Access Control Manager™ Virtual

Getting Started Guide

FR
ES
IT
DE

AVIGILON™
a Motorola Solutions Company

1. Obtain the Activation ID

When you purchase a license for your Access Control Manager Virtual appliance, Avigilon generates a unique Activation ID for your license.

The Activation ID is sent to you in:

- A confirmation email
- A package

All your Activation IDs are permanently stored in your FNO account with Avigilon.

## 2. Download the ACM Virtual Files

1. In a web browser connected to the internet, go to the Avigilon Partner Resource Center: **partners.avigilon.com**

2. Log in or register.
   Note: To register, click **Register**, complete the registration form and click **Submit**. A temporary password is emailed to the provided address.

3. In the top menu bar of the Avigilon Partner Resource Center, click **Software**.

4. In the ASSET LIBRARY under Collections, click **Software** > **ACM 6**.

5. Scroll down the list of assets to locate the most recent **ACM 6.x.x Virtual Image**.

6. Click the icon to display the information page for this asset.

7. Click the **Download** button and save the .zip file to a location accessible to your VM instance.

8. Extract the three ACM Virtual files (.ovf, .vmdk and .mf).

9. Install the files according to the VMware® ESX/ESXi system instructions.

Note: The Virtual Machine console in VMware Vsphere is not activated or available for use. Connect to the ACM appliance via the web browser only.
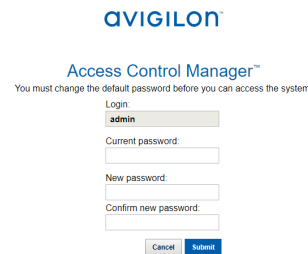
avigilon.com

3. Open Web Browser

Open the web browser on the connected PC and type this IP address: **169.254.1.250**

https://169.254.1.250|
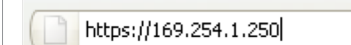
If a message indicates a connection or security error, refer to *Access Control Manager Troubleshooting Browser Issues* overleaf.

4. Log in to the Application

When the login screen appears, enter **admin** in **Login** and the default password in **Password**. Click **Sign in**. You must change the default password as shown:

AVIGILON™

Access Control Manager™
You must change the default password before you can access the system.

Login:
admin

Current password:

New password:

Confirm new password:

Cancel   Submit

The Access Control Manager application main menu appears.

5. Edit Hostname

The default hostname for each appliance is **ACM**. If you need to set a specific hostname for the appliance, do so at this point before the ACM appliance is connected to the network.

1. From the top-right corner, select ⚙ > **Appliance** to display the Appliance: Edit page on the Appliance tab.

2. On the Appliance tab, enter a new **Host Name**.

3. Click the ✓ **Save** button.

The ACM appliance automatically restarts.

6. Accept EULA

After you log in the second time, accept the end user license agreement (EULA).

1. Click the link below **End user license must be accepted. Accept EULA to stay in compliance**.

2. Review the EULA and then select the **I accept the terms of the License Agreement** check box.

3. Click **Submit**.

7. License the Application

Enter the Activation ID provided in the email from Avigilon that is marked "IMPORTANT - DO NOT DISCARD":

1. From the top-right corner, click ⚙ > **Appliance**.

2. Click the **About** tab.

3. Click ➕ Add License to display the Add Licenses dialog.

If the appliance has internet access:

1. Click the **Automatic** tab.

2. Enter the Activation ID.

3. Click Activate Licenses

If the appliance does not have internet access:

1. Click the **Manual** tab.

2. Enter the Activation ID.

3. Click Save File... to generate the activation file.

4. Complete the on-screen instructions to upload the file to Avigilon and receive a valid license file using a computer connected to the internet.

   The activation file name is: **Activation File.key**

   The license file name is: **capabilityResponse.bin**

5. Upload the license file to the ACM system and click Activate Licenses

8. Configure Port Settings

Configure the Ethernet port:

1. From the top-right corner, click ⚙ > **Appliance**.

2. Click the **Ports** tab and then select **Port-1**.

3. Enter the required values: **Name**, **IP Address**, **Netmask** and **Network Gateway**.

AVIGILON | Access Control Manager

Monitor ▾ Identities ▾ Reports ▾ Physical Access ▾ Roles ▾

Port: Edit

Appliance   Access   Ports   Replication   Backups   Lo...

Appliance: TESTTARGET-211
Port: 1
Name: Port-1
Link status: Up
IP Address: 10.40.11.1
Netmask: 255.255.255.0 ▾
Network Gateway: 10.40.11.254
MAC Address: 00:0c:29:82:b1:2f

Save   Cancel Changes

Consult your IT manager for the IP Address, Netmask and Network Gateway values appropriate for your installation.
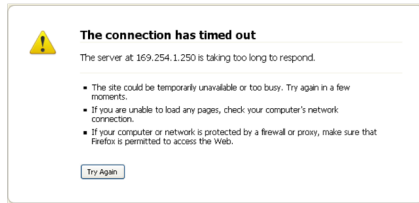
4. Click the ✓ **Save** button.

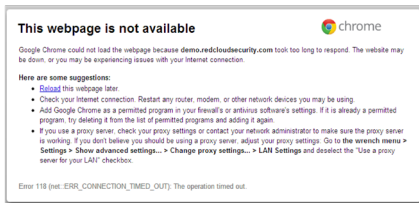The appliance automatically restarts.

Access Control Manager
Troubleshooting Browser Issues

AVIGILON™
a Motorola Solutions Company

If the Access Control Manager application site is not found and one of these messages appears...

When using Firefox:
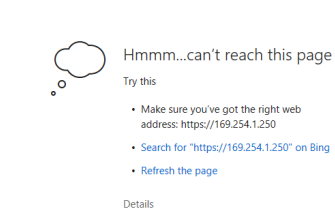
> **The connection has timed out**
>
> The server at 169.254.1.250 is taking too long to respond.
>
> - The site could be temporarily unavailable or too busy. Try again in a few moments.
> - If you are unable to load any pages, check your computer's network connection.
> - If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.
>
> [Try Again]

When using Chrome™:

> **This webpage is not available**   ⊙ chrome
>
> Google Chrome could not load the webpage because demo.redcloudsecurity.com took too long to respond. The website may be down, or you may be experiencing issues with your Internet connection.
>
> Here are some suggestions:
> - Reload this webpage later.
> - Check your Internet connection. Restart any router, modem, or other network devices you may be using.
> - Add Google Chrome as a permitted program in your firewall's or antivirus software's settings. If it is already a permitted program, try deleting it from the list of permitted programs and adding it again.
> - If you use a proxy server, check your proxy settings or contact your network administrator to make sure the proxy server is working. If you don't believe you should be using a proxy server, adjust your proxy settings: Go to the wrench menu > Settings > Show advanced settings... > Change proxy settings... > LAN Settings and deselect the "Use a proxy server for your LAN" checkbox.
>
> Error 118 (net::ERR_CONNECTION_TIMED_OUT): The operation timed out.

When using Internet Explorer:

> **Oops! Internet Explorer could not connect to 169.254.1.250**
> Here are some suggestions:
> - Check the address for typing errors such as ww.example.com instead of www.example.com
> - If you are unable to load any pages, check your computer's internet connection.
> - If your computer or network is protected by a firewall or proxy, make sure that your browser is permitted to access the Web.
>
> OR
>
> Try a Search

When using Safari:

> **Safari can't connect to the server.**
> Safari can't open the page "https://169.254.1.250 " because it could not connect to the server "169.254.1.250".

When using Edge:

> Hmmm...can't reach this page
> Try this
> - Make sure you've got the right web address: https://169.254.1.250
> - Search for "https://169.254.1.250" on Bing
> - Refresh the page
>
> Details
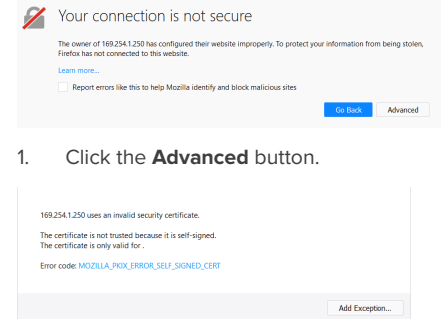
If you are using Edge, update your browser version before trying the following steps.

1. If the Link LED on your router is not lit, ensure the Ethernet cable is connected.

2. If one of the messages shown above appears, ensure the network IP address is *not* set to 169.254.1.250 which is the default IP address for the appliance port in Access Control Manager.

3. To ensure the cable is connected and no conflict occurs with the IP address, type **ping 169.254.1.250** at a DOS command prompt. If there is no response, double check the connection and IP address. If the connection and IP address are correct, call Avigilon Technical Support for assistance.
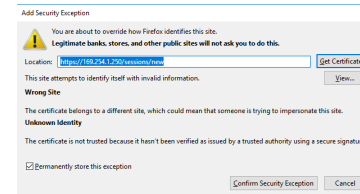
If a security exception screen appears...

When using Firefox:

> **Your connection is not secure**
>
> The owner of 169.254.1.250 has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.
>
> Learn more...
>
> ☐ Report errors like this to help Mozilla identify and block malicious sites
>
> [Go Back] [Advanced]

1. Click the **Advanced** button.

> 169.254.1.250 uses an invalid security certificate.
>
> The certificate is not trusted because it is self-signed.
> The certificate is only valid for...
>
> Error code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT
>
> [Add Exception...]

2. Click the **Add Exception...** button.

> **Add Security Exception**
>
> You are about to override how Firefox identifies this site.
> **Legitimate banks, stores, and other public sites will not ask you to do this.**
>
> Location: [https://169.254.1.250/sessions/new] [Get Certificate]
> This site attempts to identify itself with invalid information. [View...]
> **Wrong Site**
> The certificate belongs to a different site, which could mean that someone is trying to impersonate this site.
> **Unknown Identity**
> The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.
>
> ☑ Permanently store this exception
>
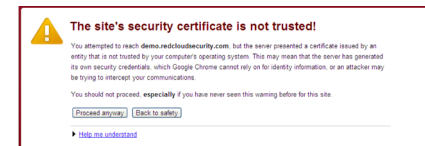> [Confirm Security Exception] [Cancel]

3. Click the **Get Certificate** button.
4. Check **Permanently store this exception**.
5. Click the "Confirm Security Exception" button.

When using Chrome:

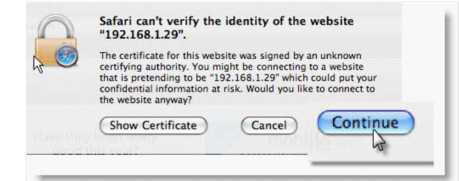> ⚠ **The site's security certificate is not trusted!**
>
> You attempted to reach **demo.redcloudsecurity.com**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Google Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications.
>
> You should not proceed, **especially** if you have never seen this warning before for this site.
>
> [Proceed anyway] [Back to safety]
>
> ▶ Help me understand

Click **Proceed anyway**.

When using Internet Explorer:

> ✖ There is a problem with this website's security certificate.
>
> The security certificate presented by this website was not issued by a trusted certificate authority.
> The security certificate presented by this website was issued for a different website's address.
>
> Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
>
> We recommend that you close this webpage and do not continue to this website.
>
> Click here to close this webpage.
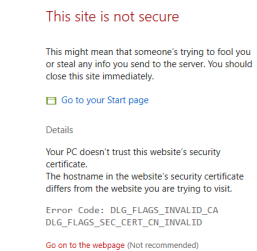> Continue to this website (not recommended).
> More information

Click **Continue to this website (not recommended)**.

When using Safari:

> **Safari can't verify the identity of the website "192.168.1.29".**
>
> The certificate for this website was signed by an unknown certifying authority. You might be connecting to a website that is pretending to be "192.168.1.29" which could put your confidential information at risk. Would you like to connect to the website anyway?
>
> [Show Certificate] [Cancel] [Continue]

Click the **Continue** button.

When using Edge:

> This site is not secure
>
> This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.
>
> 🏠 Go to your Start page
>
> Details
>
> Your PC doesn't trust this website's security certificate.
> The hostname in the website's security certificate differs from the website you are trying to visit.
>
> Error Code: DLG_FLAGS_INVALID_CA
> DLG_FLAGS_SEC_CERT_CN_INVALID
>
> Go on to the webpage (Not recommended)

Click **Go on to the webpage (Not recommended)**.