pre>
<p>Enter 1 to Automatic configure IPv6 address</p>	<pre>Select an IPv6 configuration mode: 1: Automatic 2: Manual 3: Automatic and Manual Enter index: 1</pre>
<p>Enter 2 to not use obtained IP address for management</p>	<pre>Configure Auto IPv6 Address Use obtained IP address for management? 1: Yes 2: No Enter index: 2</pre>
<p>Enter 6 to set the IPv4 default gateway</p>	<pre>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</pre>
<p>Enter the default gateway address</p>	<pre>Set IPv4 Default Gateway Enter gateway IP address: 10.0.1.1_</pre>

Configuration	Screenshot
<p>Enter 1 to specify that the 1.1 interface should be used to reach the Default Gateway</p>	<pre>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</pre>
<p>Networking configuration has been completed</p> <p>Enter n to proceed to the next screen</p>	<pre>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</pre>
<p>Select option 1 to set DNS server 1</p>	<pre>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</pre>
<p>Enter the IP address of the DNS server</p>	<pre>Set DNS Server 1 Enter the DNS server IP address: 10.0.1.2</pre>

Configuration	Screenshot
<p>Once the DNS configurations have been completed</p> <p>Enter n to continue to the next screen</p>	<pre> 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 </pre>
<p>Enter 3 to change time zone if required, or enter n to continue</p> <p>Check the time and date displayed and modify if necessary</p> <p>Once the date, time and time zone are set correctly, enter n to continue</p>	<pre> 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_ </pre>
<p>Check the data displayed in the Summary</p> <p>Enter 1 to accept and apply the specified configuration</p>	<pre> 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 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 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 </pre>

Configuration	Screenshot
If prompted, press enter to reboot and continue	
Depending on changes restart may not be required	

Step 5: Login to Web Management Interface

Configuration
<p>The appliance offers a browser-based graphical user interface In this example, the URL is https://eag.maas360swat.com The default credentials to log in to the local management interface are user admin password admin</p>

<p>The password for the Local Management Interface (LMI) can be configured via the UI</p>

<p>Set the new password if required</p>


Step 6: Configure Data Interface

Configuration

From the top menu, select System > Network Settings > Interfaces

Monitor ▾
Web ▾
System ▾

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	Silent Configuration
Scheduled Security Updates	Static Routes	Management Authorization	

Provide a Name to the interface (Reverse Proxy for example)

Networking Configuration

General Networking | DNS | **Interfaces** | Static Routes | Test Connection

Interfaces:

[+ New](#) | [Edit](#) | [Delete](#)

Interface	Enabled	Name	Address
<input type="checkbox"/> 1.1	<input checked="" type="checkbox"/>		10.0.1.5/255.255.255.0 [Management]
<input checked="" type="checkbox"/> 1.2	<input checked="" type="checkbox"/>		

Edit Interface

General Configuration | IPv4 Settings | IPv6 Settings

Interface:

Name:

Enabled

Select IPv4 Settings to configure the external interface

Enter the IP address and subnet mask of the data interface

Uncheck the Management Address

Check Enabled option to enable the interface

Edit Interface

General Configuration | **IPv4 Settings** | IPv6 Settings

Auto (DHCP)

Enabled

Management Address

Provides Default Route

Manual

[+ New](#) | [Edit](#) | [Delete](#)


Address	Management Address	Enabled
<input type="checkbox"/> 10.0.1.6/24	No	Yes

Override the Overlapping Subnet Validation


The option to override the overlapping subnet validation may have to be selected depending on the configuration of the network interfaces

A warning message is shown if this is the case

Configuration


 **System Error**
Address 10.0.1.6/24 overlaps a subnet on interface 1.1 This interface will not be able to be updated until all overlapping IPv4 addresses are removed.

Select the option to override the overlapping subnet validation if required

 **System Warning**
The check to ensure that overlapping subnets do not span multiple interfaces has been disabled. It is advised that this validation is not disabled as it can lead to networking issues in certain environments.

Override the Overlapping Subnet Validation

Review and deploy changes

 **Pending Changes**
There is currently one undeployed change.


[Review Pending Changes](#)

Deploy Pending Changes ×

Module	Date Modified
Networking Configuration	Mar 15, 2022, 11:27:16 AM

[Cancel](#) [Roll Back](#) [Deploy](#)

Proxy network connections will reset and connection is lost

 **Session Ended**
The policy was successfully applied but the nature of the changes required the user interface to restart.

This action does not disrupt the flow of network traffic.

The local management interface will be unavailable until the restart finishes.

[Click here to return to the local management interface](#)

Step 7: Activate Reverse Proxy

Configuration

System > Updates and Licensing > Licensing and Activation

Monitor ▾
Web ▾
System ▾

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	Silent Configuration
Scheduled Security Updates	Static Routes	Management Authorization	
Update Servers	Test Connection	Management SSL Certificate	
Update History	Hosts File	Account Management	
Licensing and Activation	Packet Tracing	Advanced Tuning Parameters	
Firmware Settings	Cluster Configuration	Snapshots	

Locate the license key file with the EAG media that has been downloaded from the MaaS360 Portal
On the Licensing and Activation page, click Select License and locate the license file to install
Select the license file and then click Open

Licensing and Activation

Activated Modules

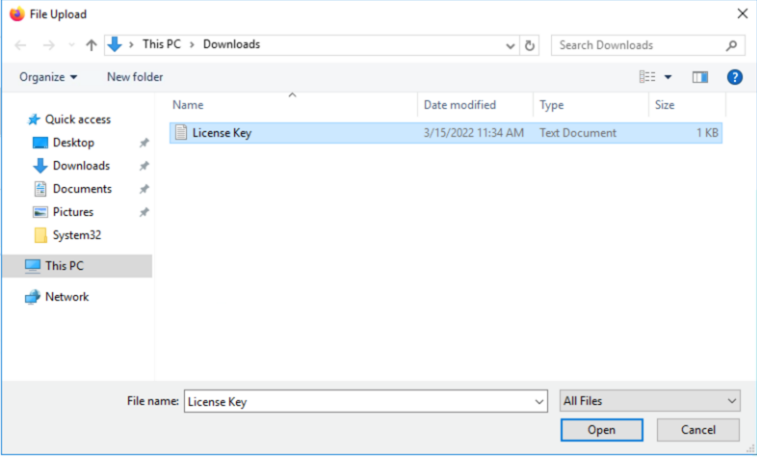
[Import](#)

Module

Support License

[Select License](#)

No licensed modules. Add a license key.



Click Save Configuration

Activated Modules

[Import](#)

The license file upload process is pending:

#	Type	File Name
1	TXT	License Key.txt

[Save Configuration](#)
[Cancel](#)

Confirm license is enabled

Configuration

Activated Modules

Import

Module

Name: IBM Security Verify Access Base Appliance
Enabled: True
Software License Agreement: [View Service Agreement](#)

Review and deploy changes

! **Pending Changes**
There is currently one undeployed change.

[Review Pending Changes](#)

Deploy Pending Changes ×

Module	Date Modified
Activation	Mar 15, 2022, 11:36:54 AM

Cancel
Roll Back
Deploy

The following message is displayed
Click on the link in the message to reconnect to the management interface

i **Session Ended**
The policy was successfully applied but the nature of the changes required the user interface to restart.

This action does not disrupt the flow of network traffic.

The local management interface will be unavailable until the restart finishes.

[Click here to return to the local management interface](#)

Reverse Proxy is now available via Web menu

Web ^
IBM Security Verify
System v

Manage

- Runtime Component
- Reverse Proxy
- Reverse Proxy
- Authorization Server

Global Settings

- URL Mapping
- Junction Mapping
- Client Certificate Mapping

Step 8: Configure Runtime Component

Configuration

Web > Manage > Runtime Component
The Runtime Component is not configured
Click Configure

Web ^
IBM Security Verify
System v

Manage
Global Settings

Runtime Component
URL Mapping

Reverse Proxy
Trustee Mapping

Authorization Server
Client Certificate Mapping

IBM Security Verify Access
Monitor v
Web v
IBM Security Verify
System v

Runtime Component

[Configure](#) |
 [Unconfigure](#) |
 [Start](#) |
 [Stop](#) |
 [Restart](#) |
 [Replicate with Cluster](#) |
 [Manage](#) v

Status: Not configured

Set Policy Server to Local
Set User Registry to LDAP Local

Runtime Environment Configure x

Main

Policy Server

LDAP

Local

Remote

Import

User Registry

LDAP Remote

LDAP Local

Previous Next Finish Cancel

Select Policy Server
Enter a new password for Administrator Password
This password is called the Security Master Password
Keep the other fields as default

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

Previous Next Finish Cancel

Select LDAP and click Finish

Runtime Environment Configure

Main Policy Server LDAP

Clean existing data

Previous Next Finish Cancel

Runtime Component status is now available

Runtime Component

Configure | Unconfigure | Start | Stop | Restart | Replicate with Cluster | Manage

Status: Available

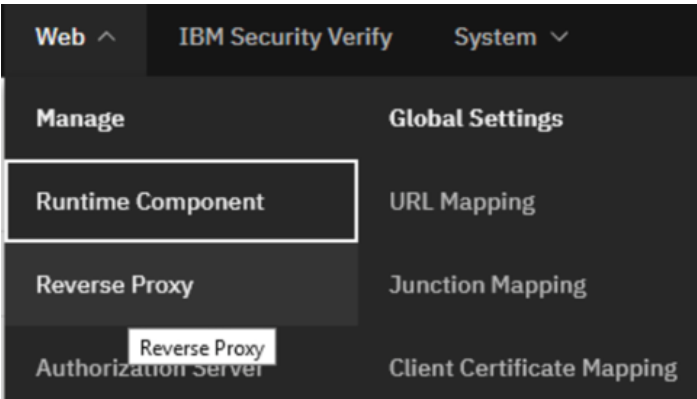
Mode: The environment is configured using a local policy server and a local user registry.

[Go to Application Log Files to view the Policy Server and User Registry log files.](#)

Step 9: Set up Reverse Proxy

Configuration

Web > Manage > Reverse Proxy
Click New



Reverse Proxy

[+ New](#) | [Edit](#) | [Delete](#) | [▶ Start All](#) | [■ Stop All](#) | [⏻ Restart All](#) | [🔄 Refresh](#) | [Manage](#) | [Troubleshooting](#)

<input type="checkbox"/> Instance Name	State	Changes are Active	Last Modified
🔍 ... No filter applied			
0 item			

10 | 25 | 50 | 100 | All

Enter the Instance name (e.g. mailproxy)
Host name is populated automatically with the hostname of the instance
Select the IP Address for the Primary Interface to the address that was configured for the data interface

New Reverse Proxy Instance

Instance IBM Security Verify Access Transport

mailproxy

Description

Host name *

eag.maas360swat.com

Listening Port *

7234

IP Address for the Primary Interface *

10.0.1.6

[Previous](#) [Next](#)

Select IBM Security Verify Access
Enter the Security Master Password that was configured during Runtime configuration step

Configuration

New Reverse Proxy Instance

Instance **IBM Security Verify Access** Transport

Administrator Name *

Administrator Password *

Domain *

[Previous](#) [Next](#)

Select Transport
Enable HTTPS Port 443

Instance IBM Security Verify Access **Transport**

Enable HTTP

HTTP Port

Enable HTTPS

HTTPS Port

[Previous](#) [Next](#) [Finish](#)

Click Finish
The reverse proxy instance is created

Reverse Proxy

[+ New](#) | [Edit](#) | [Delete](#) | [▶ Start All](#) | [■ Stop All](#) | [⏻ Restart All](#) | [🔄 Refresh](#) | [Manage](#) | [Troubleshooting](#)

Instance Name	State	Changes are Active
<input type="text" value="No filter applied"/>		
<input type="checkbox"/> mailproxy	✔ Started	✔ True

Step 10: Disable Basic Authentication

Configuration

Select Reverse Proxy instance
Click Edit

Reverse Proxy Basic Configuration - mailproxy

Server | SSL | Junction | **Authentication** | Session | Response | SSO | Logging | Interfaces

Client Connection

HTTPS

HTTPS Port *
443

HTTP

HTTP Port *
80

Threads and Connections

Persistent Connection Timeout *
5

Worker Threads *
300

Select Authentication
Set Basic Authentication Transport to None
Click Save

Reverse Proxy Basic Configuration - mailproxy

Server | SSL | Junction | **Authentication** | Session | Response | SSO | Logging | Interfaces

Basic Authentication

Transport
None

Forms Authentication

Transport
HTTPS

Review and deploy changes

! Pending Changes
There is currently one undeployed change.

[Review Pending Changes](#)

Deploy Pending Changes ×

Module	Date Modified
Authentication	Thu 11/20/2023 11:28:58 AM

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.

The following reverse proxy instances need to be restarted for updates to take effect:

- mailproxy

Reverse Proxy

+ New | Edit | Delete | Start | Stop | Restart | Refresh | Manage | Troubleshooting

Instance Name	State	Changes are Active
mailproxy	Started	False

i System Notification
Successfully restarted the proxy instance.

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

Configuration

System > Secure Settings > SSL Certificates
Select pdsrv
Click Manage > Edit SSL Certificate Database

IBM Security Verify System ^

- System Settings
- Date/Time
- Administrator Settings
- Management Authentication

Secure Settings

- SSL Certificates
- File Downloads
- SSL Certificates
- Silent Configuration

Certificate Database Name	Type	Last Modified
embedded_ldap_keys	Local	Mar 15, 2022
lmi_trust_store	Local	Mar 15, 2022, 1:30:08 PM
pdsrv	Local	Mar 18, 2022, 12:18:33 PM

Click on Signer Certificates
Select Manage > Import

Edit SSL Certificate Database - pdsrv

+ New | Edit | Delete | Refresh | Manage ^

Signer Certificates | Personal Certificates | Certificates

Label	Issuer	Subject
No filter applied		

Import the signer certificate of the mail server and any issuing CA certificates
Confirm certificate imported

Configuration

✕

Import Signer Certificate

Certificate File *

mail-server-cert.cer

[Browse](#)

Certificate Label *

Mail Server

[Import](#) [Cancel](#)

System Notification The management SSL certificate was successfully updated.

Select All option at the bottom of the screen to view all certificates
Scroll to bottom and confirm that both certificates loaded successfully
Depending on the certificate, make sure the chain is present and import any missing certificates

5 | 10 | 25 | 50 | 100 | **All**

<input type="radio"/> Mail Server	CN=MS-EXCH2016	CN=MS-EXCH2016
-----------------------------------	----------------	----------------

Review and deploy changes

! Pending Changes
There is currently one undeployed change.

[Review Pending Changes](#)

✕

Deploy Pending Changes

Module	Date Modified
mailproxy	Thu 10/26/2017 11:28:58 AM

[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.

The following reverse proxy instances need to be restarted for updates to take effect :

- mailproxy

Reverse Proxy

+ New | Edit | Delete | Start | Stop | Restart | Refresh | Manage | Troubleshooting

Instance Name	State	Changes are Active
mailproxy	Started	False

i System Notification
Successfully restarted the proxy instance.

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

Configuration

Web > Manage > Reverse Proxy
Select the reverse proxy instance
Manage > Junction Management

Reverse Proxy

[+ New](#) | [Edit](#) | [Delete](#) | [▶ Start](#) | [■ Stop](#) | [⏻ Restart](#) | [🔄 Refresh](#) | [Manage ^](#) | [Troubleshooting v](#)

<input checked="" type="checkbox"/>	Instance Name	State
Filter ... No filter applied		
<input checked="" type="checkbox"/>	mailproxy	✔ Started

Configuration

AAC and Federation Configuration

Management Root

Junction Management

Renew Management Certificate

✔ True

New > Standard Junction
Set Junction Name to /mail
Set Junction Type to SSL

Junction Management - mailproxy

[New ^](#) | [Edit](#) | [Delete](#)

Standard Junction

Virtual Junction

[Filter](#) ... No filter applied

Create a Standard Junction

Junction Servers Basic Authentication Identity SSO and LTPA General

Creation of a junction for an initial server

Junction Point Name *

Junction Type

TCP
 SSL

Select Servers and click New
Set hostname to the corporate mail server (in this example DNS is used for name resolution)
For Local Address select the IP address of data interface
Click Save

All other required values are completed automatically

Configuration

Add TCP or SSL Servers ×

<p>Hostname * ms-exch2016.maas360swat.com Lookup</p> <p>TCP or SSL Port * 443</p> <p>Virtual Host <input type="text"/></p> <p>Virtual Host Port <input type="text"/></p> <p>Local Address 10.0.1.6</p>	<p>Query Contents <input type="text"/></p> <p>UUID of the Server <input type="text"/></p> <p>Distinguished Name(DN) <input type="text"/></p> <p><input type="checkbox"/> Windows File System Support</p> <p><input type="checkbox"/> Treat URL as case insensitive</p>
--	---

Save Cancel

Confirm server added

+ New | ✎ Edit | 🗑 Delete

Hostname

🔍 ... No filter applied

- ms-exch2016.maas360swat.com

Select Identity
Change HTTP Basic Authentication Header to Ignore

Junction Servers Basic Authentication Identity

Supply identity information in HTTP headers

HTTP Basic Authentication Header

Ignore ^

Filter

Ignore

Click Save
The junction is created

Configuration

Junction Management - mailproxy

System Notification Created junction at /mail ×

New ▾ | [Edit](#) | [Delete](#)

Junction Point Name	Virtual or Standard
▽ ... No filter applied	
○ /mail	Standard Junction

Click Edit and select Servers
Confirm junction is running

+ New | [Edit](#) | [Delete](#)

Hostname	Server State	Server Operational State
▽ ... No filter applied		
○ 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 ^

System Settings

Date/Time

Administrator Settings

Management Authentication

Secure Settings

SSL Certificates

File Downloads

SSL Certificates

Silent Configuration

SSL Certificates

+ New | [Delete](#) | [Refresh](#) | Replicate with Cluster | Manage ^

▽ No filter applied

Certificate Database Name	Type	Last Mo
embedded_ldap_keys	Local	Mar 15, 2
lmi_trust_store	Local	Mar 15, 2022, 1:30:08 PM
pdsrv	Local	Mar 18, 2022, 12:18:33 PM

Edit SSL Certificate Database
Edit Properties
Details
Describe
Rename
Import
Export

Click on Personal Certificates
Select Manage > Import

Configuration

Edit SSL Certificate Database - pdsrv

+ New | Edit | Delete | Refresh | **Manage** ^

Signer Certificates | **Personal Certificates** | Certificates

Label	Default	Issuer
No filter applied		

View
Receive
Import
Export
Extract
Load

Import the SSL certificate for the data interface
Enter the password that is used to protect the certificate
Click Import

Use a friendly Name field when creating an SSL certificate as this label is used display the certificate for selection from the drop-down menu options

Import Personal Certificate ×

Type *

PKCS12

Certificate File *

mail-server.pfx

Password

••••••••

Confirm certificate was imported
Confirm certificate and associated signer certificates are present in the SSL store

System Notification The management SSL certificate was successfully updated.

○	{B160BE23-E826-4A2E-BEC0-6C545B3546F4}	false	CN=R3,O=Let's Encrypt,C=US	CN=*.maas360swat.com
○	R3-inter		CN=ISRG Root X1,O=Internet Security Research Group,C=US	CN=R3,O=Let's Encrypt,C=US
○	ISGR-root		CN=ISRG Root X1,O=Internet Security Research Group,C=US	CN=ISRG Root X1,O=Internet Security Research Group,C=US

Configuration

Review and deploy changes

! Pending Changes
There is currently one undeployed change.

[Review Pending Changes](#)

Deploy Pending Changes ×

Module	Date Modified

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.

The following reverse proxy instances need to be restarted for updates to take effect :

– mailproxy

Reverse Proxy

+ New |
 ✎ Edit |
 🗑 Delete |
 ▶ Start |
 ■ Stop |
 🔄 Restart |
 🔄 Refresh |
 Manage ▾ |
 Troubleshooting ▾

Instance Name	State	Changes are Active
▽ ... No filter applied		
<input checked="" type="checkbox"/> mailproxy	Started	False

i System Notification
Successfully restarted the proxy instance.

Edit the reverse proxy instance
Select SSL
Select the newly imported certificate
Click Save

Reverse Proxy Basic Configuration - mailproxy

Server |
 SSL |
 Junction |
 Authentication

SSL

SSL Certificate Key File

pdsrv Edit

Network HSM Key File

 Edit

SSL Server Certificate

{A2E-BEC0-6C545B3546F4} ^

WebSEAL-Test-Only

{B160BE23-E826-4A2E-BEC0-6C545B3546F4}

! Pending Changes
There is currently one undeployed change.

[Review Pending Changes](#)

Deploy Pending Changes ×

Module	Date Modified

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.

The following reverse proxy instances need to be restarted for updates to take effect :

– mailproxy

Reverse Proxy

+ New |
 ✎ Edit |
 🗑 Delete |
 ▶ Start |
 ■ Stop |
 🔄 Restart |
 🔄 Refresh |
 Manage ▾ |
 Troubleshooting ▾

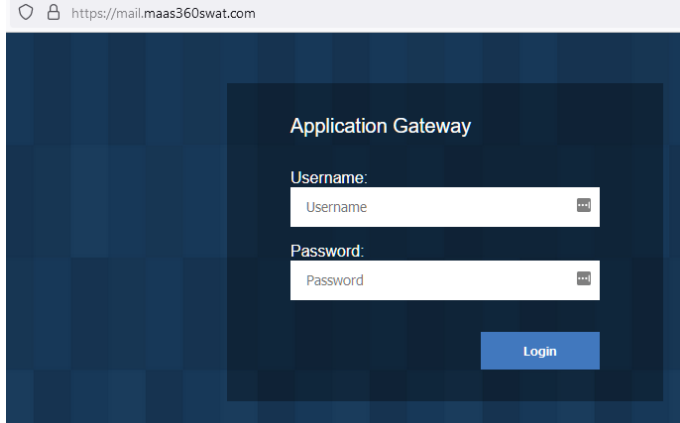
Instance Name	State	Changes are Active
▽ ... No filter applied		
<input checked="" type="checkbox"/> mailproxy	Started	False

i System Notification
Successfully restarted the proxy instance.

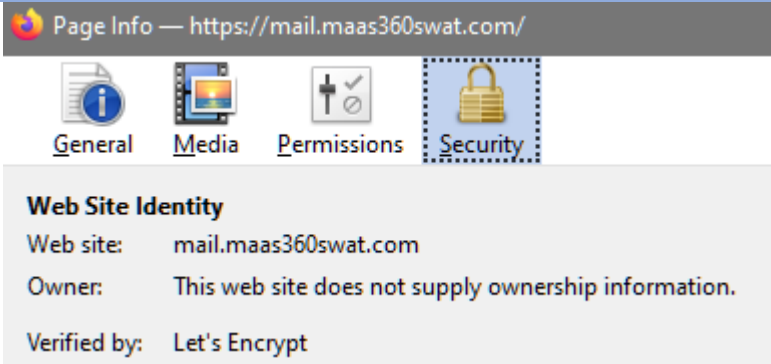
Step 14: Validating Setup

Configuration

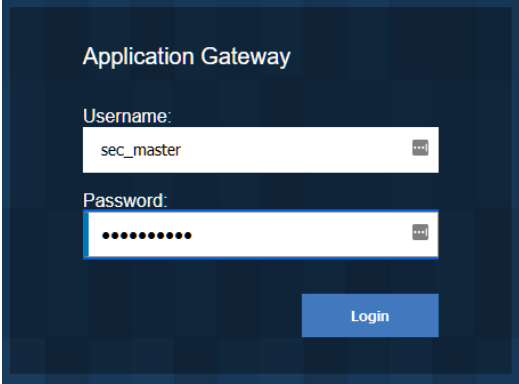
Browse to public interface
(e.g. <https://mail.maas360swat.com>)




The SSL certificate being used can be verified



Enter the Security Master credentials

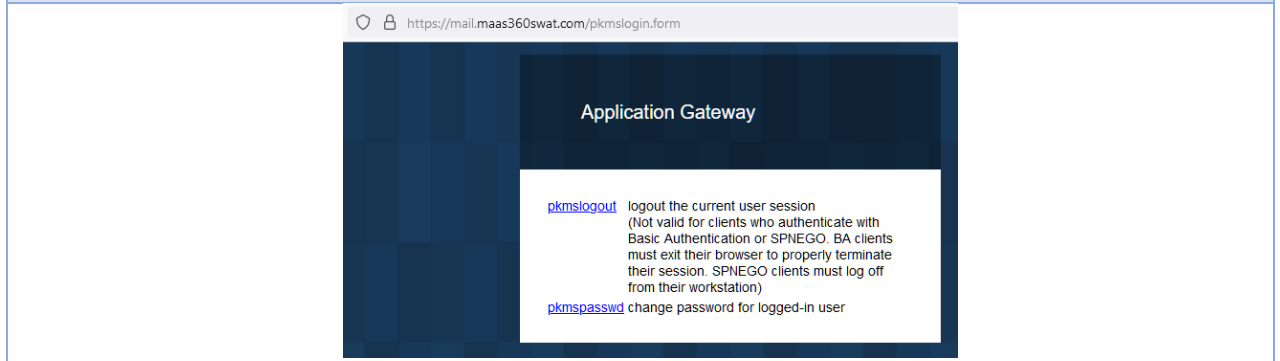


A successful logon will display the splash screen



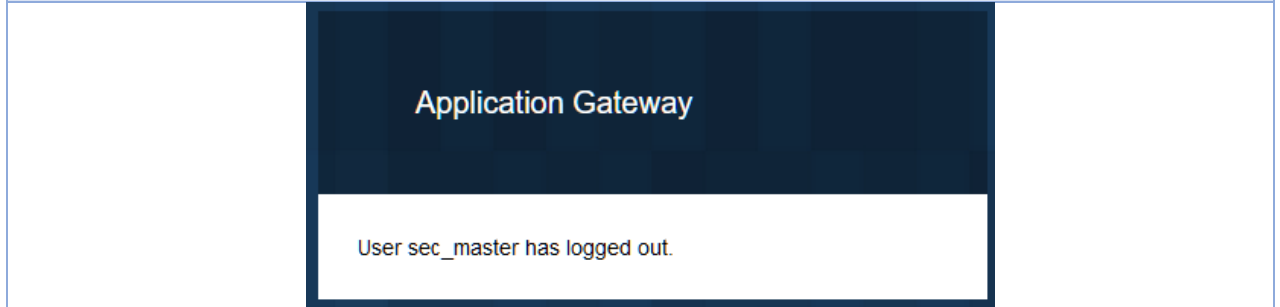
Configuration

**Logout using the pkmslogin form
(e.g. <https://mail.maas360swat.com/pkmslogin.form>)**



The screenshot shows a web browser window with the URL <https://mail.maas360swat.com/pkmslogin.form>. The page content includes the heading "Application Gateway" and two links: [pkmslogout](#) and [pkmspasswd](#). The [pkmslogout](#) link is accompanied by a detailed explanation: "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)".

Click logout and confirm user logged out



The screenshot shows the "Application Gateway" page with a white message box at the bottom stating "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:

Configuration

Web > Manage > Policy Administration
Sign on with Security Master credentials

IBM Security Verify Access
Monitor ▾
Web ▾
IBM Security Verify
System ▾

Policy Administration

Task List	Security Verify Access Sign On
	<p>Secure Domain <input type="text"/></p> <p>+User Id <input type="text" value="sec_master"/></p> <p>+Password <input type="password" value="••••••••"/></p> <p style="text-align: center;"><input type="button" value="Sign On"/></p>

ACL > Create ACL
ACL Name > mailproxy-unauthenticated
Description > allow unauthenticated access to mail proxy resource
Click Create
Confirm ACL created
Click Done

Policy Administration
Create ACL

Task List	Create ACL	Create ACL
<ul style="list-style-type: none"> ▶ User ▶ Group ▶ Object Space ▼ ACL <ul style="list-style-type: none"> Search ACLs Create ACL Import ACL Export All ACLs List Action Groups 	<p>+ACL Name <input type="text" value="mailproxy-unauthenticated"/></p> <p>Description <input type="text" value="allow unauthenticated access to mail proxy resou"/></p> <p style="text-align: center;"><input type="button" value="Create"/> <input type="button" value="Cancel"/></p>	<div style="border: 1px solid #0056b3; padding: 5px;"> <p style="font-size: 1.2em; font-weight: bold; color: #0056b3;">i</p> <p>The ACL was created successfully</p> <p style="color: #0056b3; text-decoration: underline;">mailproxy-unauthenticated</p> <p style="text-align: center;"><input type="button" value="Create Another"/></p> <p style="text-align: center;"><input type="button" value="Done"/></p> </div>

ACL > Search ACL
Click on the Search button
Confirm new ACL is listed

Configuration

Policy Administration

Task List

- ▶ User
- ▶ Group
- ▶ Object Space
- ▼ ACL
 - Search ACLs
 - Create ACL
 - Import ACL
 - Export All ACLs
 - List Action Groups
 - Create Action Group
- ▶ POP
- ▶ AuthzRule
- ▶ GSO Resource
- ▶ Secure Domain

Search ACLs

+ACL Name +Maximum Results

11 ACLs matched the search criteria

Create...	Delete	Export	Options	Filters	Select	ACL Name
<input type="checkbox"/>					<input type="checkbox"/>	default-config
<input type="checkbox"/>					<input type="checkbox"/>	default-domain
<input type="checkbox"/>					<input type="checkbox"/>	default-gso
<input type="checkbox"/>					<input type="checkbox"/>	default-management
<input type="checkbox"/>					<input type="checkbox"/>	default-management-proxy
<input type="checkbox"/>					<input type="checkbox"/>	default-policy
<input type="checkbox"/>					<input type="checkbox"/>	default-replica
<input type="checkbox"/>					<input type="checkbox"/>	default-root
<input type="checkbox"/>					<input type="checkbox"/>	default-webseal
<input type="checkbox"/>					<input type="checkbox"/>	favicon
<input type="checkbox"/>					<input type="checkbox"/>	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

Description

ACL Entries

Create...	Delete	Select	Entry Name	Entry Type	Permissions
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	sec_master	User	Tc-mdbsvaB-R-!---
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		Any-other	T-----rx---
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		Unauthenticated	T-----rx---

Object Space > Browse Object Space

Policy Administration

Task List

- ▶ User
- ▶ Group
- ▼ Object Space
 - Browse Object Space
 - Copy/Paste Object Space

Browse Object Space

Path	ACL	POP	AuthzRule
<input type="button" value="+"/> /	default-root		

Configuration

Expand Object Space

Browse Object Space

Refresh Prune

Path	ACL	POP	AuthzRule
/	default-root		
Management	default-management		
WebSEAL	default-webseal		
eag.maas360swat.com-mailproxy			
favicon.ico	favicon	favicon	
icons			
index.html			
mail			
pics			

Select mail junction
Click Attach (ACL)
Select ACL that was previously created
Click Apply
Click Apply again on the main screen

Protected Object Properties

General Extended Attributes

Object Name
 [/WebSEAL/eag.maas360swat.com-mailproxy/mail]

Description
 Object from host eag.maas360swat.com.

Can Policy be attached to this object

ACL Attached
 mailproxy-unauthenticated Detach

POP Attached
 Attach...

AuthzRule Attached
 Attach...

[Create Child Object...](#)

Apply Delete Export Cancel

Browse Object Space and hit the Refresh button to refresh the ACL associations to junctions
Confirm that the ACL is associated to the junction
Sign Off from Policy Administration

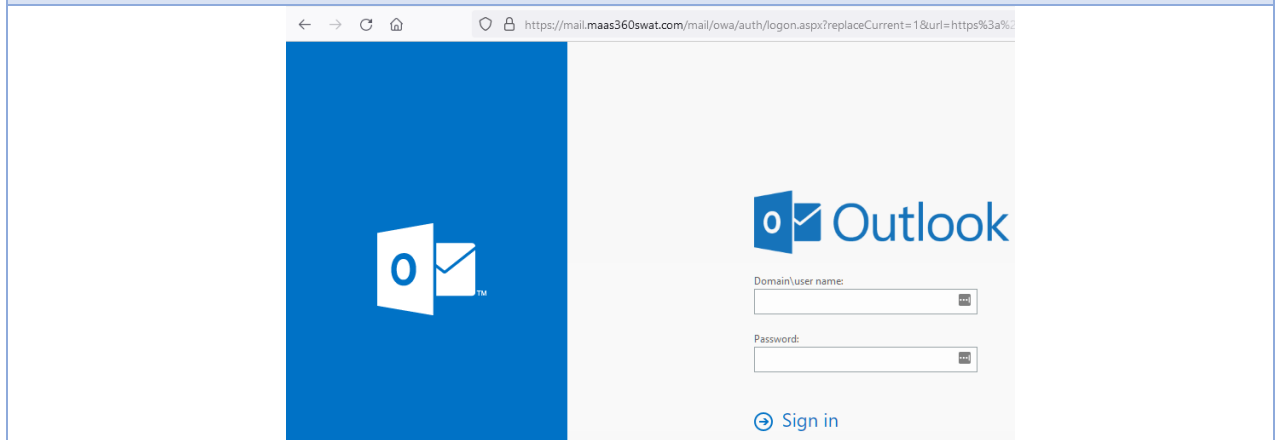
Refresh Prune

Path	ACL	POP	AuthzRule
/	default-root		
Management	default-management		
WebSEAL	default-webseal		
eag.maas360swat.com-mailproxy			
favicon.ico	favicon	favicon	
icons			
index.html			
mail	mailproxy-unauthenticated		
pics			

Configuration

If OWA is enabled, then this is accessible without requiring entering credentials because the unauthenticated ACL was added to the junction

Browse to the OWA URL via EAG URL



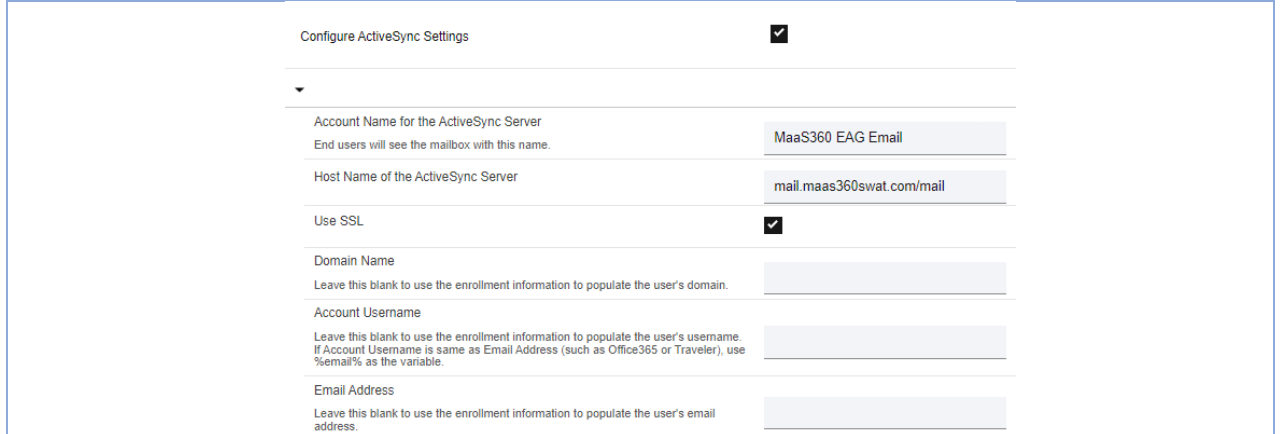
MaaS360 Configuration:

Configuration

To configure native mail use the MaaS360 MDM policies

Browse to Security > Policies on the MaaS360 portal and edit the MDM Policy
Browse to Device Settings > ActiveSync
Configure the host name to point to the data interface of EAG (e.g. mail.maas360swat.com/mail)
Enable SSL
The username and email fields can be configured with wildcard variables like %username%, %email% etc. depending on the username format of email environment

Save and publish the policy



Configuration

To configure MaaS360 Secure Mail use the MaaS360 WorkPlace Persona policies

Browse to Security > Policies on the MaaS360 portal and edit the WorkPlace Persona Policy

Browse to Email > Configuration

Configure the Mail Server to point to the data interface of EAG (e.g. mail.maas360swat.com/mail)

Enable SSL

The username and email fields can be configured with wildcard variables like %username%, %email% etc. depending on the username format of email environment

Save and publish the policy

▼ Configure Secure Mail

Mail Server

Exchange

Select the appropriate email server to ensure that the devices get approved automatically. Auto Approval supported for Exchange, Office 365, IBM Traveler and IBM Connections Cloud.

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 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.

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 Username is same as Email Address (such as Office365 or IBM Traveler) use %email% as the variable.

Once the policy has been pushed to the device the email client will prompt for user credentials when the connection to the email server (via the proxy) 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:

Configuration

Complete all the steps for EAG configuration in Scenario #1

Web > Manage > Reverse Proxy
Select reverse proxy instance and click Manage > Configuration > Edit Configuration File

Search for text: [azn-decision-info]
Copy this text: useragent = header:user-agent

Click Save

Advanced Configuration File Editor - mailproxy

```
# mobileNumber = mobile
#
# [TAM_CRED_ATTRS_SVC:organisationalPerson]
# emailAddress = mail
# mobileNumber = mobile
#
[azn-decision-info]
useragent = header:user-agent
#
# This stanza is used to define any extra information which should
# be made available to the authorization framework when making
# authorization decisions. This extra information can be obtained
# from various elements of the HTTP request, namely:
#   - HTTP method
#   - HTTP scheme
```

Review and deploy changes

⚠ Pending Changes
 There is currently one undeployed change.

[Review Pending Changes](#)

Deploy Pending Changes

Module	Date Modified
...	...

Restart reverse proxy instance if prompted
Select the reverse proxy instance and click Restart

Configuration

System Warning
Successfully deployed all pending changes.

The following reverse proxy instances need to be restarted for updates to take effect:

- mailproxy

Reverse Proxy

+ New | Edit | Delete | Start | Stop | Restart | Refresh | Manage | Troubleshooting

Instance Name	State	Changes are Active
mailproxy	Started	False

System Notification
Successfully restarted the proxy instance.

Web > Manage > Policy Administration
Sign on with Security Master credentials

IBM Security Verify Access
Monitor
Web
IBM Security Verify
System

Policy Administration

Task List

Security Verify Access Sign On

Secure Domain

* User Id

* Password

AuthzRule > Create AuzthRules

Name: MaaS360-Mail-Only
Description: Only Allow MaaS360 Mail Client
Text :
`<xsl:if test='contains(/XMLADI/useragent, "MaaS360")'>`
!TRUE!
`</xsl:if>`
Fail Reason: Only MaaS360 Mail Client Allowed

Policy Administration

Task List

- ▶ User
- ▶ Group
- ▶ Object Space
- ▶ ACL
- ▶ POP
- ▶ AuthzRule
 - List AuthzRules
 - Create AuthzRule
 - Import AuthzRule
 - Export All AuthzRules
- ▶ GSO Resource
- ▶ Secure Domain

Create AuthzRule

* AuthzRule Name

Description


* AuthzRule Text

`<xsl:if test='contains(/XMLADI/useragent, "MaaS360")'>`
!TRUE!
`</xsl:if>`

Fail Reason

Click Create
Click Done

Configuration

 The AuthzRule was created successfully

[MaaS360-Mail-Only](#)

List of all AuthzRules

Select	AuthzRule Name
<input type="checkbox"/>	MaaS360-Mail-Only

Page 1 of 1 Total: 1

Browse Object Space and locate the mail junction

Policy Administration

Task List	Browse Object Space																																								
<ul style="list-style-type: none"> ▶ User ▶ Group ▼ Object Space <ul style="list-style-type: none"> Browse Object Space Copy/Paste Object Space Create Object Import Object Create Object Space ▶ ACL ▶ POP ▶ AuthzRule ▶ GSO Resource ▶ Secure Domain 	<p><input type="button" value="Refresh"/> <input type="button" value="Prune"/></p> <table border="1"> <thead> <tr> <th>Path</th> <th>ACL</th> <th>POP</th> <th>AuthzRule</th> </tr> </thead> <tbody> <tr> <td>/</td> <td>default-root</td> <td></td> <td></td> </tr> <tr> <td> Management</td> <td>default-management</td> <td></td> <td></td> </tr> <tr> <td> WebSEAL</td> <td>default-webseal</td> <td></td> <td></td> </tr> <tr> <td> eag.maas360swat.com-mailproxy</td> <td></td> <td></td> <td></td> </tr> <tr> <td> favicon.ico</td> <td>favicon</td> <td>favicon</td> <td></td> </tr> <tr> <td> icons</td> <td></td> <td></td> <td></td> </tr> <tr> <td> index.html</td> <td></td> <td></td> <td></td> </tr> <tr> <td> mail</td> <td>mailproxy-unauthenticated</td> <td></td> <td></td> </tr> <tr> <td> pics</td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	Path	ACL	POP	AuthzRule	/	default-root			Management	default-management			WebSEAL	default-webseal			eag.maas360swat.com-mailproxy				favicon.ico	favicon	favicon		icons				index.html				mail	mailproxy-unauthenticated			pics			
Path	ACL	POP	AuthzRule																																						
/	default-root																																								
Management	default-management																																								
WebSEAL	default-webseal																																								
eag.maas360swat.com-mailproxy																																									
favicon.ico	favicon	favicon																																							
icons																																									
index.html																																									
mail	mailproxy-unauthenticated																																								
pics																																									

Click on the entry for the mail junction
Attach the new AuthzRule
Click Apply

General	Extended Attributes
<p>Object Name <input type="text" value="/WebSEAL/eag.maas360swat.com-mailproxy/mai"/></p> <p>Description <input type="text" value="Object from host eag.maas360swat.com."/></p> <p><input checked="" type="checkbox"/> Can Policy be attached to this object</p> <p>ACL Attached <input type="text" value="mailproxy-unauthenticated"/> <input type="button" value="Detach"/></p> <p>POP Attached <input type="text" value=""/> <input type="button" value="Attach..."/></p> <p>AuthzRule Attached <input type="text" value="MaaS360-Mail-Only"/> <input type="button" value="Detach"/></p> <p>Create Child Object...</p> <p><input type="button" value="Apply"/> <input type="button" value="Delete"/> <input type="button" value="Export"/> <input type="button" value="Cancel"/></p>	

Refresh the Object Space and confirm AuthzRule is now visible

Configuration

Browse Object Space

Refresh
Prune

Path	ACL	POP	AuthzRule
/	default-root		
Management	default-management		
WebSEAL	default-webseal		
eag.maas360swat.com-mailproxy			
favicon.ico	favicon	favicon	
icons			
index.html			
mail	mailproxy-unauthenticated		MaaS360-Mail-Only
pics			

Web > Manage > Runtime Component
Restart the Runtime Component

Runtime Component

System Notification
 Successfully restarted the runtime component.

Configure
Unconfigure
Start
Stop
Restart
Replicate with Cluster
Manage

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.](#)

Only MaaS360 Secure Mail client is allowed to connect via EAG Proxy

MaaS360 Configuration:

Configuration

To configure native mail use the MaaS360 MDM policies

Browse to Security > Policies on the MaaS360 portal and edit the MDM Policy

Browse to Device Settings > ActiveSync

Configure the host name to point to the data interface of EAG (e.g. mail.maas360swat.com/mail)

Enable SSL

The username and email fields can be configured with wildcard variables like %username%, %email% etc. depending on the username format of email environment

Save and publish the policy

Configure ActiveSync Settings

Account Name for the ActiveSync Server
End users will see the mailbox with this name.

Host Name of the ActiveSync Server

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

Web > Manage > Runtime Component
Manage > Federate Directories

Runtime Component

Configure |
 Unconfigure |
 Start |
 Stop |
 Restart |
 Replicate with Cluster |
 Manage ^

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.](#)

Federated Directories

+ New |
 Edit |
 Delete |
 SSL Settings |
 Refresh

Name	Suffix

Configuration

Enter details for the corporate directory server

Example

Connect Name: MaaS360 SWAT LDAP

Hostname: maas360swat.com

Port: 389

Suffix: ou=maas360 users, dc=maas360swat, dc=com

Bind DN: cn=ldapbinduser, cn=managed service accounts, dc=maas360swat, dc=com

Click Save

Name
MaaS360 SWAT LDAP

Hostname *
maas360swat.com

Port *
389

Suffix *
ou=maas360 users
,dc=maas360swat,dc=com

Bind DN
cn=ldapbinduser,cn=managed service accounts,dc=maas360swat,dc=com

Bind Password
••••••••

Enable SSL

Client Certificate
▼

Verify that the specific settings are correct

Click Close

Federated Directories x

System Notification Successfully updated the directory x

[+ New](#)
[Edit](#)
[Delete](#)
[SSL Settings](#)
[Refresh](#)
[Help](#) ?

Name	Suffix	Server	SSL
No filter applied			
<input checked="" type="radio"/> MaaS360 SWAT LDAP	ou=maas360 users ,dc=maas360swat,dc=com	maas360swat.com:389 Bind DN: CN=LDAPBindUser,CN=Managed Service Accounts,DC=maas360swat,DC=com	Disabled
1 - 1 of 1 item 10 25 50 100 All			

Configuration

Review and deploy changes

! Pending Changes
There is currently one undeployed change.

[Review Pending Changes](#)

Deploy Pending Changes ×

Module	Date Modified

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.

The following reverse proxy instances need to be restarted for updates to take effect:

- mailproxy

Reverse Proxy

+ New
✎ Edit
🗑 Delete
▶ Start
■ Stop
🔄 Restart
🔄 Refresh
⌵ Manage
⌵ Troubleshooting

<input checked="" type="checkbox"/> Instance Name	State	Changes are Active
⌵ ... No filter applied		
<input checked="" type="checkbox"/> mailproxy	Started	False

i System Notification
Successfully restarted the proxy instance.

Web > Manage > Runtime Component
Manage > Configuration Files > ldap.conf

Manage ^

- Configuration Files ▶ pd.conf
- Embedded LDAP ▶ ivmgrd.conf
- Server Cleanup ldap.conf
- Federated Directories ▶ Tracing Configuration File

Search for basic-user-support and set value to yes

```
# Basic user support enablement. Basic user support allows the use of LDAP
# users without the need to import them into IBM Security Verify Access.
basic-user-support = yes
```

Search for basic-user-principal-attribute = uid

In this example, the corporate directory is Microsoft Active Directory, and the username attribute is mapped to userPrincipalName

Copy this text and paste it at the bottom of the stanza under the suffix entry

Change this value from uid to userPrincipalName

```
[server:MaaS360 SWAT LDAP]
host = maas360swat.com
port = 389
bind-dn = CN=LDAPBindUser,CN=Managed Service Accounts,DC=maas360swat,DC=com
ssl-enabled = no
suffix = ou=maas360 users ,dc=maas360swat,dc=com
basic-user-principal-attribute = userPrincipalName
```

Search for basic-user-no-duplicates attribute and set value to no

Configuration

```
# If Basic user support is enabled, this option will control whether users with
# duplicate names are detected across suffixes. If a duplicate name is detected,
# then the operation on the user will return an error. If this option is
# disabled, the server will not complete any cross-suffix checks to ensure that
# there are no duplicates. Disabling this option allows for significant
# performance gains as the search across each suffix will stop immediately once
# the first match user name is located. To determine whether disabling this
# option is appropriate you must determine whether user names can be guaranteed
# to be unique, or whether security requirements allows for duplicates. If
# disabled then the basic-user-suffix-optimizer enablement must also be
# considered if duplicate user names can be present.
basic-user-no-duplicates = no
```

Save Changes

Review and deploy changes

! Pending Changes
There is currently one undeployed change.

[Review Pending Changes](#)

Deploy Pending Changes X

Module	Date Modified

Cancel
Roll Back
Deploy

Restart reverse proxy instance if prompted
Select the reverse proxy instance and click Restart

System Warning X

Successfully deployed all pending changes.

The following reverse proxy instances need to be restarted for updates to take effect:

- mailproxy

Instance Name	State	Changes are Active
mailproxy	Started	False

i System Notification X

Successfully restarted the proxy instance.

Web > Manage > Policy Administration
Sign on with Security Master credentials

IBM Security Verify Access
Monitor
Web
IBM Security Verify
System

Policy Administration

Task List	Security Verify Access Sign On
<ul style="list-style-type: none"> User Search Users Create User Import User Show Global User Policy Change My Password Group 	<p>Secure Domain</p> <input style="width: 100%;" type="text"/> <p>* User Id</p> <input style="width: 100%; background-color: #fff9c4;" type="text" value="sec_master"/> <p>* Password</p> <input style="width: 100%; background-color: #fff9c4;" type="password" value="*****"/> <p style="text-align: center;">Sign On</p>

User > Search Users > Search
All directory users should show up in the list

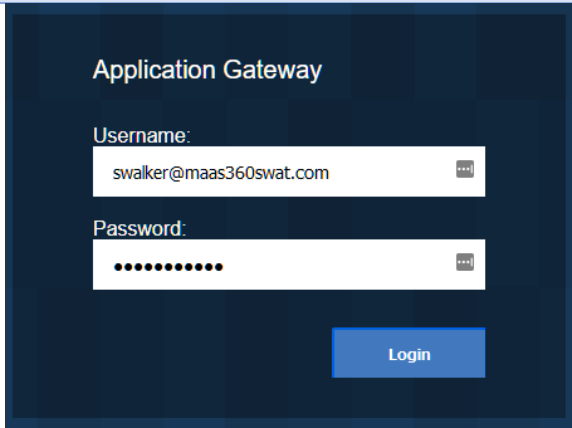
Policy Administration

Task List	User Search
<ul style="list-style-type: none"> User Search Users Create User Import User Show Global User Policy Change My Password Group 	<p>* User Id * Maximum Results</p> <p><input style="width: 100%; background-color: #fff9c4;" type="text" value="*"/> <input style="width: 100%; background-color: #fff9c4;" type="text" value="100"/> Search</p> <p>75 users matched the search criteria</p> <p style="text-align: center;"> Create... Delete Options Filters </p>

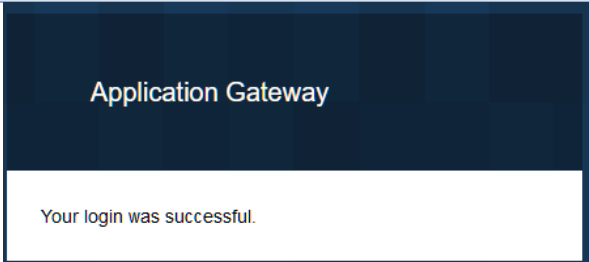
Configuration

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

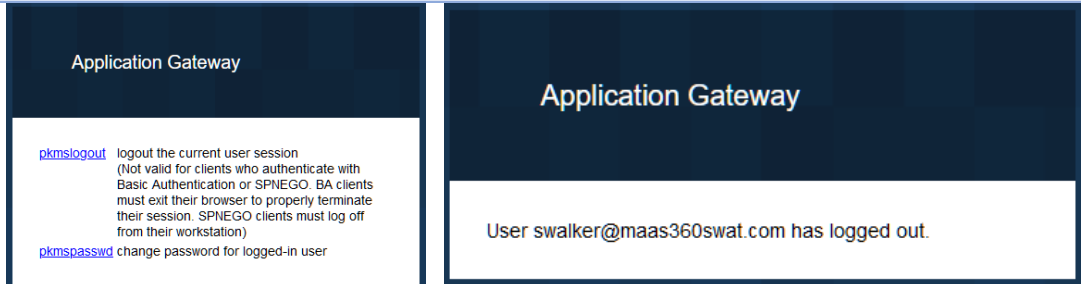


Enter the UPN as a username to validate configuration
Enter the password and click Login
Confirm login successful



Logout using the pkmslogin form
(e.g. <https://mail.maas360swat.com/pkmslogin.form>)

Click logout and confirm user logged out



Web > Manage > Policy Administration
Sign on with Security Master credentials

Configuration

IBM Security Verify Access | Monitor ▾ | Web ▾ | IBM Security Verify | System ▾

Policy Administration

Task List

Security Verify Access Sign On

Secure Domain

+User Id

+Password


Browse Object Space and locate the mail junction

Browse Object Space

Path	ACL	POP	AuthzRule
/	default-root		
Management	default-management		
WebSEAL	default-webseal		
eag.maas360swat.com-mailproxy			
favicon.ico	favicon	favicon	
icons			
index.html			
mail	mailproxy-unauthenticated		MaaS360-Mail-Only
pics			

Select mail and detach ACL
AuthzRule is optional depending on use case

Detach ACL



Detach the ACL from the Object?

Refresh Object Space and confirm ACL removed

Path	ACL	POP	AuthzRule
/	default-root		
Management	default-management		
WebSEAL	default-webseal		
eag.maas360swat.com-mailproxy			
favicon.ico	favicon	favicon	
icons			
index.html			
mail			MaaS360-Mail-Only
pics			

Configuration

Web > Manage > Reverse Proxy
Select instance and click Edit

Reverse Proxy

+ New | [Edit](#) | Delete | Start | Stop

<input checked="" type="checkbox"/> Instance Name
<div style="display: flex; align-items: center; margin-bottom: 5px;"> 🔍 ... No filter applied </div> <div style="display: flex; align-items: center;"> <input checked="" type="checkbox"/> mailproxy </div>

Authentication > Basic Authentication > Transport > HTTPS
Click Save

Server
SSL
Junction
Authentication
Session
Response
SSO
Logging
Interfaces

Basic Authentication

Transport

HTTPS ▼

Forms Authentication

Transport

HTTPS ▼

Review and deploy changes

! Pending Changes
 There is currently one undeployed change.

[Review Pending Changes](#)

Deploy Pending Changes ✕

Module	Date Modified
Authentication	Thu Jul 20 2018 11:28:58 AM

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.

The following reverse proxy instances need to be restarted for updates to take effect:

- mailproxy

Reverse Proxy

+ New | [Edit](#) | Delete | Start | Stop | Restart | Refresh | Manage | Troubleshooting

<input checked="" type="checkbox"/> Instance Name	State	Changes are Active
<div style="display: flex; align-items: center; margin-bottom: 5px;"> 🔍 ... No filter applied </div> <div style="display: flex; align-items: center;"> <input checked="" type="checkbox"/> mailproxy </div>	<div style="display: flex; align-items: center;"> Started </div>	<div style="display: flex; align-items: center;"> False </div>

i System Notification
 Successfully restarted the 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**

Configuration

System > Secure Settings > SSL Certificates
Select pdsrv
Click Manage > Edit SSL Certificate Database

Click on Signer Certificates
Select Manage > Import

Import the signer certificate of the LDAP server (*ldap-certificate.cer*) and any relevant issuing CA signer certificate(s)
Click Import and confirm certificate store updated

System Notification The management SSL certificate was successfully updated.

Select All option at the bottom of the screen to view all certificates
Scroll to bottom and confirm that both certificates loaded successfully
Depending on the certificate, make sure the chain is present and import any missing certificates

<input type="radio"/>	LDAP	CN=maas360swat-MS-DC01-CA,DC=maas360swat,DC=com	CN=maas360swat-MS-DC01-CA,DC=maas360swat,DC=com
-----------------------	------	---	---

Review and deploy changes

Configuration

! Pending Changes
There is currently one undeployed change.

[Review Pending Changes](#)

Deploy Pending Changes x

Module	Date Modified

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.

The following reverse proxy instances need to be restarted for updates to take effect :

- mailproxy

Reverse Proxy

+ New
Edit
Delete
▶ Start
■ Stop
⏻ Restart
↻ Refresh
Manage
Troubleshooting

Instance Name	State	Changes are Active
▽ ... No filter applied		
<input checked="" type="checkbox"/> mailproxy	Started	False

i System Notification
Successfully restarted the proxy instance.

Web > Manage > Runtime Component
Manage > Federated Directories
SSL Settings > set keyfile > pdsrv
Click Save

SSL Settings x

These settings are only valid if the primary LDAP directory is not configured to use SSL

Keyfile *

pdsrv

Save
Cancel

Select the federated directory > Edit
Change Port to 636
Enable SSL
Enter bind password > Save

Port *

636

Enable SSL

Click Close
Review and deploy changes

! Pending Changes
There is currently one undeployed change.

[Review Pending Changes](#)

Deploy Pending Changes x

Module	Date Modified

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.

The following reverse proxy instances need to be restarted for updates to take effect :

- mailproxy

Reverse Proxy

+ New
Edit
Delete
▶ Start
■ Stop
⏻ Restart
↻ Refresh
Manage
Troubleshooting

Instance Name	State	Changes are Active
▽ ... No filter applied		
<input checked="" type="checkbox"/> mailproxy	Started	False

i System Notification
Successfully restarted the proxy instance.

Page 53 of 76

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



Enter the UPN as a username to validate configuration
Enter the password and click Login
Confirm login successful (splash screen displayed)



Logout using the pkmslogin form
(e.g. <https://mail.maas360swat.com/pkmslogin.form>)

Click logout and confirm user 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.

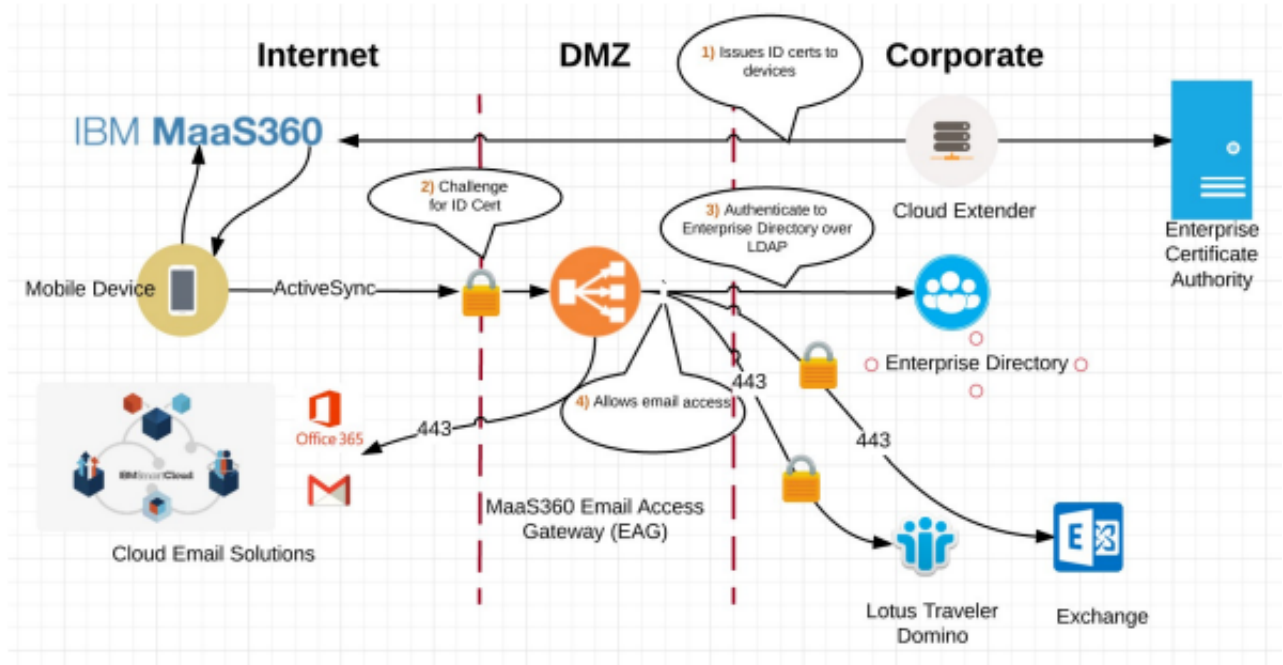
Mail servers will use the user corporate credentials to perform authentication.

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

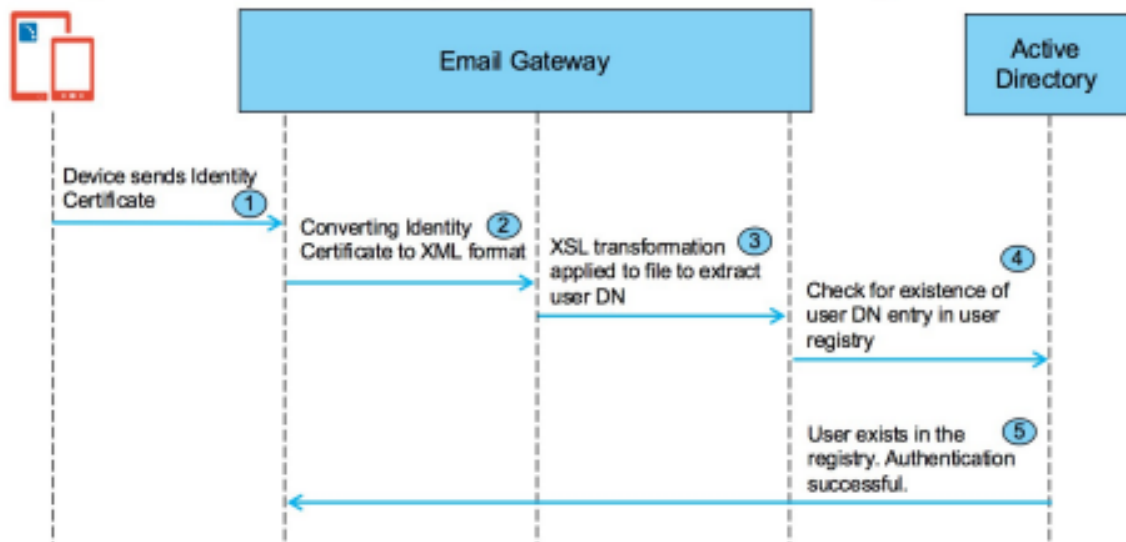


To successfully identify users via certificates, EAG needs to be configured to communicate with the user registry (LDAP in this case).

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.

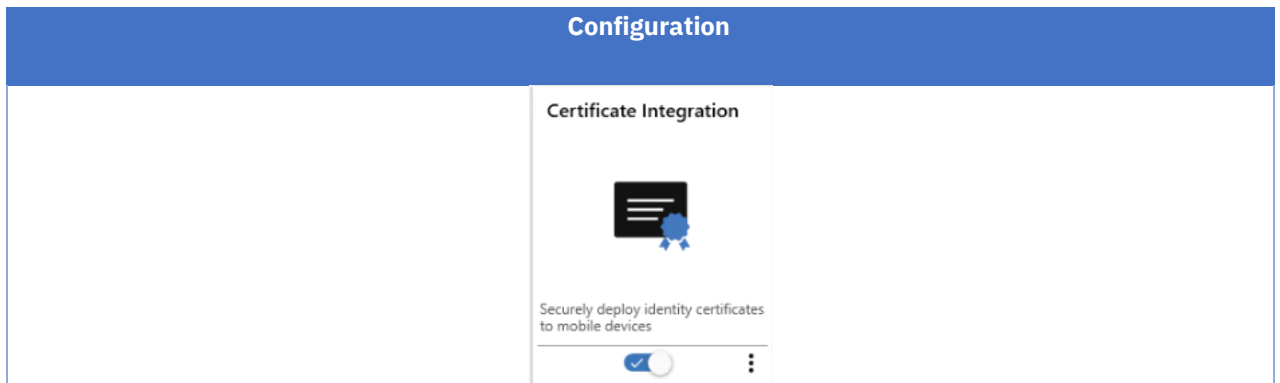
Setup MaaS360 Cloud Extender to integrate with a PKI.

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.

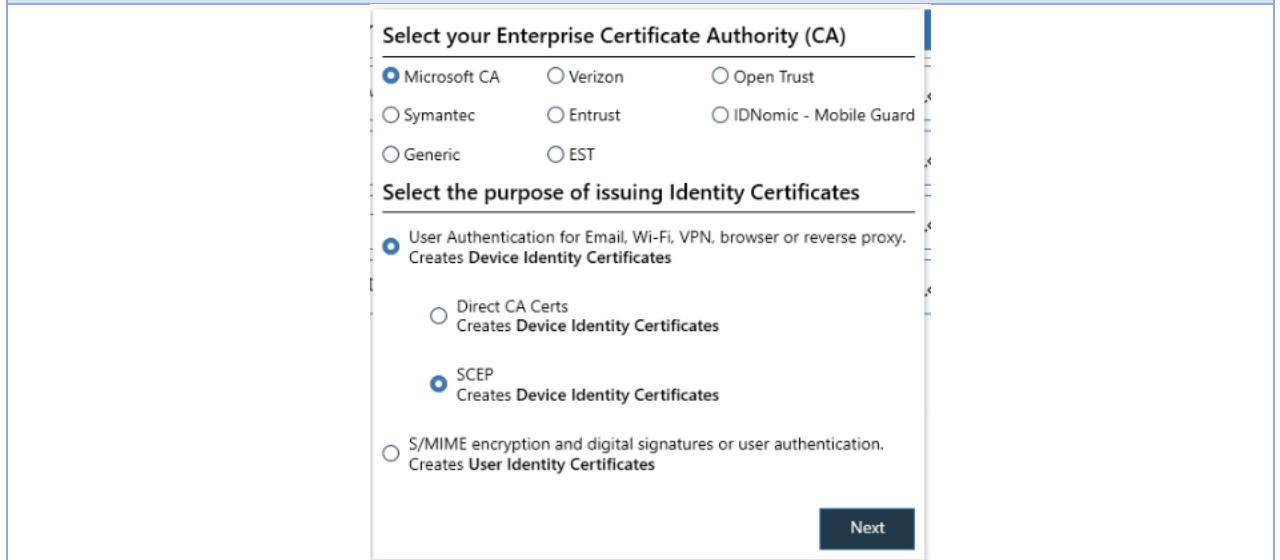
Detailed instructions on how to set this up is described in the IBM MaaS360's Knowledge Center page under [Certificate Integration Cloud Extender module](#).

Configuration

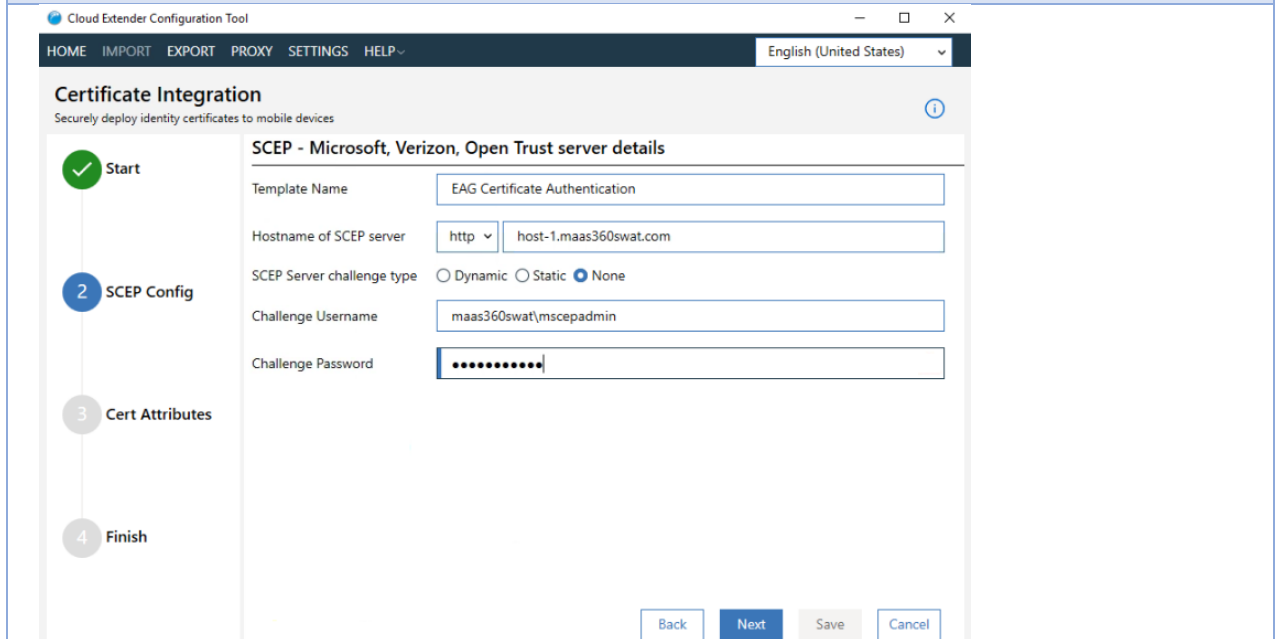
From Cloud Extender select the Certificate Integration module.



Once in the module, click “Add New Template”. This action will open the “Select your Enterprise Certificate Authority (CA)” panel below.



Make the following selections on this panel and click “Next”.



Configuration

Set the server details on the following panel and “Next”:

The screenshot shows the 'Certificate Integration' configuration panel in the 'Cloud Extender Configuration Tool'. The panel has a navigation sidebar on the left with steps: 1. Start (checked), 2. SCEP Config (checked), 3. Cert Attributes, and 4. Finish. The main area is titled 'Certificate Properties' and contains the following fields:

- Subject Name:** A text input field containing the value `/CN=%dn%`. This field is highlighted with a red rectangular border.
- Subject Alternate Name:** A dropdown menu currently set to 'UPN'.
- Cache certs on Cloud Extender:** An unchecked checkbox.
- Location of Certificate Cache:** A text input field with the placeholder 'Choose a location to store cached certificates' and a 'Browse' button to its right.

At the bottom of the panel, there are four buttons: 'Back', 'Next' (highlighted in blue), 'Save', and 'Cancel'.

Configure the Subject Name of the certificate to have the user Distinguished Name (DN).

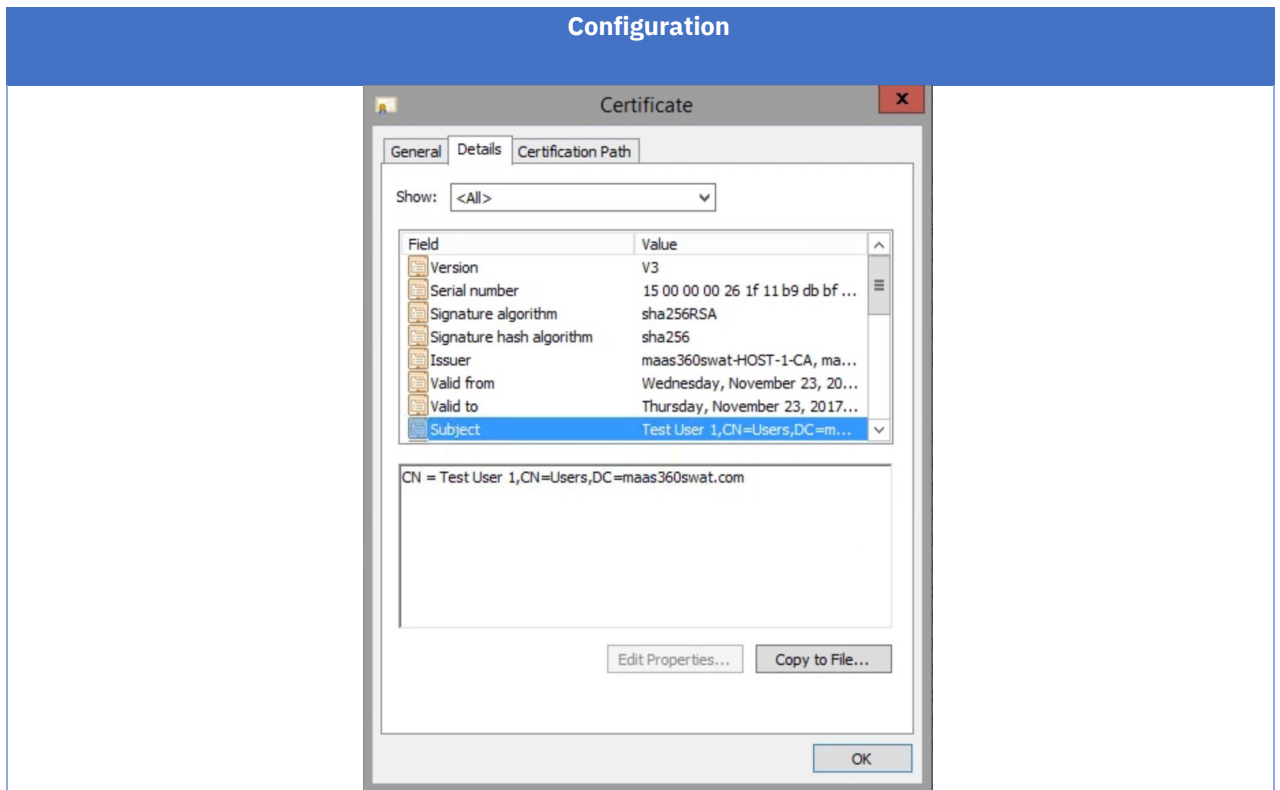
The format is: `/CN=%dn%`.

This requires MaaS360 User

Visibility Service to be enabled in order for MaaS360 to have access to user 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.



The issued certificate will look like this.

The Subject Name will have the user DN

```
<XMLUMI>
<!-- Certificate Example A --!>
  <stsuser:STSUniversalUser xmlns:stsuser="urn:ibm:names:ITFIM:1.0:stsuser">
    <stsuser:Principal>
      <stsuser:Attribute name="name">
        <stsuser:Value>CN=Test User 1,CN=Users,DC=maas360swat.com</stsuser:Value>
      </stsuser:Attribute>
    </stsuser:Principal>
    <stsuser:AttributeList>
      <stsuser:Attribute name="SubjectCN"
type="urn:ibm:security:gskit">
        <stsuser:Value> Test User 1,CN=Users,DC=maas360swat.com</stsuser:Value>
      </stsuser:Attribute>
    </stsuser:AttributeList>
  </stsuser:STSUniversalUser>
</XMLUMI>
```

This certificate when presented to EAG is represented in an XML format.

The section marked in **blue** is attribute that EAG needs to extracted, properly formatted and compared against the user Distinguished Name (DN) on LDAP.

EAG Configuration:

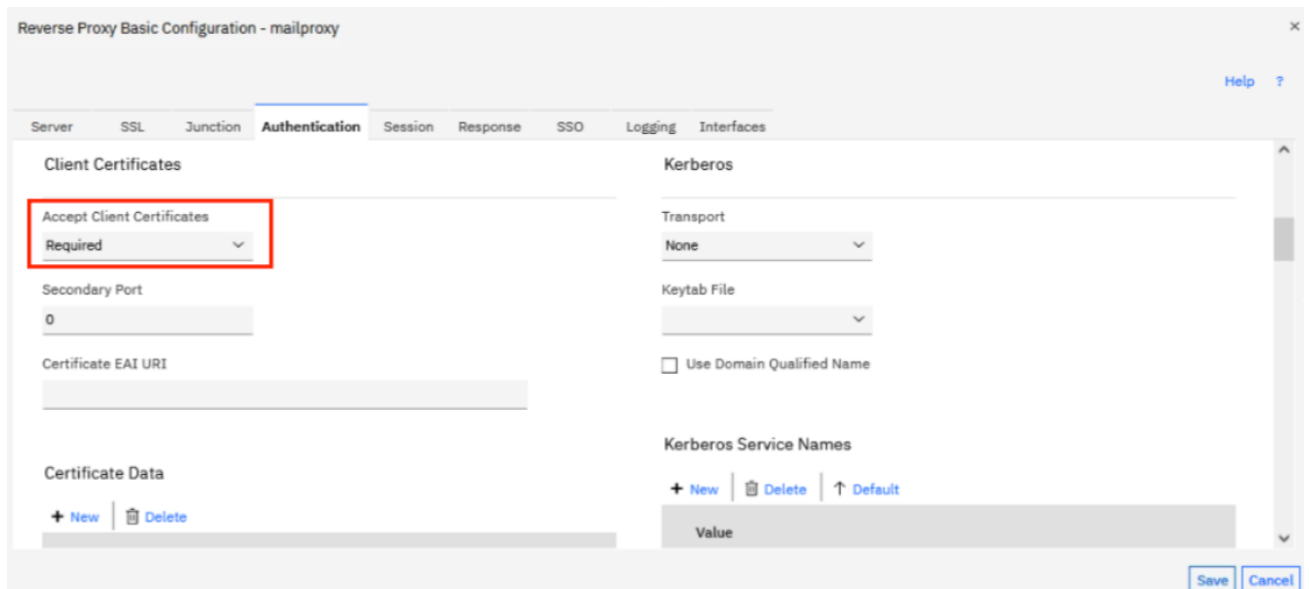
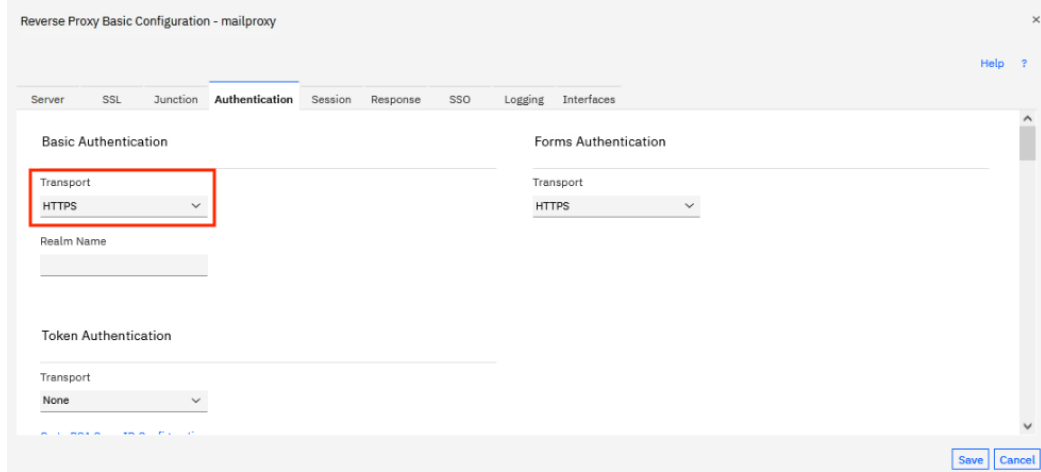
To configure EAG to use certificates the following steps needs to be completed:

- Enable Client Certificates
- Setup Certificate Mapping

Enable Client Certificates:

Configuration

From IBM Security Verify Access Local Management Interface



Browser to *Web > Reverse Proxy*

Select the proxy instance and click Edit

On Authentication, set *Basic Authentication >> Transport = HTTPS*

Set *Client Certificates >> Accept Client Certificates = Required*

Click Save

Configuration

! **Pending Changes**
 There is currently one undeployed change.

?

Review Pending Changes

i **System Notification** ×
 Successfully submitted changes to configuration.

Click on Review Pending Changes to deploy changes.

Deploy Pending Changes ×

Module	Date Modified
Reverse Proxy Configuration File	Jul 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

NOTE: This XSL Template assumes usage of NDES

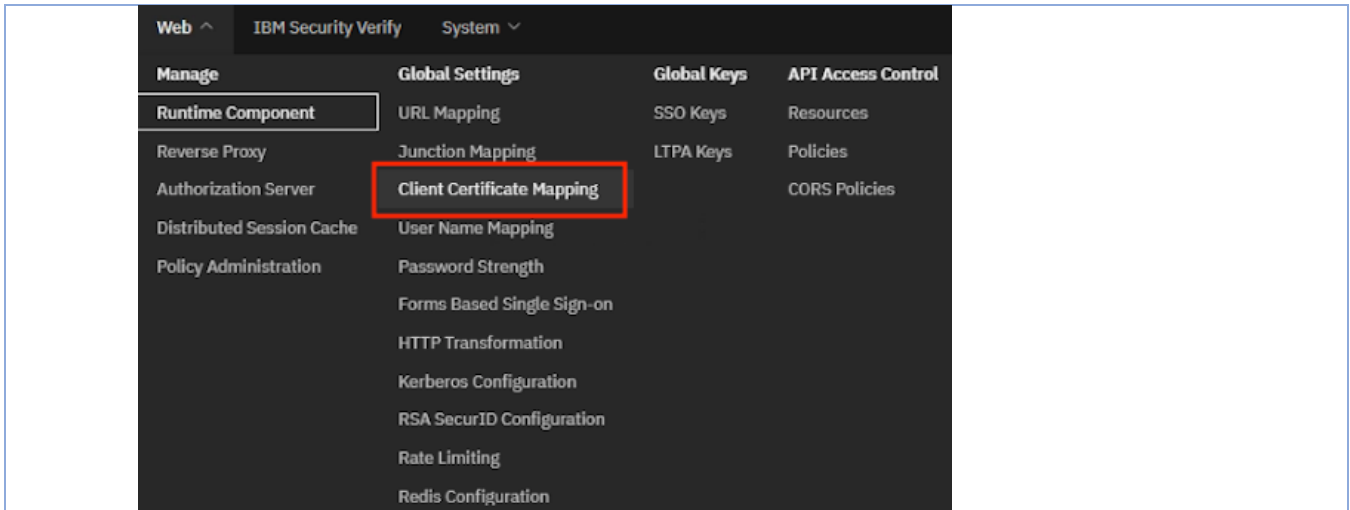
Below the template contents can be observed. Modify provided XSL template above with the domain name and other information that is different that given example :

```

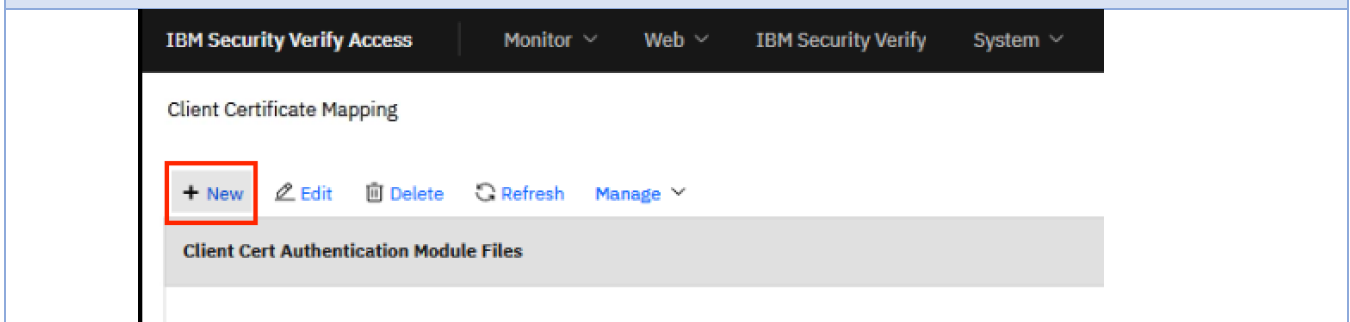
<!-- XSL-Template.txt -->
<xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:stsuser="urn:ibm:names:ITFIM:1.0:stsuser"
version="1.0">
  <xsl:output method="text" omit-xml-declaration="yes"
encoding='UTF-8' indent="no"/>
  <xsl:template match="text()"/>
  <xsl:template
match="/XMLUMI/stsuser:STUniversalUser/stsuser:AttributeList">
    <xsl:variable name="subjectCN">
      <xsl:call-template name="tokenize">
        <xsl:with-param name="rawSubjectCN"
select="stsuser:Attribute[@name='SubjectCN']/stsuser: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,','.> !CN=<xsl:value-of select="substring- before($subjectCN,','.>DC=com!
          </xsl:when>
          <xsl:otherwise> !CN=<xsl:value-of select="$subjectCN" />!
        </xsl:otherwise>
      </xsl:choose>
    </xsl:when>
    <xsl:otherwise> !CN=<xsl:value-of select="substring before($subjectCN,','.>DC=com!
  </xsl:otherwise>
  </xsl:choose>
</xsl:template>
  <xsl:template name="tokenize">
    <!-- this template removes backslashes, might be
not needed -->
    <xsl:param name="rawSubjectCN" />
    <xsl:variable name="first-item" select="normalize-
space(substring-before(concat($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>

```

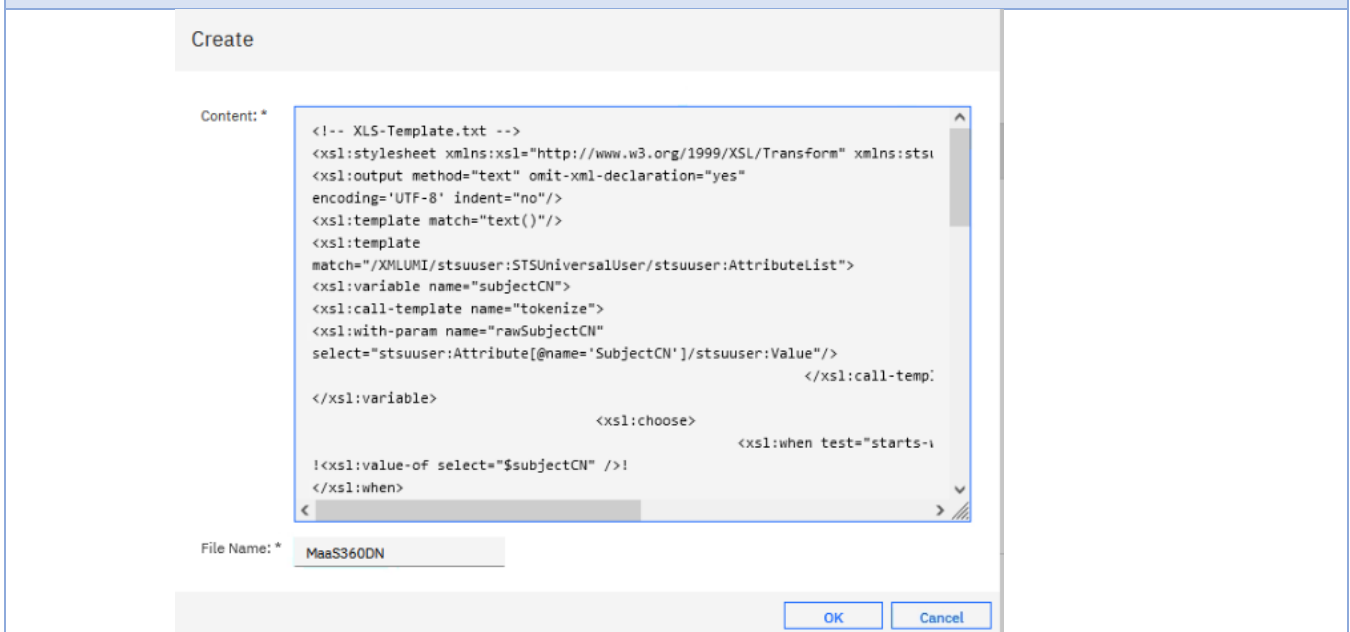
XSL Template can be modified from the IBM Security Verify Access management interface. See steps below.



Go to Web > Global Settings > Client Certificate Mapping > Client Certificate Mapping



Select New to access the XSL Template

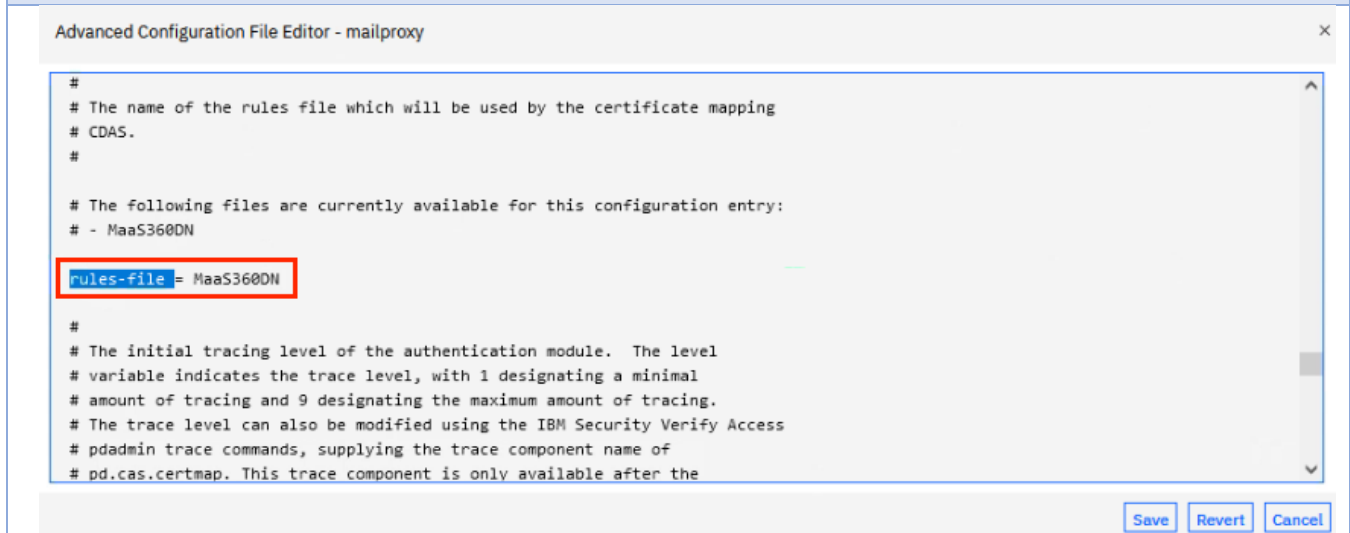


Copy the entire content of the XSL-Template.txt. Clear the contents of the screen and paste the copied contents of the XSL-Template.txt

Save the file with the name
MaaS360DN



Deploy the changes and restart reverse proxy.

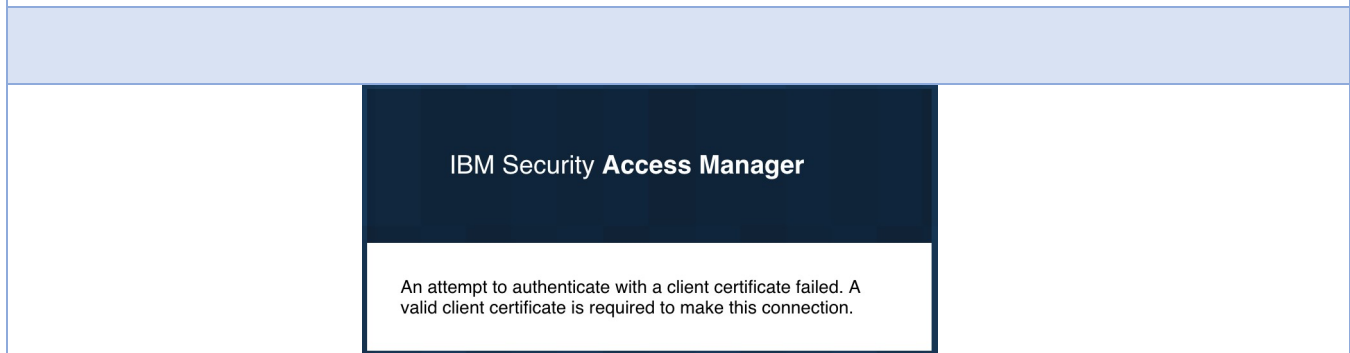


**Navigate to Web > Reverse Proxy > select proxy instance
Manage > Configuration > Edit Configuration File**

**Search for the parameter:
rules-file**

**Configure the rules-file value to the Client Certificate Mapping
File from the previous step -
MaaS360DN**

Save and Deploy the changes. Restart the reverse proxy



**Browse to the EAG data interface (in this example
<https://mail.maas360swat.com>)**

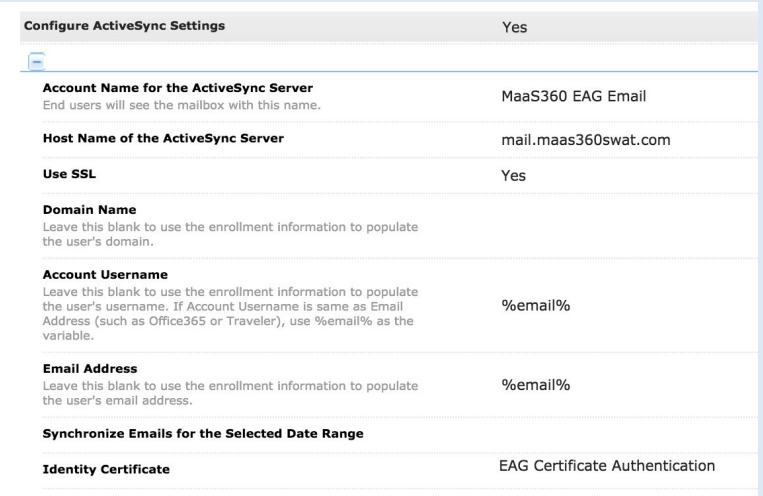
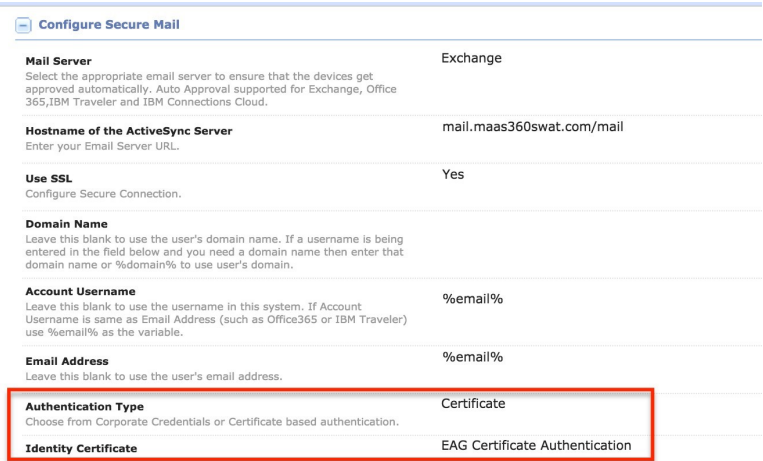
An error should be displayed as shown indicating that the EAG is configured to require an Identity Certificate for authentication

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

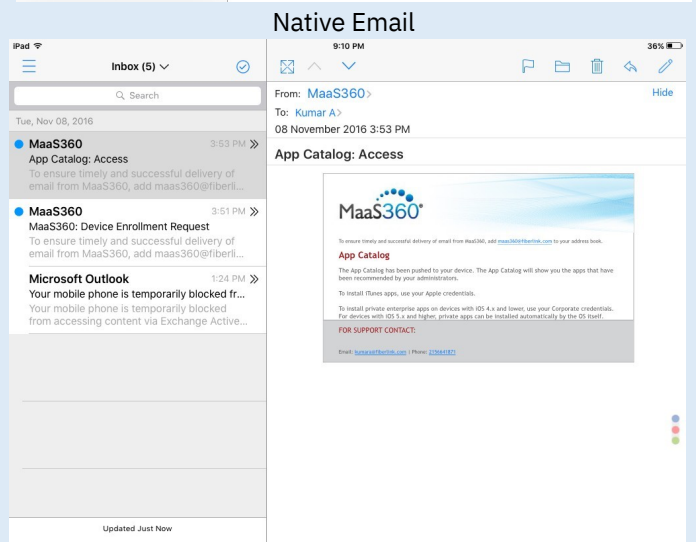
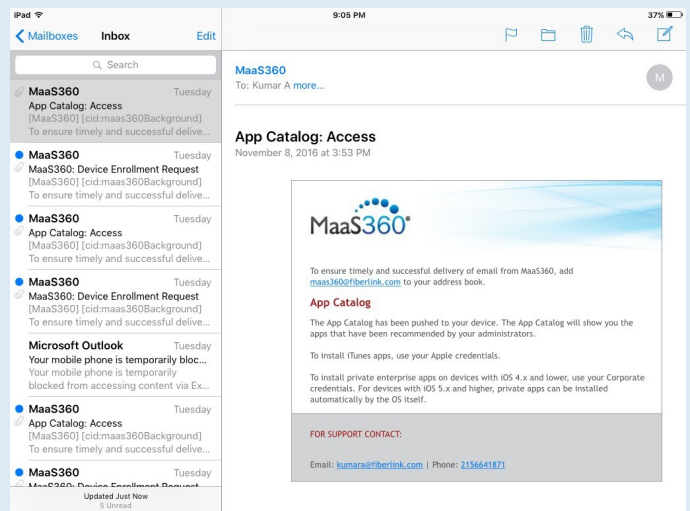
MaaS360 Configuration:

#	Configuration	Screenshot
	<p>If native email needs to be configured on end user devices, MaaS360 MDM policies need to be configured.</p> <ul style="list-style-type: none"> Browse to Security >> Policies on the MaaS360 portal. On iOS, Android or Windows MDM policy, browse to Device Settings >> ActiveSync Configure the hostname to point to the data interface of EAG (mail.maas360swat.com) Enable SSL The username and email fields can be configured with wildcard variables. Use %email% or %upn% for both Username and Email Address field since this user authentication is now configured to use UPN Leave Domain Name as blank. Save and Publish the policy 	
	<p>If MaaS360 Secure Mail needs to be configured on end user devices, MaaS360 Persona policies need to be configured.</p> <p>Browse to Security >> Policies on the MaaS360 portal.</p> <ul style="list-style-type: none"> On persona policy, browse to Email >> Configuration Choose the Mail Server type. Configure the hostname to point to the data interface of EAG (mail.maas360swat.com) Enable Use SSL The username and email fields can be configured with wildcard . Use %email% or %upn% for both Username and Email Address field since this user authentication is now configured to use UPN Leave Domain Name as blank. 	

	<ul style="list-style-type: none">• Set Authentication Type to Password.• Save and Publish the policy	
--	---	--

Enter the email password on the end device. Mail should start to sync

MaaS360 Secure Mail also displays the Identity Certificate that is used for authentication before prompting to enter the password.



MaaS360 Secure Mail

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.

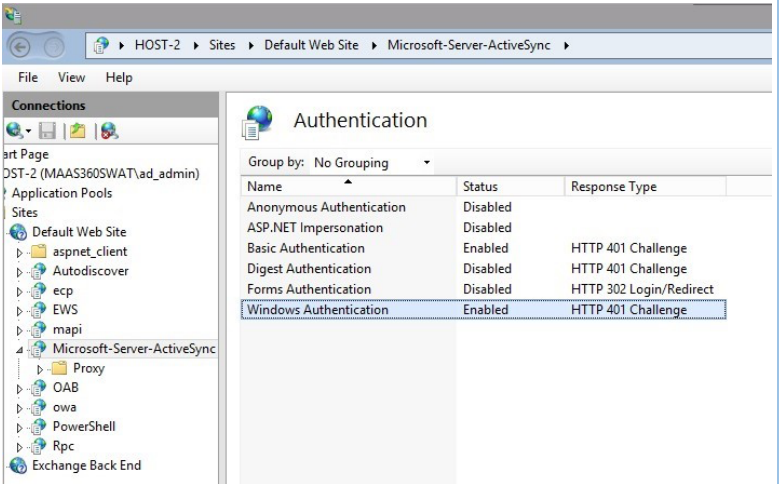
Workflow:

- 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:

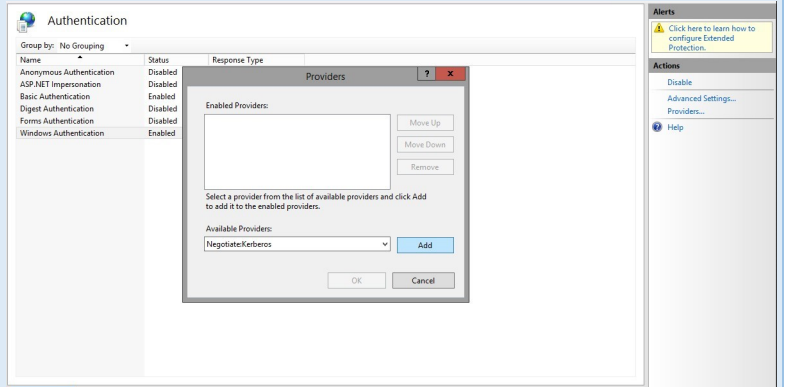
1. Setup Cloud Extender for Direct Certificate Authority Integration
2. Setup Certificate Mapping
3. Configure Kerberos Constrained Delegation
4. Enable Kerberos SSO for HTTPS junction

#	Configuration	Screenshot																					
	Complete all the steps for EAG configuration in Scenario #4. This covers Steps 1 – 3 above.																						
	<p>Ensure that ActiveSync application on the server is configured for Kerberos authentication.</p> <p>In Microsoft IIS, set the permission on MS-Server-ActiveSync site to have Windows Authentication enabled</p>	 <p>The screenshot shows the IIS Manager interface. The left-hand pane displays the 'Connections' tree with the path: HOST-2 > Sites > Default Web Site > Microsoft-Server-ActiveSync. The right-hand pane shows the 'Authentication' settings for this site. A table lists various authentication methods with their status and response types:</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Status</th> <th>Response Type</th> </tr> </thead> <tbody> <tr> <td>Anonymous Authentication</td> <td>Disabled</td> <td></td> </tr> <tr> <td>ASP.NET Impersonation</td> <td>Disabled</td> <td></td> </tr> <tr> <td>Basic Authentication</td> <td>Enabled</td> <td>HTTP 401 Challenge</td> </tr> <tr> <td>Digest Authentication</td> <td>Disabled</td> <td>HTTP 401 Challenge</td> </tr> <tr> <td>Forms Authentication</td> <td>Disabled</td> <td>HTTP 302 Login/Redirect</td> </tr> <tr> <td>Windows Authentication</td> <td>Enabled</td> <td>HTTP 401 Challenge</td> </tr> </tbody> </table>	Name	Status	Response Type	Anonymous Authentication	Disabled		ASP.NET Impersonation	Disabled		Basic Authentication	Enabled	HTTP 401 Challenge	Digest Authentication	Disabled	HTTP 401 Challenge	Forms Authentication	Disabled	HTTP 302 Login/Redirect	Windows Authentication	Enabled	HTTP 401 Challenge
Name	Status	Response Type																					
Anonymous Authentication	Disabled																						
ASP.NET Impersonation	Disabled																						
Basic Authentication	Enabled	HTTP 401 Challenge																					
Digest Authentication	Disabled	HTTP 401 Challenge																					
Forms Authentication	Disabled	HTTP 302 Login/Redirect																					
Windows Authentication	Enabled	HTTP 401 Challenge																					

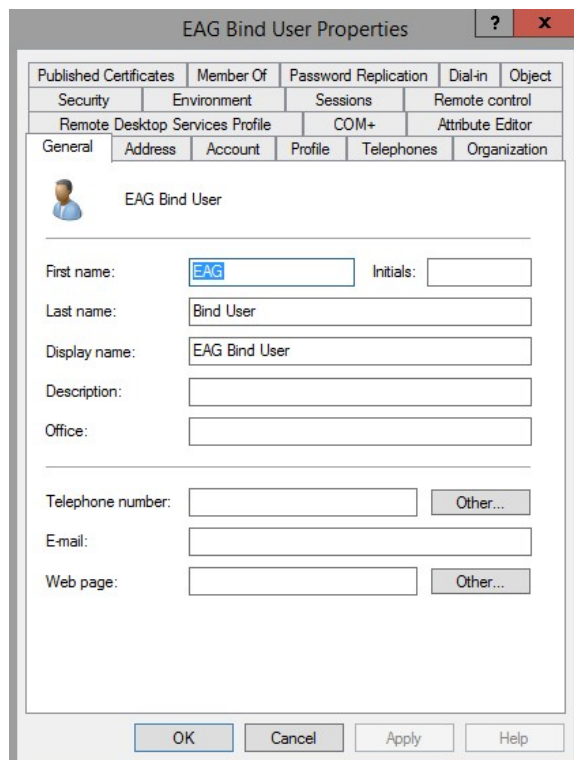
Ensure that Negotiate:Kerberos is listed as an available provider for Windows Authentication.

If it is not listed, add Negotiate:Kerberos provider to the list.

Restart IIS after the changes are made



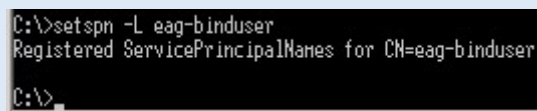
Identify a domain user that can be used as a service account in EAG to request Kerberos service tickets



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.

Command:
setspn -L eag-binduser

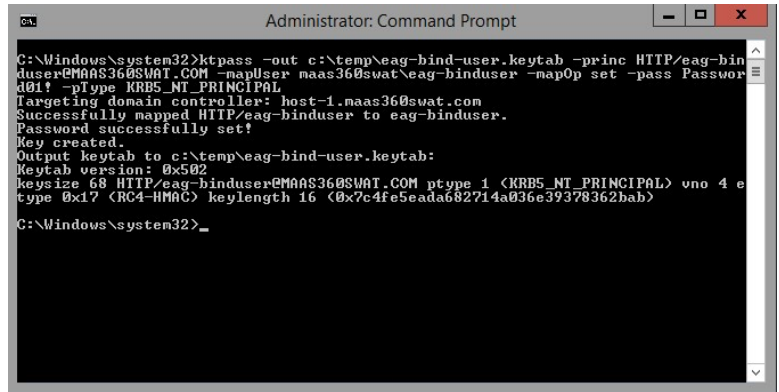


Generate a keytab file for the service account user and register the user principal in Active Directory for future Kerberos transactions

Command: ktpass -out C:\Windows\Temp\eag-binduser.keytab -princ HTTP/eag-binduser@MAAS360SWAT.COM -mapUser maas360swat\eag-binduser -mapOp set -pass Password01! -pType KRB5_NT_PRINCIPAL

Note: that the @DOMAIN.NAME must be in an upper case for the HTTP principal attribute

Confirm that the keytab file has been created.



Name	Date modified	Type	Size
eag-bind-user.keytab	19/01/2017 16:40	KEYTAB File	1 KB

Update service account user in Active Directory and set delegation for the email server

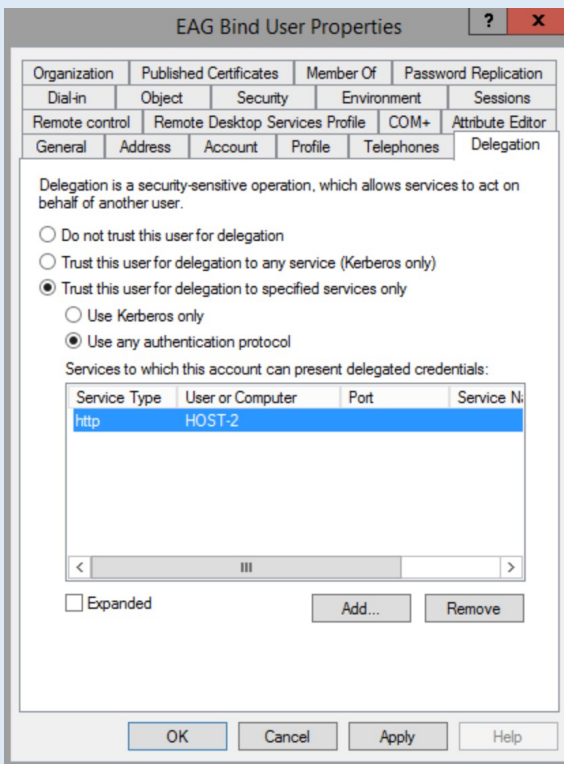
Open the user account properties and select **Delegation**

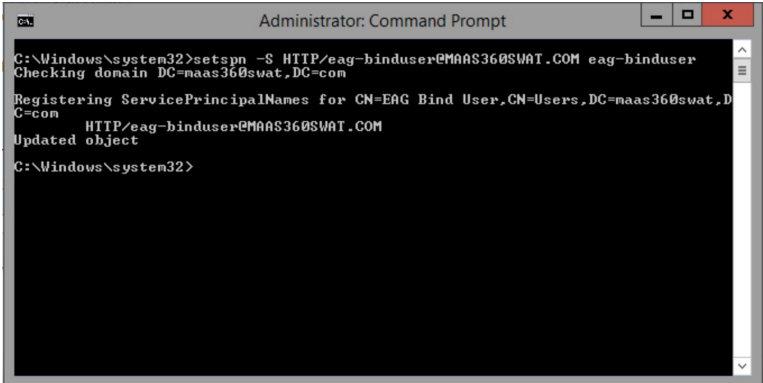
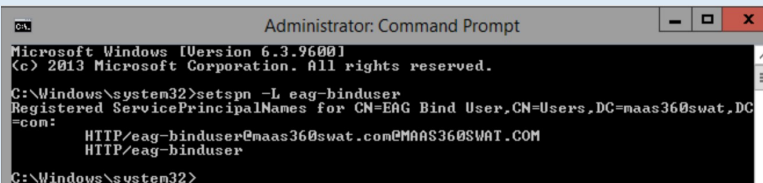
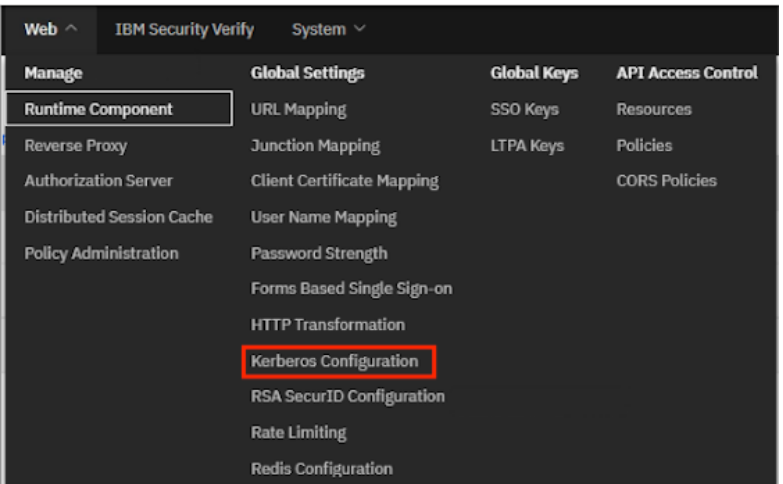
Select **Trust using authentication protocol**

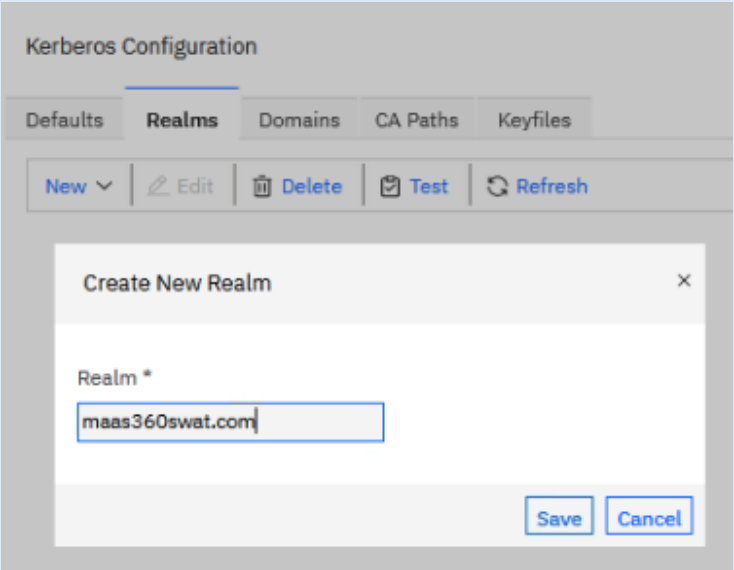
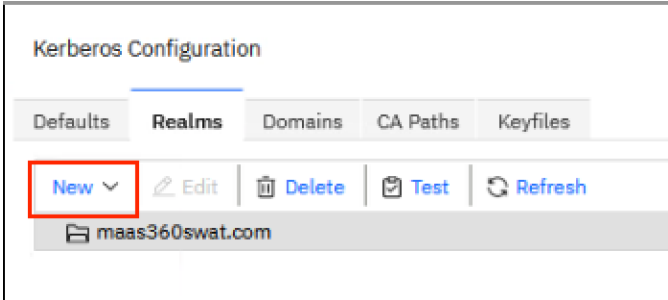
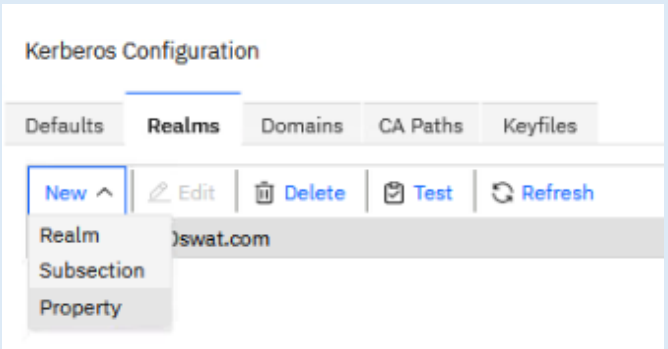
Click Add >> Users or Computers >> enter name for the mail server and >> Check Names >> OK

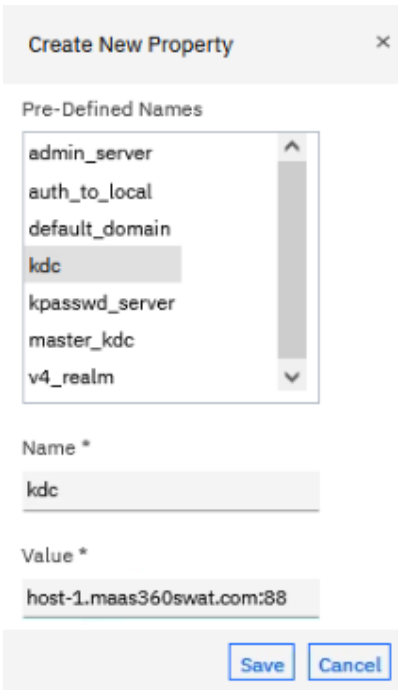
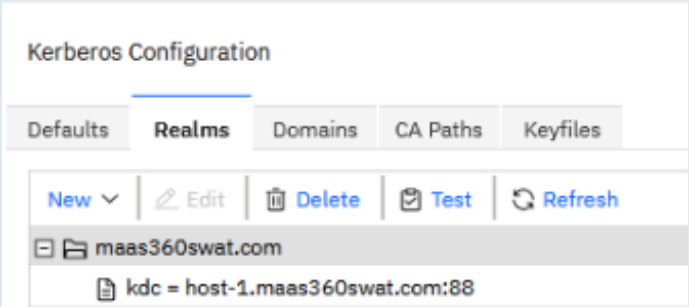
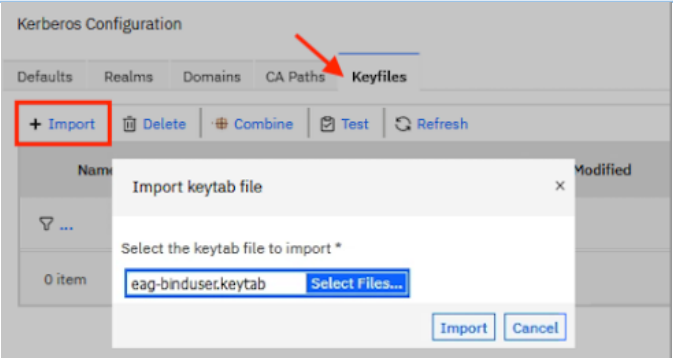
Scroll down the Services list and ensure to select the **Service Type** as **http**

Apply the changes on the service account user



<p>Add another SPN of the service account user: HTTP/eag-binduser@maas360swat.com@MAAS360SWAT.COM</p> <pre>setspn -S HTTP/eag-binduser@maas360swat.com@MAAS360SWAT.COM maas360swat\eag-binduser</pre>	 <pre>Administrator: Command Prompt C:\Windows\system32>setspn -S HTTP/eag-binduser@MAAS360SWAT.COM eag-binduser Checking domain DC=maas360swat.DC=com Registering ServicePrincipalNames for CN=EAG Bind User,CN=Users,DC=maas360swat.DC=com HTTP/eag-binduser@MAAS360SWAT.COM Updated object C:\Windows\system32></pre>
<p>Review the configured service principal names (SPN).</p> <p>Command: setspn -L eag-binduser</p>	 <pre>Administrator: Command Prompt Microsoft Windows [Version 6.3.9600] (c) 2013 Microsoft Corporation. All rights reserved. C:\Windows\system32>setspn -L eag-binduser Registered ServicePrincipalNames for CN=EAG Bind User,CN=Users,DC=maas360swat.DC=com: HTTP/eag-binduser@maas360swat.com@MAAS360SWAT.COM HTTP/eag-binduser C:\Windows\system32></pre>
<p><u>Configure Kerberos Realm:</u></p> <p>Browse to Web > Global Settings >> Kerberos Configuration.</p>	 <p>The screenshot shows a web-based configuration interface for IBM Security Verify. The navigation menu includes 'Web', 'IBM Security Verify', and 'System'. Under 'Web', there are sections for 'Manage', 'Global Settings', 'Global Keys', and 'API Access Control'. The 'Global Settings' section is expanded, showing options like 'URL Mapping', 'Junction Mapping', 'Client Certificate Mapping', 'User Name Mapping', 'Password Strength', 'Forms Based Single Sign-on', 'HTTP Transformation', 'Kerberos Configuration' (highlighted with a red box), 'RSA SecurID Configuration', 'Rate Limiting', and 'Redis Configuration'.</p>

<p>Click Realm, select New >> Realm</p> <p>Enter the Kerberos realm, this value can be the directory domain name.</p> <p>Do not use spaces in the Realm Name</p> <p>Hit Save</p> <p>Deploy pending changes and restart reverse proxy for changes to take effect.</p>	 <p>The screenshot shows the 'Kerberos Configuration' interface with the 'Realms' tab selected. A 'Create New Realm' dialog box is open, featuring a text input field for 'Realm *' containing 'maas360swat.com'. Below the input field are 'Save' and 'Cancel' buttons. The background interface includes tabs for 'Defaults', 'Realms', 'Domains', 'CA Paths', and 'Keyfiles', and a toolbar with 'New', 'Edit', 'Delete', 'Test', and 'Refresh' options.</p>
<p>Select the new realm and look for the "New" pulldown just above the name.</p>	 <p>This screenshot shows the 'Kerberos Configuration' interface with the 'Realms' tab selected. The 'New' button in the toolbar is highlighted with a red rectangular box. Below the toolbar, the realm 'maas360swat.com' is visible in a list view.</p>
<p>Click New > Property</p>	 <p>This screenshot shows the 'Kerberos Configuration' interface with the 'Realms' tab selected. The 'New' button's dropdown menu is open, displaying options: 'Realm', 'Subsection', and 'Property'. The 'Property' option is highlighted, indicating it has been selected.</p>

<p>In the Create New Property window, select kdc</p> <p>Enter the Directory KDC address in the Value field. The Directory KDC address is the name of the domain controller. For example, <machine>.<domain>, click Save</p> <p>Note that using port 88 is optional for Active Directory as this is default value</p> <p>Depending on the configuration, using the domain name may be a more preferred option instead of linking to only a single directory server. In this example, the setting is : maas360swat.com</p> <p>Deploy changes.</p>	
<p>The following realm is now created</p>	
<p>On Keyfiles, click on the Import button to import the keytab file that was generated for the EAG service account user</p>	

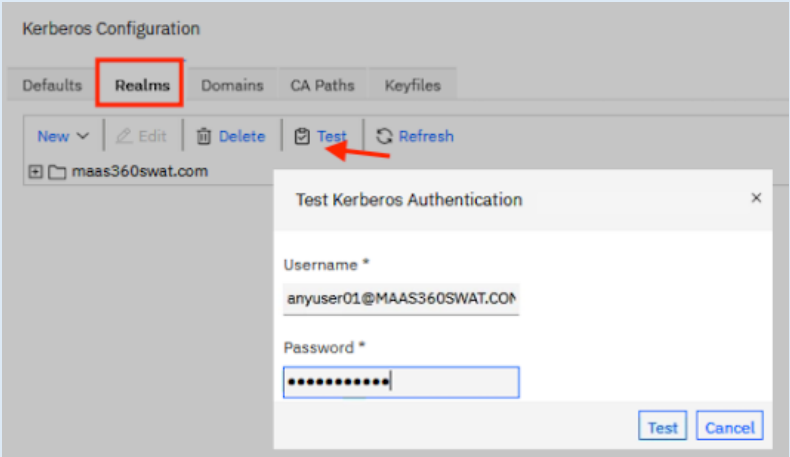

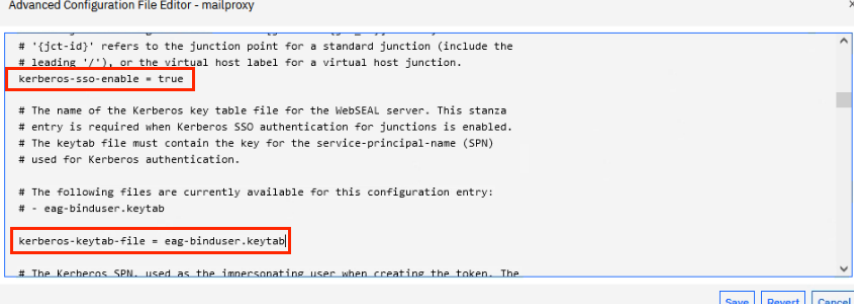
Deploy the pending changes.

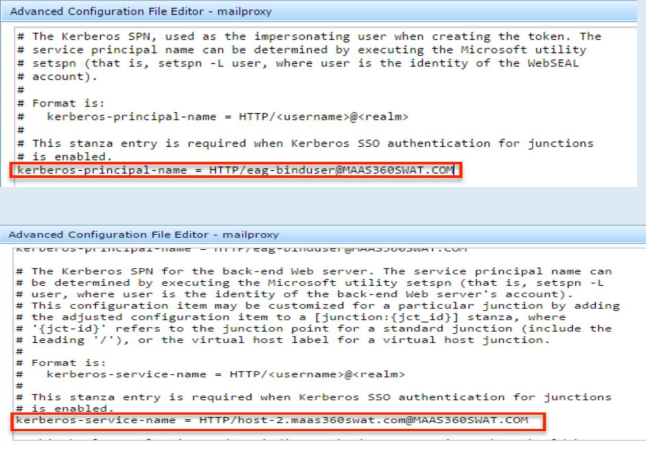
On Defaults, select the **default_realm** item, Edit and set the value to the newly created Kerberos realm on the pull down.

Deploy the pending changes and restart the reverse proxy instance

Select **Keyfiles**, select the keytab file and test authentication with the recently configured SPN:
[HTTP/eag-binduser@MAAS360SWAT.COM](http://eag-binduser@MAAS360SWAT.COM)

If the setup is correct, a successful test action notification is shown

<p>Confirm Kerberos authentication is working as expected for any user</p> <p>Select the newly configured Realm from Realms and click Test</p> <p>Enter the valid credentials for a user in the corporate directory in the format user@DOMAIN.NAME</p> <p>Confirm test is successful.</p>	 <p>The screenshot shows the 'Kerberos Configuration' window with the 'Realms' tab active. A 'Test' button is highlighted with a red arrow. A modal dialog titled 'Test Kerberos Authentication' is open, containing fields for 'Username *' (filled with 'anyuser01@MAAS360SWAT.COM') and 'Password *' (masked with dots). 'Test' and 'Cancel' buttons are at the bottom right.</p>
<p>Browser to Web > Manage > Reverse Proxy</p> <p>Select the reverse proxy instance.</p> <p>Click Manage >> Configuration >> Edit Configuration File.</p> <p>Locate the [junction] stanza.</p>	 <p>The screenshot shows the 'Advanced Configuration File Editor - mailproxy' window. The configuration file content is visible, with the '[junction]' stanza highlighted in green. The text includes comments about the listen-interface, junction location, and available files like 'jmt.conf'.</p>
<p>Update the following properties:</p> <p>kerberos-ss0-enable = true</p> <p>kerberos-keytab-file = eag-binduser.keytab</p>	 <p>The screenshot shows the 'Advanced Configuration File Editor - mailproxy' window with the configuration file updated. Two lines are highlighted with red boxes: 'kerberos-ss0-enable = true' and 'kerberos-keytab-file = eag-binduser.keytab'. The rest of the configuration text is visible in the background.</p>

<p>Update the following properties:</p> <p>kerberos-principal-name = HTTP/eag-binduser@MAAS360SWAT.COM</p> <p>kerberos-service-name = HTTP/host-2.maas360swat.com@MAAS360SWAT.COM</p> <p>Note that these values are replaced with those specific to the current implementation</p>	 <p>The top screenshot shows the configuration for 'kerberos-principal-name' set to 'HTTP/eag-binduser@MAAS360SWAT.COM'. The bottom screenshot shows the configuration for 'kerberos-service-name' set to 'HTTP/host-2.maas360swat.com@MAAS360SWAT.COM'. Both values are highlighted with a red box in the original image.</p>
<p>Deploy changes and restart the reverse proxy instance</p>	<p>Test authentication with MaaS360 Secure Mail. Authentication should succeed with certificates and the end user should not be prompted for a password.</p>

MaaS360 Configuration:

#	Configuration	Screenshot
	<p>MaaS360 configuration remains the same as Scenario #4</p>	