Authenticating SMTP Sessions Using Client Certificates

This chapter contains the following sections:

- Overview of Certificates and SMTP Authentication, on page 1
- Checking the Validity of a Client Certificate, on page 3
- Authenticating a User Using an LDAP Directory, on page 4
- Authenticating an SMTP Connection Over TLS Using a Client Certificate, on page 4
- Establishing a TLS Connection from the Email Gateway, on page 5
- Updating a List of Revoked Certificates, on page 6

Overview of Certificates and SMTP Authentication

The email gateway supports the use of client certificates to authenticate SMTP sessions between the email gateway and users' mail clients. The email gateway can request a client certificate from a user's mail client when the application attempts to connect to the email gateway to send messages. When the email gateway receives the client certificate, it verifies that the certificate is valid, has not expired, and has not been revoked. If the certificate is valid, the email gateway allows an SMTP connection from the mail application over TLS.

Organizations that require their users to use a Common Access Card (CAC) for their mail clients can use this feature to configure the email gateway to request a certificate that the CAC and ActivClient middleware application will provide to the email gateway.

You can configure the email gateway to require users to provide a certificate when sending mail, but still allow exceptions for certain users. For these users, you can configure the email gateway to use the SMTP authentication LDAP query to authenticate the user.

Users must configure their mail client to send messages through a secure connection (TLS) and accept a server certificate from the email gateway.

Related Topics

- How to Authenticate a User with a Client Certificate, on page 2
- How to Authenticate a User with an SMTP Authentication LDAP Query, on page 2
- How to Authenticate a User with an LDAP SMTP Authentication Query if the Client Certificate is Invalid, on page 2

How to Authenticate a User with a Client Certificate

Table 1: How to Authenticate a User with a Client Certificate

	Do This	More Info
Step 1	Define a certificate query for your LDAP server.	Checking the Validity of a Client Certificate, on page 3
Step 2	Create a certificate-based SMTP authentication profile.	Authenticating an SMTP Connection Over TLS Using a Client Certificate, on page 4
Step 3	Configure a listener to use the certificate SMTP authentication profile.	Listening for Connection Requests by Creating a Listener Using Web Interface
Step 4	Modify the RELAYED mail flow policy to require TLS, a client certificate, and SMTP authentication.	Establishing a TLS Connection from the Email Gateway, on page 5

How to Authenticate a User with an SMTP Authentication LDAP Query

Table 2: How to Authenticate a User with an SMTP Authenticate LDAP Query

	Do This	More Info
Step 1	Define an SMTP authentication query for your server that uses an allowance query string and Bind for the authentication method.	Authenticating a User Using an LDAP Directory, on page 4
Step 2	Create an LDAP-based SMTP authentication profile.	Configuring AsyncOS for SMTP Authentication
Step 3	Configure a listener to use the LDAP SMTP authentication profile.	If the user is not allowed to use LDAP-based SMTP authentication for their connection, you can select whether the email gateway rejects the connection or temporarily allows it while logging all activity.
Step 4	Modify the RELAYED mail flow policy to require TLS and SMTP authentication.	Establishing a TLS Connection from the Email Gateway, on page 5

How to Authenticate a User with an LDAP SMTP Authentication Query if the Client Certificate is Invalid

Table 3: How to Authenticate a User with a Client Certificate or an LDAP SMTP Authentication Query

	Do This	More Info
Step 1	Define an SMTP authentication query for your server that uses an allowance query string and Bind for the authentication method.	Authenticating a User Using an LDAP Directory, on page 4

	Do This	More Info
Step 2	Define a certificate-based query for your LDAP server.	Checking the Validity of a Client Certificate, on page 3
Step 3	Create a certificate-based SMTP authentication profile	Authenticating an SMTP Connection Over TLS Using a Client Certificate, on page 4
Step 4	Create an LDAP SMTP authentication profile.	Configuring AsyncOS for SMTP Authentication
Step 5	Configure a listener to use the certificate SMTP authentication profile.	Listening for Connection Requests by Creating a Listener Using Web Interface
Step 6	1. Modify the RELAYED mail flow policy to use the following settings: 2. TLS Preferred 3. SMTP authentication required 4. Require TLS for SMTP authentication	Establishing a TLS Connection from the Email Gateway, on page 5

Checking the Validity of a Client Certificate

The Certificate Authentication LDAP query checks the validity of a client certificate in order to authenticate an SMTP session between the user's mail client and the email gateway. When creating this query, you select a list of certificate fields for authentication, specify the User ID attribute (the default is uid), and enter the query string.

For example, a query string that searches for the certificate's common name and serial number may look like `(&(objectClass-posixAccount)(caccn={cn})(cacserial={sn})`. After you have created the query, you can use it in a Certificate SMTP Authentication Profile. This LDAP query supports OpenLDAP, Active Directory, and Oracle Directory.

See LDAP Queries for more information on configuring LDAP servers.

Procedure

Step 1 Select **System Administration** > **LDAP**.

Step 2 Create a new LDAP profile. See Creating LDAP Server Profiles to Store Information About the LDAP Server for more information.

Step 3 Check the **Certificate Authentication Query** checkbox.

Step 4 Enter the query name.

Step 5 Enter the query string to authenticate the user's certificate. For example, `(&(objectClass=user)(cn={cn}))` .

Step 6 Enter the user ID attribute, such as `sAMAccountName` .

Step 7 Submit and commit your changes.

Authenticating a User Using an LDAP Directory

The SMTP Authentication LDAP query has an Allowance Query String that allows the email gateway to check whether the user's mail client is allowed to send mail through the email gateway based on the user's record in the LDAP directory. This allows users who don't have a client certificate to send mail as long as their record specifies that it's allowed.

You can also filter out results based on other attributes. For example, the query string `(&(uid={u})(|(!(caccn=*))(cacexempt=*)(cacemergency>={t})))` checks to see if any of the following conditions are true for the user:

- CAC is not issued to the user `( caccn=* )`
- CAC is exempt `( cacexempt=* )`
- the time period that a user may temporarily send mail without a CAC expires in the future `( cacemergency>={t} )`

See Configuring AsyncOS for SMTP Authentication for more information on using the SMTP Authentication query.

Procedure

Step 1	Select **System Administration > LDAP**.
Step 2	Define an LDAP profile. See Creating LDAP Server Profiles to Store Information About the LDAP Server for more information.
Step 3	Define an SMTP authentication query for the LDAP profile.
Step 4	Check the SMTP Authentication Query checkbox.
Step 5	Enter the query name.
Step 6	Enter the string to query for the user's ID. For example, `(uid={u})`.
Step 7	Select LDAP BIND for the authentication method.
Step 8	Enter an allowance query string. For example, `(&(uid={u})(|(!(caccn=*))(cacexempt=*)(cacemergency>={t})))` .
Step 9	Submit and commit your changes.

Authenticating an SMTP Connection Over TLS Using a Client Certificate

The certificate-based SMTP authentication profile allows the email gateway to authenticate an SMTP connection over TLS using a client certificate. When creating the profile, you select the Certificate Authentication LDAP query to use for verifying the certificate. You can also specify whether the email gateway falls back to the **`SMTP AUTH`** command to authenticate the user if a client certificate is not available.

For information on authenticating an SMTP connection by using LDAP, see Configuring AsyncOS for SMTP Authentication.

Procedure

Step 1 Select **Network > SMTP Authentication**.

Step 2 Click **Add Profile**.

Step 3 Enter the name for the SMTP authentication profile.

Step 4 Select **Certificate** for the Profile Type.

Step 5 Click **Next**.

Step 6 Enter the profile name.

Step 7 Select the certificate LDAP query you want to use with this SMTP authentication profile.

Note
Do not select the option to allow the SMTP AUTH command if a client certificate is not available.

Step 8 Click **Finish**.

Step 9 Submit and commit your changes.

Establishing a TLS Connection from the Email Gateway

The Verify Client Certificate option in the RELAYED mail flow policy directs the email gateway to establish a TLS connection to the user's mail application if the client certificate is valid. If you select this option for the TLS Preferred setting, the email gateway still allows a non-TLS connection if the user doesn't have a certificate, but rejects a connection if the user has an invalid certificate. For the TLS Required setting, selecting this option requires the user to have a valid certificate in order for the email gateway to allow the connection.

To authenticate a user's SMTP session with a client certificate, select the following settings:

- TLS - Required
- Verify Client Certificate
- Require SMTP Authentication

Note Although SMTP authentication is required, the email gateway will not use the SMTP authentication LDAP query because it is using certificate authentication.

To authenticate a user's SMTP session using the SMTP authentication query instead of a client certificate, select the following settings for the RELAYED mail flow policy:

- TLS - Required
- Require SMTP Authentication

If you require the email gateway to ask for a client certificate from certain users while allowing LDAP-based SMTP authentication from others, select the following settings for the RELAYED mail flow policy:

- TLS - Preferred
- Require SMTP Authentication
- Require TLS to Offer SMTP Authentication

Updating a List of Revoked Certificates

The Email Security appliance checks a list of revoked certificates (called a Certificate Revocation List) as part of its certificate verification to make sure that the user's certificate hasn't been revoked. You keep an up-to-date version of this list on a server and the email gateway downloads it on a schedule that you create.

Procedure

Step 1 Go to **Network > CRL Sources**.

Step 2 Enable CRL checking for SMTP TLS connections:

a) Click Edit Settings under Global Settings.

b) (Optional) Select the **Global Settings** checkbox if you want to select all options:

- CRL check for inbound SMTP TLS.
- CRL check for outbound SMTP TLS
- CRL Check for Web Interface

c) Select the checkbox for either 'CRL check for inbound SMTP TLS', 'CRL check for outbound SMTP TLS' or 'CRL Check for Web Interface' options.

d) Submit your change.

Step 3 Click **Add CRL Source**.

Step 4 Enter a name for the CRL source.

Step 5 Select the file type. This can be either ASN.1 or PEM.

Step 6 Enter the URL for the primary source for the file, including the filename. For example, `https://crl.example.com/certs.crl`

Step 7 Optionally, enter the URL for a secondary source in case the email gateway cannot contact the primary source.

Step 8 Specify a schedule for downloading the CRL source.

Step 9 Enable the CRL source.

Step 10 Submit and commit your changes.

Authenticating a User's SMTP Session With a Client Certificate

Procedure

Step 1 Go to **System Administration > LDAP** to configure an LDAP server profile.s

Step 2 Define a certificate query for the LDAP profile.

a) Enter the query name.

b) Choose the certificate fields to authenticate, such as the serial number and common name.

c) Enter the query string. For example, `(&(caccn={cn})(cacserial={sn}))`.
d) Enter the user ID field, such as uid.
e) Submit your changes.

Step 3 Go to **Network > SMTP Authentication** to configure a Certificate SMTP authentication profile.
a) Enter the profile name.
b) Select the certificate LDAP query you want to use.
c) Do not select the option to allow the **`SMTP AUTH`** command if a client certificate is not available.
d) Submit your changes.

Step 4 Go to **Network > Listeners** to configure a listener to use the certificate SMTP authentication profile that you created.

Step 5 Modify the RELAYED mail flow policy to require TLS and a client certificate, as well as require SMTP authentication.

Note
Although SMTP authentication is required, the email gateway will not use the SMTP AUTH command because it is using certificate authentication. The email gatewaywill require a client certificate from the mail application to authenticate the user.

Step 6 Submit and commit your changes.

Authenticating a User's SMTP Session with the SMTP AUTH Command

The email gateway can use the SMTP AUTH command to authenticate a user's SMTP session instead of a client certificate. If you user is not allowed to use SMTP AUTH for their connection, you can select whether the email gateway rejects the connection or temporarily allows it while logging all activity.

Procedure

Step 1 Go to **System Administration > LDAP** to configure an LDAP server profile.

Step 2 Define an SMTP authentication query for the LDAP profile.
a) Enter the query name.
b) Enter the query string. For example, `(uid={u})`.
c) Select LDAP Bind for the authentication method.
d) Enter an allowance query string. For example,
`(&(uid={u})(|(!(caccn=*))(cacexempt=*)(cacemergency>={t})))`.
e) Submit your changes.

Step 3 Go to **Network > SMTP Authentication** to configure an LDAP SMTP authentication profile.
a) Enter the profile name.
b) Select the SMTP authentication LDAP query you want to use.
c) Select the Check with LDAP if user is allowed to use SMTP AUTH Command and choose to monitor and report the user's activity.
d) Submit your changes.

Step 4 Go to **Network** > **Listeners** to configure a listener to use the LDAP SMTP authentication profile that you created.

Step 5 Modify the RELAYED mail flow policy to require TLS and SMTP authentication.

Step 6 Submit and commit your changes.

Authenticating a User's SMTP Session with Either a Client Certificate or SMTP AUTH

This configuration requires the email gateway to ask for a client certificate from users with a client certificate while allowing SMTP AUTH for users without one, or who cannot use one for sending email.

Any attempt to use the SMTP AUTH command by a user who is not allowed will be prohibited.

Procedure

Step 1 Go to **System Administration** > **LDAP** to configure an LDAP server profile.

Step 2 Define an SMTP authentication query for the profile.

a) Enter the query name.
b) Enter the query string. For example, `(uid={u})`.
c) Select LDAP Bind for the authentication method.
d) Enter an allowance query string. For example, `(&(uid={u})(|(!(caccn=*))(cacexempt=*)(cacemergency>={t})))`.

Step 3 Define a certificate query for the LDAP profile.

a) Enter the query name.
b) Choose the client certificate fields to authenticate, such as the serial number and common name.
c) Enter the query string. For example, `(&(caccn={cn})(cacserial={sn}))`.
d) Enter the user ID field, such as uid .
e) Submit your changes.

Step 4 Go to **Network** > **SMTP Authentication** to configure an LDAP SMTP authentication profile.

a) Enter the profile name.
b) Select the SMTP authentication LDAP query you want to use.
c) Select the Check with LDAP if user is allowed to use SMTP AUTH Command and choose to reject the connection.
d) Enter a custom SMTP AUTH response. For example, 525, "Dear user, please use your CAC to send email."
e) Submit your changes.

Step 5 Configure a Certificate SMTP authentication profile.

a) Enter the profile name.
b) Select the certificate LDAP query you want to use.
c) Select the option to allow the SMTP AUTH command if a client certificate is not available.
d) Select your LDAP SMTP authentication profile for the email gateway to use if the user does not have a client certificate.

e) Submit your changes.

Step 6 Go to **Network > Listeners** to configure a listener to use the certificate SMTP authentication profile you created.

Step 7 Modify the RELAYED mail flow policy to select the following options:

- TLS Preferred
- SMTP authentication required
- Require TLS for SMTP Authentication

Step 8 Submit and commit your changes.