Application Note

Configuring Department of Defense Common Access Card Authentication on McAfee® Firewall Enterprise

McAfee® Firewall Enterprise

version 7.x and 8.x

This application note describes how to configure Department of Defense Common Access Card authentication for Admin Console, Telnet, and SSH on McAfee® Firewall Enterprise version 7.x and 8.x. It also describes logon procedures.

In this document ...

Overview

Common Access Card (CAC) authentication allows you to log on to McAfee® Secure Firewall or McAfee® Firewall Enterprise (hereinafter Firewall Enterprise) using a U.S. Department of Defense Common Access Card. Users can log on to a firewall through the Admin Console, Telnet, or SSH by generating a one-time password on a secure webpage and typing that password into the appropriate logon field.

CAC authentication is available on:

- Secure Firewall version 7.0.1.01.E12
- Firewall Enterprise version 7.0.1.02
- Firewall Enterprise version 7.0.1.03
- Firewall Enterprise version 8.x

This application note describes how to configure CAC authentication for firewall users and how to log on to a firewall using CAC authentication.

Configure authentication

To configure CAC authentication, perform the following tasks:

- *Procedure 1 — Create the CAC authenticator*
- *Procedure 2 — Create rules that will use CAC authentication*
- *Procedure 3 — Export CAC credentials*
- *Procedure 4 — Configure system administrators for CAC authentication*
- *Procedure 5 — Import the firewall's CAC certificate into the browser's trusted store*

For additional configuration information, refer to the Administration Guide for your version.

Procedure 1 — Create the CAC authenticator

Create the CAC authenticator using the procedure specific to your version:

- *Create the CAC authenticator — version 7.0.1.01.E12*
- *Create the CAC authenticator — version 7.0.1.02 and 8.x*
- *Create the CAC authenticator — version 7.0.1.03*

Create the CAC authenticator — version 7.0.1.01.E12

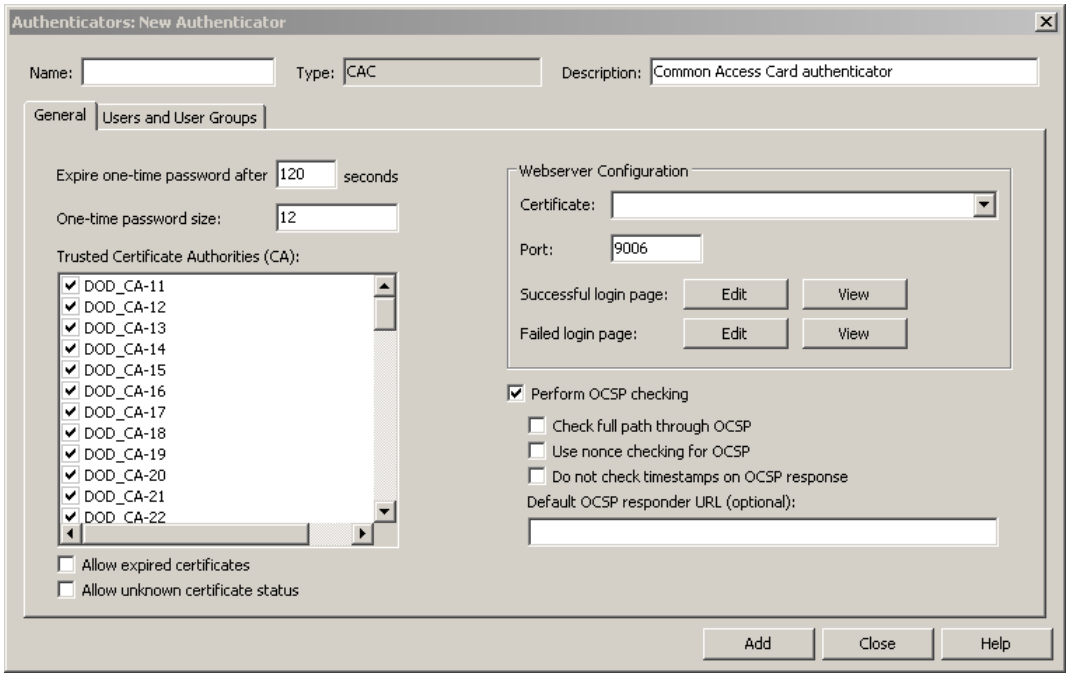
If you are using version 7.0.1.01.E12, use this procedure to create a new CAC authenticator.

Note: Only one CAC authenticator can exist on the firewall.

1 Select **Policy | Rule Elements | Authenticators**. The Authenticators window appears.

2 Click **New**, then select **CAC**. The New Authenticator window appears.

Figure 1 New Authenticator window



3 Type a name for the CAC authenticator.

4 Configure the password settings.

- **Expire one-time password after** — Type the length of time in seconds that the password on the webpage is valid.
- **One-time password size** — Type the number of characters in the password.

5 Configure the Webserver Configuration settings.

a From the **Certificate** drop-down list, select the certificate that the firewall will use to identify itself.

You can select a self-signed certificate or an imported Certificate Authority certificate. See the *Certificate/Key Management* chapter of the Administration Guide for details.

If you select a self-signed certificate, you must perform a one-time procedure to import the certificate into your web browser's trusted store. See *Procedure 5 — Import the firewall's CAC certificate into the browser's trusted store* for details.

The certificate you select should be suitable as an HTTPS server certificate as specified in RFC 2818 (HTTP for use over TLS): either the certificate's CommonName (CN) field should match the host name from the server's URI, or it should include a fully qualified domain name as a SubjectAltName extension to the certificate.

If IP addresses will be used to access the cac server, the certificate should include an IP address as a SubjectAltName extension. For example, if you select CAC authentication for a rule with the internal burb as the source, the URL used to access the server would look like one of these:

- https://*internal domain name for firewall*:9006
- https://*internal IP address for firewall*:9006

If you don't select an appropriate certificate for HTTPS traffic, your web clients connecting to the cac server might deny the connection or issue a Certificate Error.

Note: If the host name identified in the CommonName of the Default_SSL_Cert matches the host name used to connect to the cac server, you can select the Default_SSL_Cert for the CAC authenticator.

b In the **Port** field, type the port that the server listens on. Port 9006 is the default.

c [Optional] You can change the Successful login and Failed login webpages to meet your site's requirements.

- **Successful login page** — Click **Edit** to modify the message displayed for successfully logging on. Click **View** to see the webpage.
- **Failed login page** — Click **Edit** to modify the message displayed for a failed logon. Click **View** to see the webpage.

6 Configure the CA certificate settings.

The Trusted Certificate Authorities (CA) pane displays all of the certificates that have been configured in the Certificate Authorities window (Maintenance | Certificate/Key Management). These certificates include:

- Root (self-signed) certificates
- Intermediate certificates (untrusted, but available for use in certificate validation)

These certificates are used to validate the following:

- Certificate presented by the user in CAC authentication
- Response from an OCSP responder

Note: These responses may be validated by the same CA certificates as end user certificates, or they may be different. For example, OCSP responses may be signed by a self-signed certificate that is not part of the U.S. Department of Defense certificate hierarchy. In this case, the certificate must be imported as a CA certificate and enabled in the New Authenticator window.

Tip: The certificates needed to validate a CAC certificate are preloaded and enabled for your use.

You can configure these CA certificate options:

- **Add a new CA certificate** — [Optional] If you need to add a new certificate:
  - Select **Maintenance | Certificate/Key Management**. The Certificate/Key Management window appears.
  - Select the **Certificate Authorities** tab, then create the new certificate.
  - Enable this certificate as a trusted certificate by returning to the New Authenticator window, Trusted Certificate Authorities (CA) pane, and selecting the checkbox for the certificate.
- **Allow expired certificates** — [Conditional] If you have an expired certificate that you must continue using, select this checkbox.

  Tip: Select this option only when you need to work around an issue with an expired CA certificate.
- **Allow unknown certificate status** — [Conditional] If you want to allow a certificate to be used when the configured OCSP server is unavailable or does not know about the certificate, select this checkbox.

  Tip: Use this option to allow some leniency with OCSP checking (for example, when you need to work around an issue with an unavailable OCSP server).

7 [Optional] If you want to enable certificate status checking by means of an OCSP server, follow these steps.

To help you determine your configuration, consider how the firewall determines the OCSP responder URL.

- First, the firewall looks for the responder URL that is configured on the CA entry of the issuing CA (Certificate/Key Management window, Certificate Authorities tab).
- If there is no responder URL, the firewall looks next at the responder URL configured in the Authority Information Access extension of the certificate.
- If there is no responder URL, the firewall accepts the global, default responder URL for CAC authentication (New Authenticator window).

a Select the **Perform OCSP checking** checkbox.

b Configure the following:

- **Check full path through OCSP** — If you want the firewall to perform OCSP status checking on all certificates in the chain below the root certificate, select this checkbox.

  When this option is deselected, the firewall performs OCSP checking only on the end user certificate.
- **Use nonce checking for OCSP** — If you want the firewall to use nonce (random value) to make sure the response is fresh, select this checkbox. The firewall sends a nonce on the OCSP request and checks the nonce in the response.

  Note: Nonce checking can slow down certificate status checking because the responder cannot return a pre-generated response.
- **Do not check timestamps on OCSP response** — The firewall requires that the OCSP response is no more than one week old. If you want to use an OCSP responder that generates responses less frequently, select this checkbox.

  Tip: Use this option if you want to override timestamp checking.

- **Default OCSP responder URL** — If you want to configure a global default OCSP responder address for use when there is no URL configured on the CA entry or in the Authority Information Access field of the certificate being checked, type the responder URL.

  Note: This is not an override URL. If the firewall finds the URL in the CA entry or the certificate, it uses that responder URL.

  If you want to configure a CA-specific OCSP responder URL that overrides any responder URL found in the certificate being checked:

  - Select **Maintenance | Certificate/Key Management**.
  - Click the **Certificate Authorities** tab.
  - In the **OCSP Responder URL** field, type the URL.

  This field allows you to override the AIA certificate extension or the CA official responder with a private responder. There is no default for this field.

8 Click **Add**.

9 Save your changes.

Create the CAC authenticator — version 7.0.1.02 and 8.x

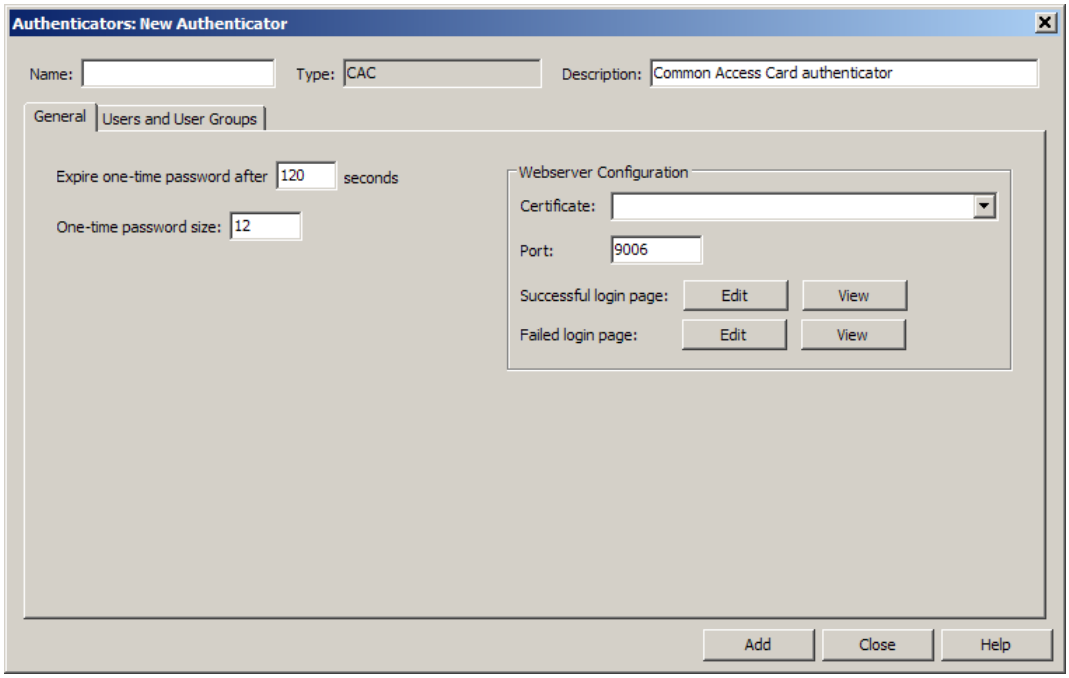
If you are using version 7.0.1.02 or 8.x, use this procedure to create a new CAC authenticator.

Note: Only one CAC authenticator can exist on the firewall.

1 Select **Policy | Rule Elements | Authenticators**. The Authenticators window appears.

2 Click **New**, then select **CAC**. The New Authenticator window appears.

Figure 2 New Authenticator window



Note: In 8.x, the Users and User Groups tab is unavailable on the New Authenticator window.

3 Type a name for the CAC authenticator.

4 Configure the password settings.

- **Expire one-time password after** — Type the length of time in seconds that the password on the webpage is valid.
- **One-time password size** — Type the number of characters in the password.

5 Configure the Webserver Configuration settings.

a From the **Certificate** drop-down list, select the certificate that the firewall will use to identify itself.

You can select a self-signed certificate or an imported Certificate Authority certificate. See the *Certificate/Key Management* chapter of the administration guide for details.

If you select a self-signed certificate, you must perform a one-time procedure to import the certificate into your web browser's trusted store. See *Procedure 5 — Import the firewall's CAC certificate into the browser's trusted store* for details.

The certificate you select should be suitable as an HTTPS server certificate as specified in RFC 2818 (HTTP for use over TLS): either the certificate's CommonName (CN) field should match the host name from the server's URI, or it should include a fully qualified domain name as a SubjectAltName extension to the certificate.

If IP addresses will be used to access the cac server, the certificate should include an IP address as a SubjectAltName extension. For example, if you select CAC authentication for a rule with the internal burb as the source, the URL used to access the server would look like one of these:

- https://*internal domain name for firewall*:9006
- https://*internal IP address for firewall*:9006

If you don't select an appropriate certificate for HTTPS traffic, your web clients connecting to the cac server might deny the connection or issue a Certificate Error.

Note: If the host name identified in the CommonName of the Default_SSL_Cert matches the host name used to connect to the cac server, you can select the Default_SSL_Cert for the CAC authenticator.

b In the **Port** field, type the port that the server listens on. Port 9006 is the default.

c [Optional] You can change the Successful login and Failed login webpages to meet your site's requirements.

- **Successful login page** — Click **Edit** to modify the message displayed for successfully logging on. Click **View** to see the webpage.
- **Failed login page** — Click **Edit** to modify the message displayed for a failed logon. Click **View** to see the webpage.

6 Click **OK**.

7 Save your changes.

Create the CAC authenticator — version 7.0.1.03

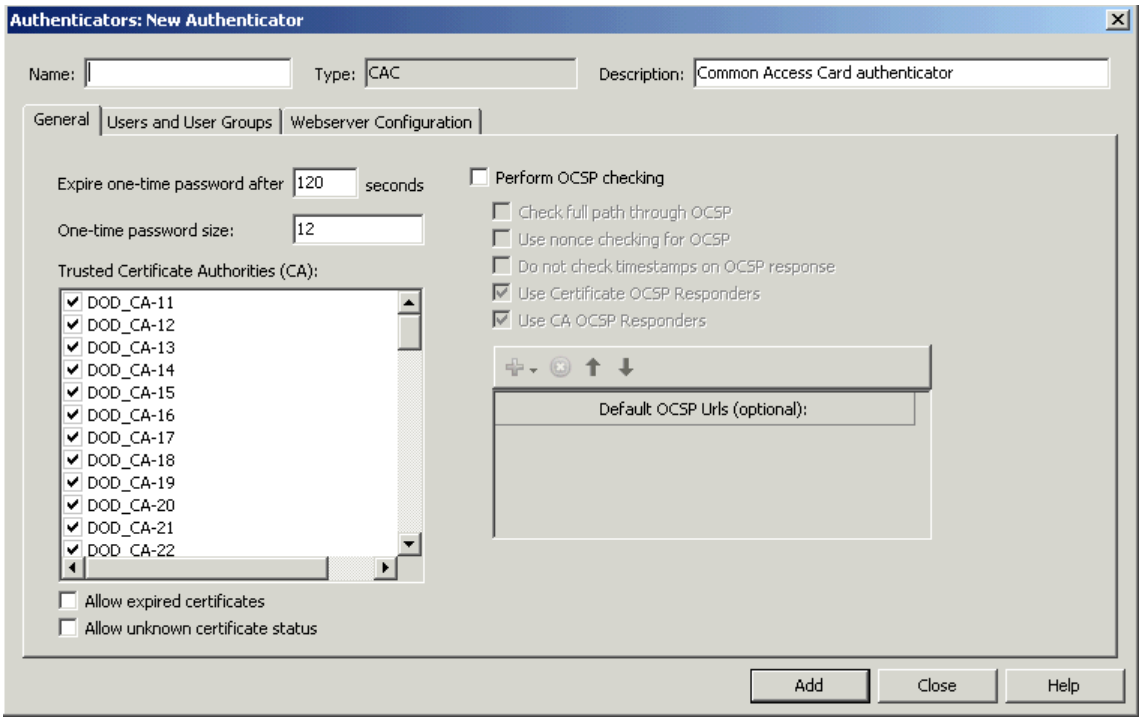
If you are using version 7.0.1.03, use this procedure to create a new CAC authenticator.

Note: Only one CAC authenticator can exist on the firewall.

1 Select **Policy | Rule Elements | Authenticators**. The Authenticators window appears.

2 Click **New**, then select **CAC**. The New Authenticator window appears.

Figure 3 New Authenticator window



3 Type a name for the CAC authenticator.

4 Configure the password settings.

- **Expire one-time password after** — Type the length of time in seconds that the password on the webpage is valid.
- **One-time password size** — Type the number of characters in the password.

5 Configure the CA certificate settings.

- **Trusted Certificate Authorities (CA)** — The list displays the list of all the certificates that have been configured in the Certificate Authorities window. Deselect a CA if you do not want the certificates signed by that CA for CAC authentication.
- **Allow expired certificates** — Select this checkbox if you want to ignore certificate expiration while validating certificates.
- **Allow unknown certificate status** — If the certificate revocation status cannot be determined using OCSP, select this checkbox to allow certificate validation to succeed.

- **Perform OCSP checking** — Select this checkbox if you want to enable certificate status checking by means of an OCSP server. Configure the following:

  To help you determine your configuration, consider how the firewall determines the OCSP responder URL.
  - A list of responder URLs is consolidated using the URLs from the following:
    - Certificate (Authority Information Access extension of the certificate)
    - CA entry of the issuing CA (Certificate/Key Management window, Certificate Authorities tab)
    - Global or default responder URLs for CAC authentication (New Authenticator window)

    Note: Each of these can supply multiple URLs to the list.
  - The list is then traversed until an OCSP responder responds with a definitive yes or no. If there is no responder URL, the firewall accepts the global, default responder URL for CAC authentication.

    Note: Deselect the **Use Certificate OCSP Responders** and **Use CA OCSP Responders** checkboxes if you want to disable the certificate and CA URL entries.

  - **Check full path through OCSP —** Select this checkbox if you want the firewall to perform OCSP status checking on all certificates in the chain below the root certificate.
  - **Use nonce checking for OCSP —** Select this checkbox if you want the firewall to use a nonce (random value) to make sure the response is fresh.
  - **Do not check timestamps on OCSP response —** Select this checkbox if you want to use an OCSP responder that generates responses less frequently than once a week.
  - **Use Certificate OCSP Responders —** Select this checkbox to use OCSP responder URLs that are embedded in certificates.

    When you select Perform OCSP checking, this checkbox is selected by default.
  - **Use CA OCSP Responders —** Select this checkbox to use OCSP responder URLs that are configured in CA entries.

    When you select Perform OCSP checking, this checkbox is selected by default.
  - **Default OCSP Urls —** Add, delete, and order a list of OCSP responder URLs that will be consulted if the URLs found in the certificate or on the CA entry do not respond.

6 Configure the Webserver Configuration settings.

  a Click the **Webserver configuration** tab.

  b From the **Certificate** drop-down list, select the certificate that the firewall will use to identify itself.

  You can select a self-signed certificate or an imported Certificate Authority certificate. See the *Certificate/Key Management* chapter of the Administration Guide for details.

  If you select a self-signed certificate, you must perform a one-time procedure to import the certificate into your web browser's trusted store. See *Procedure 5 — Import the firewall's CAC certificate into the browser's trusted store* for details.

  The certificate you select should be suitable as an HTTPS server certificate as specified in RFC 2818 (HTTP for use over TLS): either the certificate's CommonName (CN) field should match the host name from the server's URI, or it should include a fully qualified domain name as a SubjectAltName extension to the certificate.

  If IP addresses will be used to access the cac server, the certificate should include an IP address as a SubjectAltName extension. For example, if you select CAC authentication for a rule with the internal burb as the source, the URL used to access the server would look like one of these:

- https://*internal domain name for firewall*:9006
- https://*internal IP address for firewall*:9006

If you don't select an appropriate certificate for HTTPS traffic, your web clients connecting to the cac server might deny the connection or issue a Certificate Error.

Note: If the host name identified in the CommonName of the Default_SSL_Cert matches the host name used to connect to the cac server, you can select the Default_SSL_Cert for the CAC authenticator.

c In the **Port** field, type the port that the server listens on. Port 9006 is the default.

d [Optional] You can change the Successful login and Failed login webpages to meet your site's requirements.

- **Successful login page** — Click **Edit** to modify the message displayed for successfully logging on. Click **View** to see the webpage.
- **Failed login page** — Click **Edit** to modify the message displayed for a failed logon. Click **View** to see the webpage.

7 Click **OK**.

8 Save your changes.

Procedure 2 — Create rules that will use CAC authentication

Create the rules that will use CAC authentication using the procedure specific to your version:

- *Create rules that will use the CAC authentication — version 7.0.1.01.E12, 7.0.1.02, and 7.0.1.03*
- *Create rules that will use the CAC authentication — version 8.x*

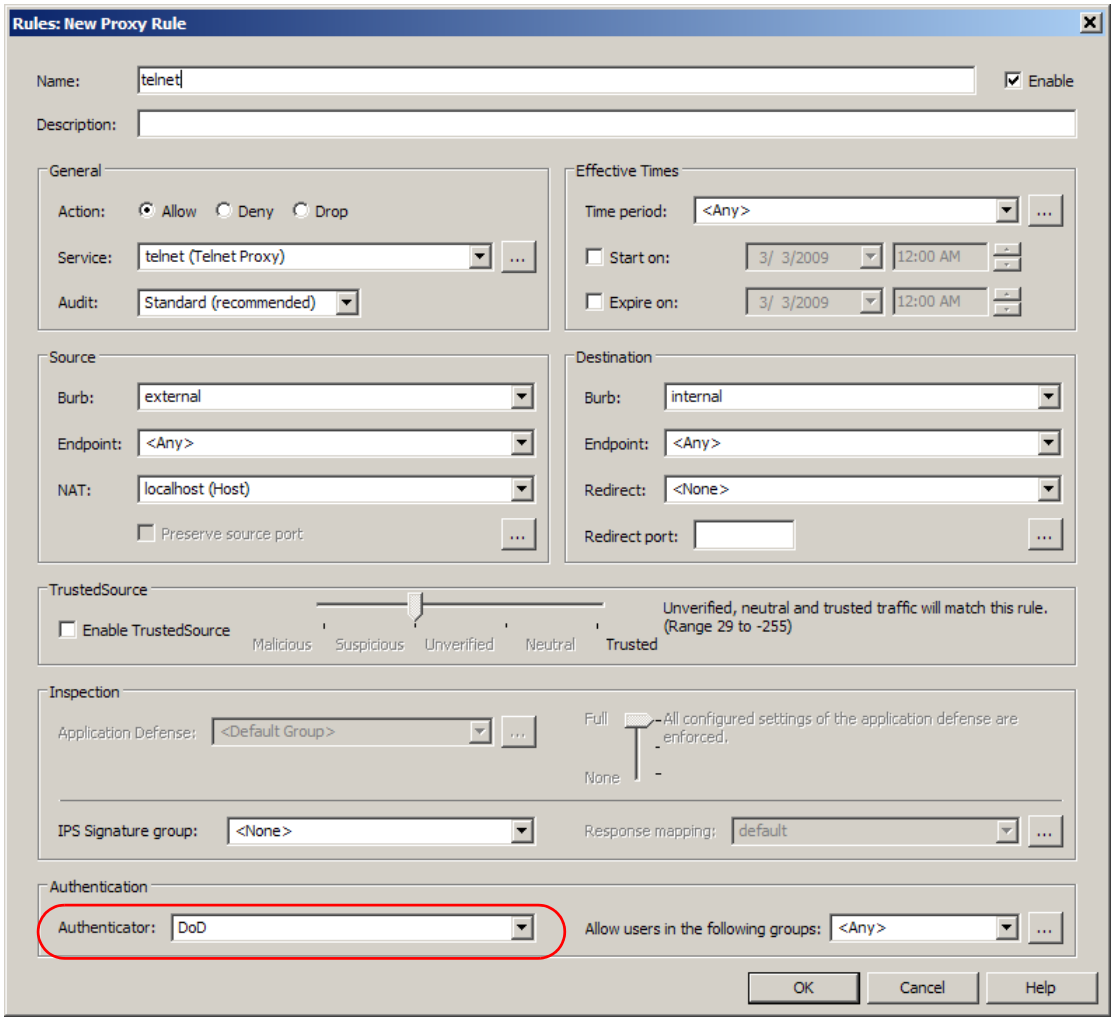
Create rules that will use the CAC authentication — version 7.0.1.01.E12, 7.0.1.02, and 7.0.1.03

If you are using version 7.0.1.01.E12, 7.0.1.02, or 7.0.1.03, use this procedure to create a new rule.

1 Select **Policy | Rules**. The Rules window appears.

2 Click **New Rule** to create a rule that will use CAC authentication, or select an existing rule and click **Modify**. The New Rule window appears.

Figure 4 New Rule window



3 Configure the rule as necessary to enforce your security policy.

4 From the **Authenticator** drop-down list, select the CAC authenticator.

5 Click **OK** and save your changes.

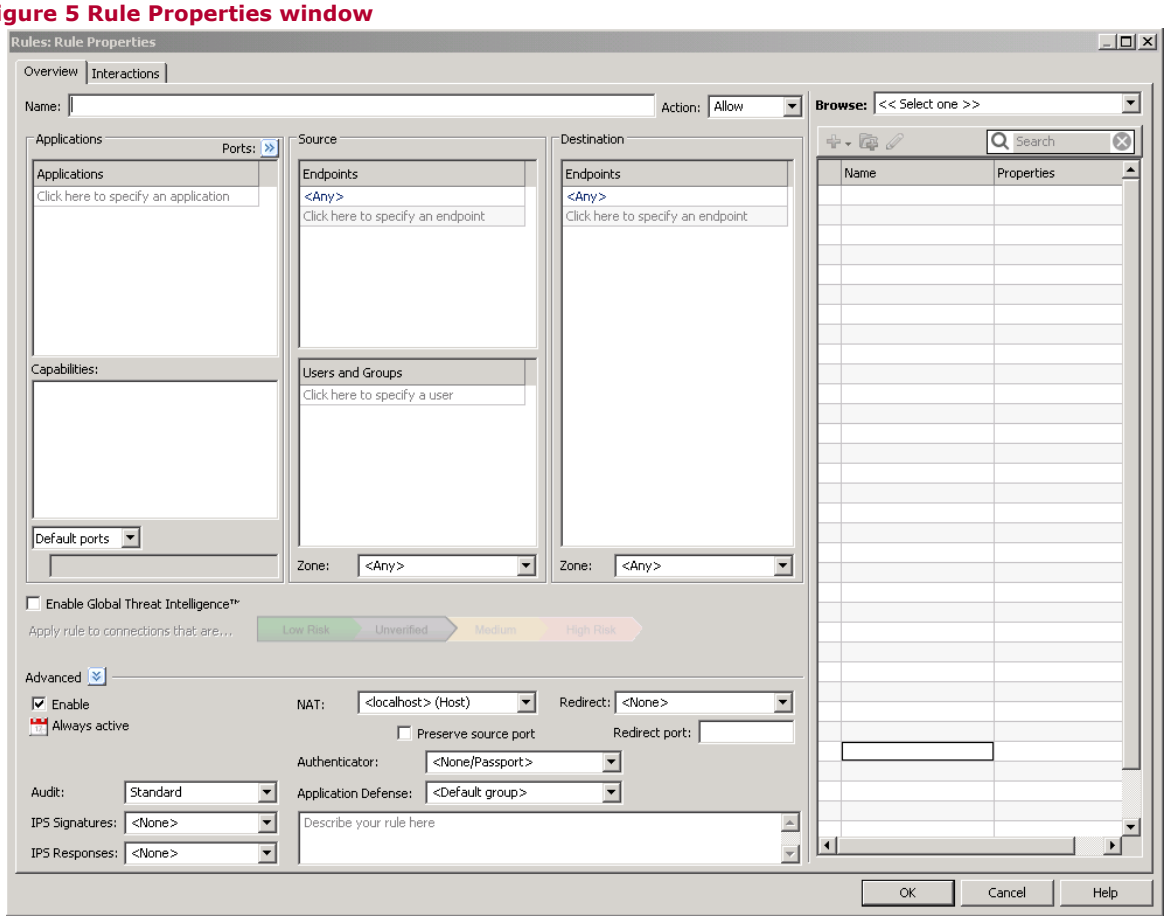
Create rules that will use the CAC authentication — version 8.x

If you are using version 8.x, use this procedure to create a new rule.

1 Select **Policy | Access Control Rules**. The Access Control Rules window appears.

2 Click **New Rule** to create a rule that will use CAC authentication, or select an existing rule and click **Modify**. The Rule Properties window appears.

Figure 5 Rule Properties window



3 Configure the rule as necessary to enforce your security policy.

4 From the **Authenticator** drop-down list, select the CAC authenticator.

5 Click **OK** and save your changes.

Procedure 3 — Export CAC credentials

Each administrator account using CAC authentication must have a CAC public certificate registered to that account. You do this by exporting CAC certificates from the Common Access Card.

This procedure shows how to export a CAC certificate using ActivCard CAC utility software and Microsoft Internet Explorer 7. If you use different CAC utility software or a different browser, the steps might vary.

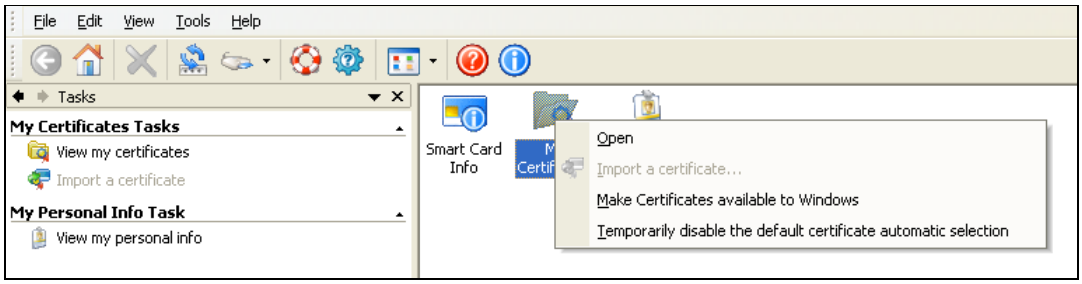
Perform this procedure for each administrator using CAC authentication.

To export CAC credentials:

1 Start ActivCard Utilities, insert your CAC, and type your PIN when requested to log on to the CAC.

2 Right-click **My Certificates** and select **Make Certificates available to Windows** from the pop-up menu.

Figure 6 ActivCard Utilities home window

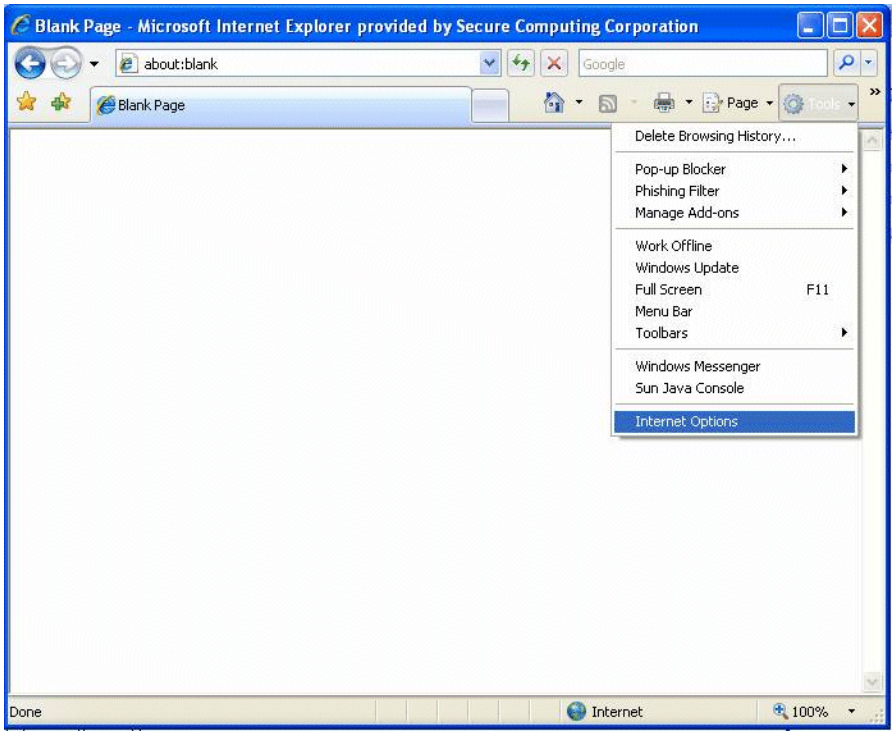


3 Follow the on-screen instructions to make certificates available. This allows other applications to access the certificates stored on the CAC.

4 Start an Internet Explorer browser.

5 From the **Tools** drop-down list, select **Internet Options**. The Internet Options window appears.

Figure 7 Internet Explorer: Tools menu

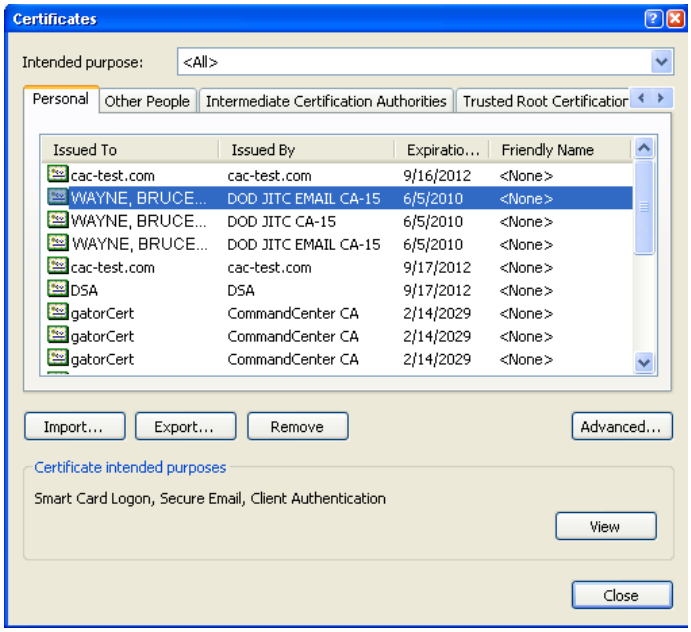


6 Click the **Content** tab.

7 Click **Certificates**. The Certificates window appears.

8 On the Personal tab, select the certificate you want to export.

Figure 8 Certificates window: Personal tab



9 Click **Export**. The Certificate Export Wizard welcome window appears.

10 Follow the on-screen instructions to export the certificate to a file.

- The file format can be DER-encoded binary X.509, Base-64 encoded X.509, or PKCS #7.
- Save the file in a location accessible to the Admin Console, or save the file and transfer it to the computer running the Admin Console.

Procedure 4 — Configure system administrators for CAC authentication

Perform this procedure to associate the exported CAC certificate with a system administrator. This certificate is used to identify the administrator to the firewall.

1 Import the certificate you exported from the CAC.

For information on importing remote certificates, see the *Certificate/Key Management* chapter of the Administration Guide.

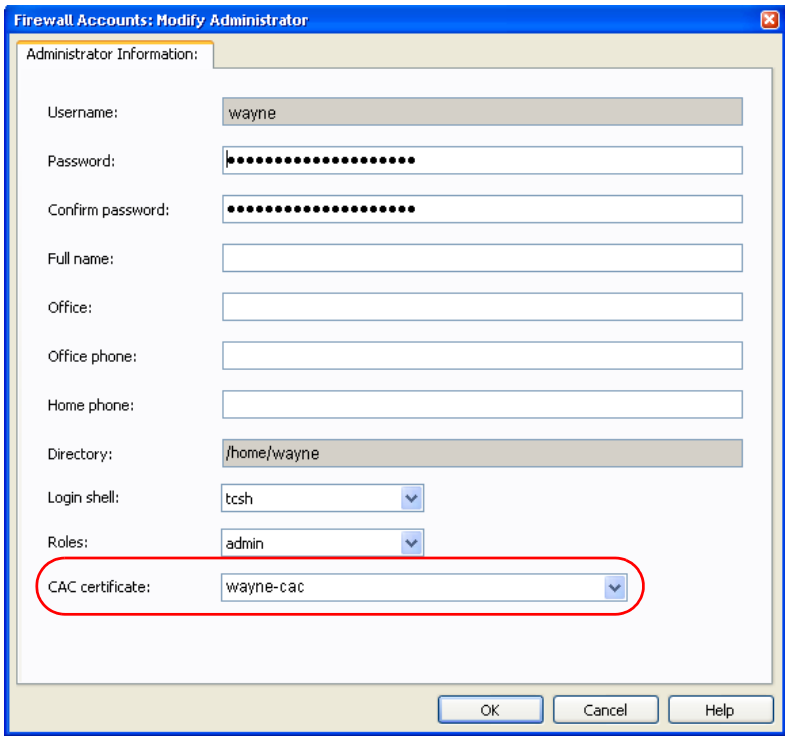
2 Select **Maintenance | Administrator Accounts**. The Administrator Accounts window appears.

3 Select the desired administrator and click **Modify**.

4 From the **CAC certificate** drop-down list, select the remote certificate imported for the administrator.

Note: To disable CAC authentication for a user, select ***None***.

Figure 9 Firewall Accounts: Modify Administrator window



5 Click **OK** and save your changes.

Procedure 5 — Import the firewall's CAC certificate into the browser's trusted store

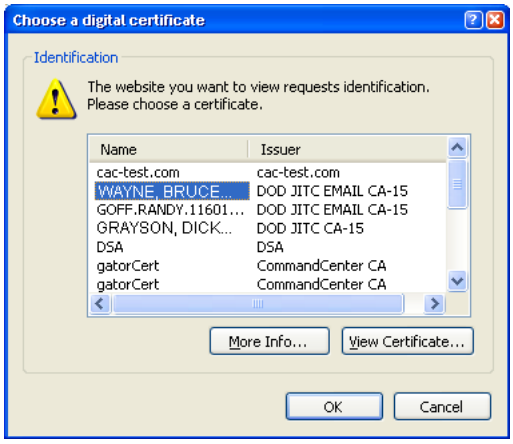
[Conditional] If you created a self-signed certificate for the firewall's CAC server, a message will warn that the server certificate is not trusted the first time you connect to the CAC server. Perform this procedure to import the firewall's CAC server certificate into the browser's trusted store. Performing this procedure will eliminate further certificate warnings.

1 Start the CAC utility software, insert your CAC, and type your PIN when requested to log on to the CAC.

2 Open a browser and go to https://*firewall address or FQDN*:9006. (9006 is the port default; if you configured a different port for the CAC authenticator, type that port number.)

The Choose a digital certificate window appears.

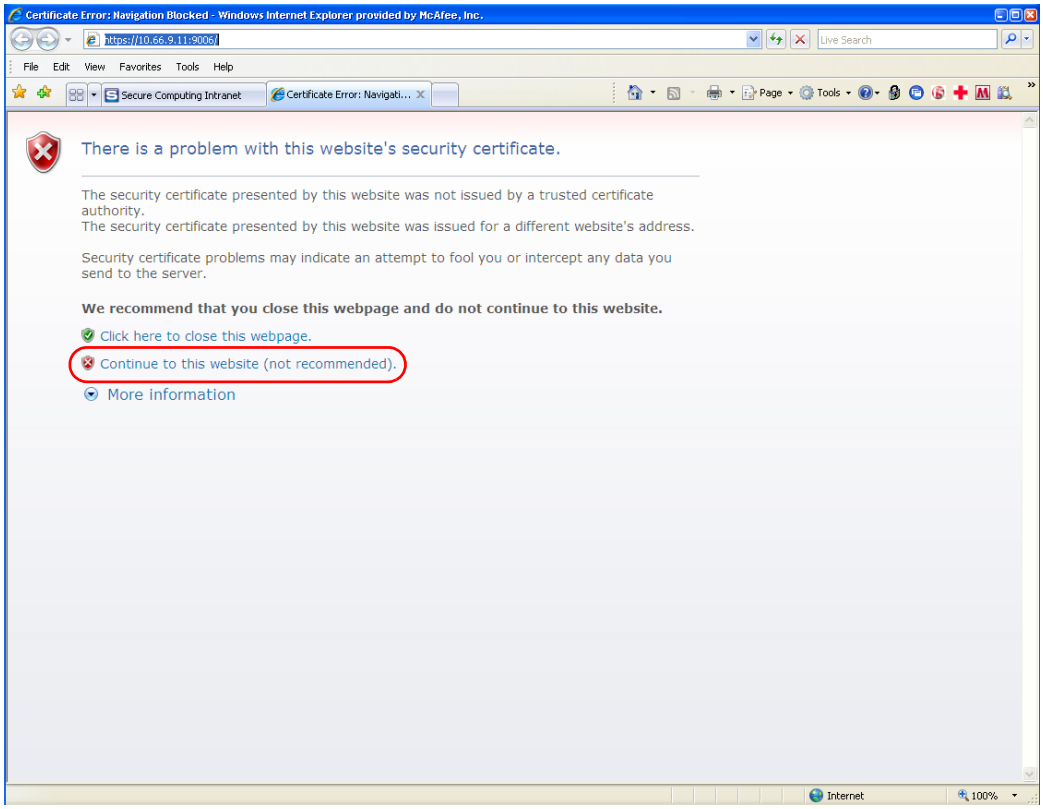
Figure 10 Choose a digital certificate window



3 Select the appropriate certificate and click **OK**. A Certificate Error webpage appears.

4 Click **Continue to this website (not recommended)**. The Successful Login webpage appears.

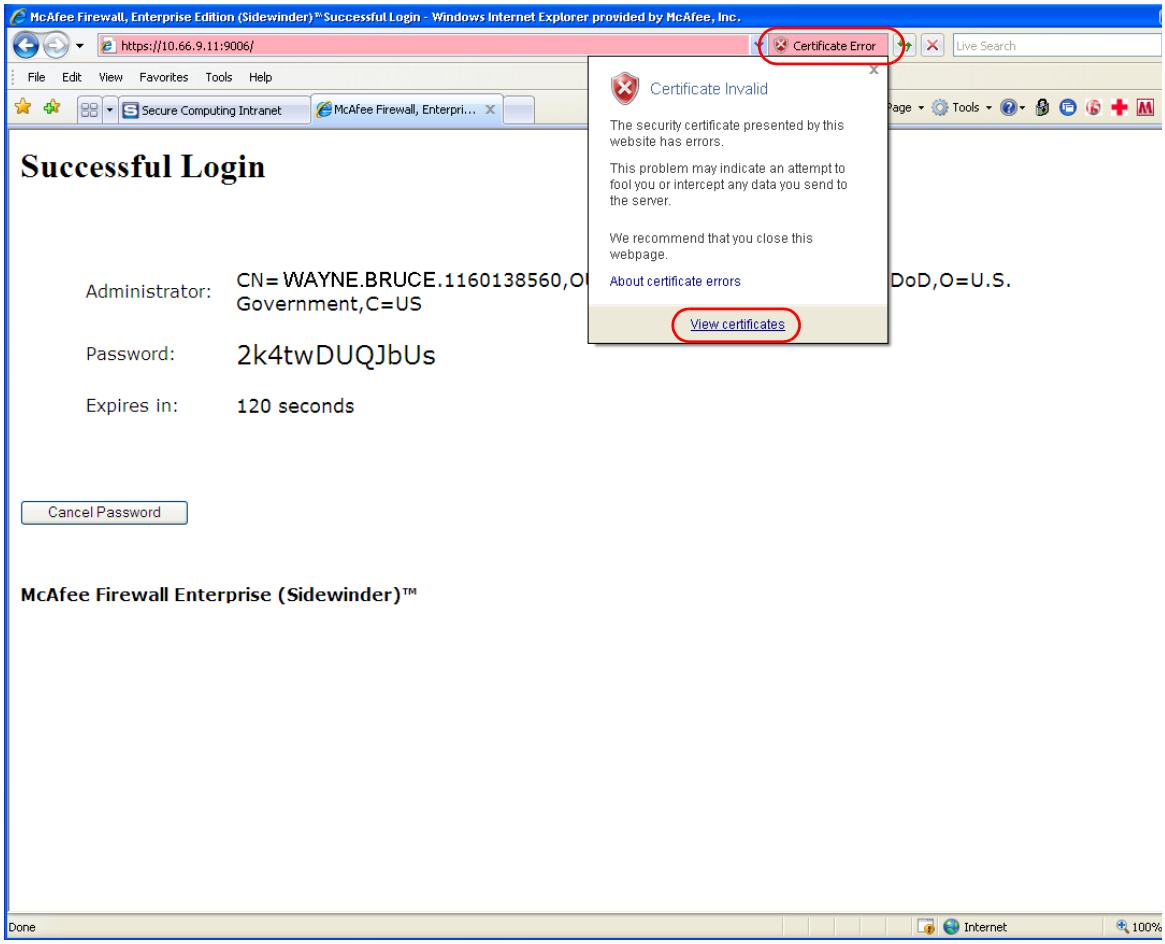
Figure 11 Certificate Error webpage



5 Next to the URL field, click **Certificate Error**. The Untrusted Certificate pop-up window appears.

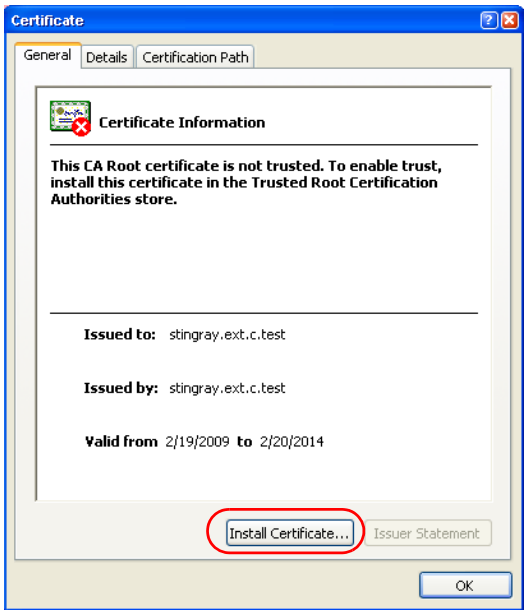
6 Click **View Certificates**. The Certificates window appears.

Figure 12 Successful Login webpage with Untrusted Certificate pop-up



7 Click **Install Certificate**. The Import Wizard welcome window appears.

Figure 13 Certificate window



8 Follow the on-screen instructions to import the certificate.

9 Close the browser.

CAC authentication configuration is complete. To log on to the firewall, follow the instructions in *Log on using Common Access Card authentication*.

Log on using Common Access Card authentication

To log on to the firewall:

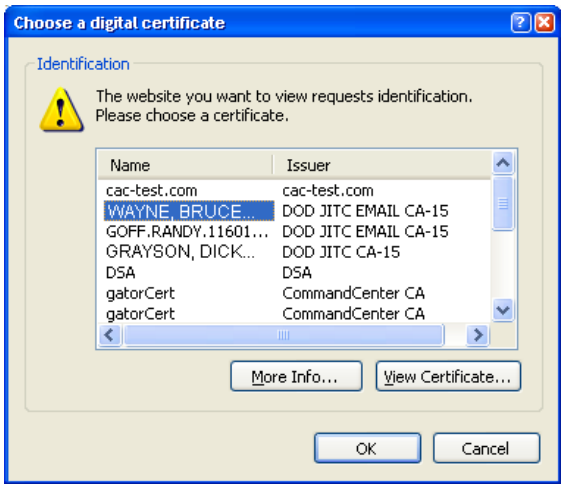
1 Start the CAC utility software, insert your CAC, and type your PIN when requested to log on to the CAC.

2 Open a browser and go to https://*firewall address or FQDN*:9006. (9006 is the port default; if you configured a different port for the CAC authenticator, type that port number.)

The Choose a digital certificate window appears.

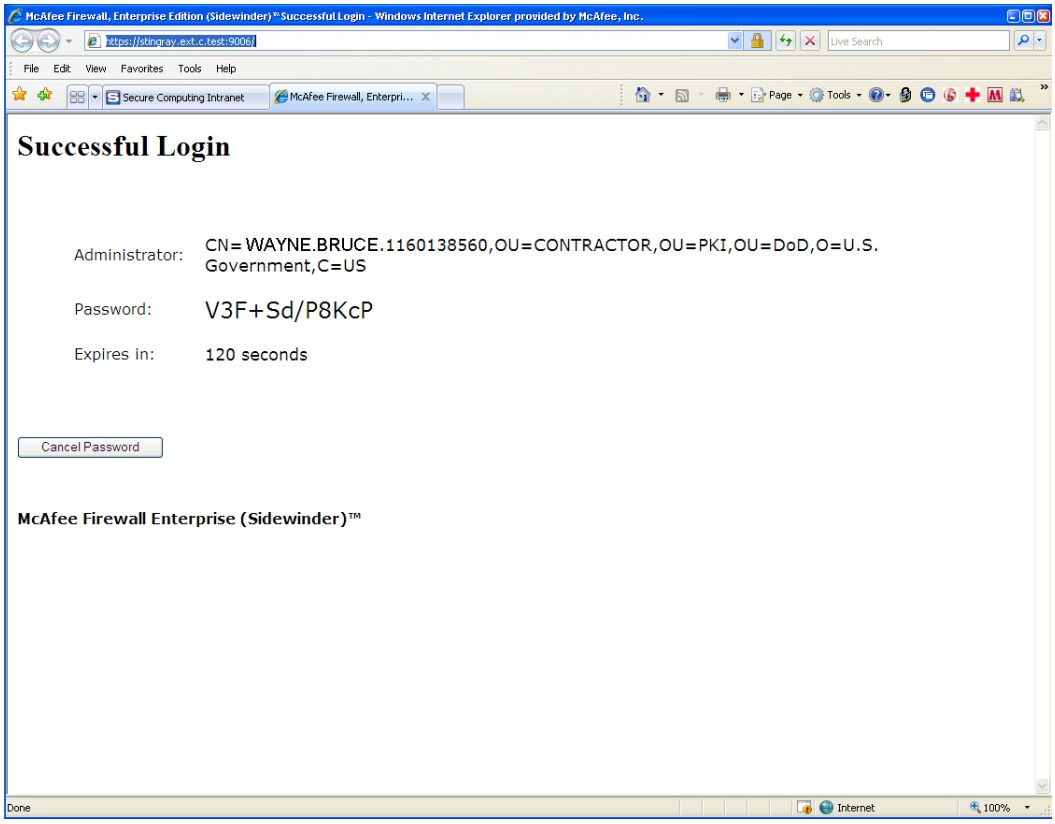
- If you have already connected to the CAC web service during the same browser session, the browser has cached the certificate and this window will not appear.
- If the browser has cached the certificate and you want to select a different certificate, you must close the browser and start another browser session.

Figure 14 Choose a digital certificate window



3 Select the appropriate certificate and click **OK**.The Successful Login webpage appears.

Figure 15 Successful Login webpage



If a Login Failure page appears, verify that you are using the same CAC certificate registered with your administration account:

a Restart the browser and go to https://*firewall address or FQDN*:9006. On the Choose a digital certificate window, click **View Certificate** and note the issuer distinguished name and serial number of the certificate.

b On the firewall:

- Select **Maintenance | Certificate/Key Management**. The Remote Certificates window appears.
- Select the CAC certificate you imported to the firewall.
- Click **Export**. The Certificate Export window appears.
- Select **Export Certificate to screen**, then click **OK**. The Certificate Data window appears.
- Verify that the distinguished name and serial number match.

If the certificates do not match, you must export the CAC certificate from your CAC card again, or select a matching certificate on the Choose a digital certificate window.

4 Remember or write down the password.

- If the browser is on the same computer as the Admin Console, you can copy and paste the password.
- If you will not use the password and want to terminate it before the configured expiration time, click **Cancel**.

5 Complete the appropriate logon procedure:

Admin Console

a Start the Admin Console and click **Connect**. The Login window appears.

b Type your user name.

c From the **Authenticator** drop-down list, select the CAC authenticator created by the administrator.

d Click **OK**. The Common Access Card Authentication window appears.

e Type or copy the password into the password field, then click **Enter**. The Dashboard appears.

Telnet

a Start the Telnet client.

b Complete the logon dialog and connect.

- [Conditional] If CAC authentication is not the default authentication method, append `:-cac` to the user name.
- Type or copy the password into the **Password** field.

SSH

a Start the SSH client.

b Complete the logon dialog and connect.

- [Conditional] If CAC authentication is not the default authentication method, append `:-cac` to the user name, for example:

  ```
  ssh user:-cac@firewall address
  ```

- Type or copy the password into the Password field.