AVIGILON™

Access Control Manager™ System Integration Guide

For ASSA ABLOY™ Door Service Router and Lock Configuration Tool

This document has been compiled and published using product descriptions and specifications available at the time of publication. The contents of this document and the specifications of the products discussed herein are subject to change without notice. Avigilon Corporation reserves the right to make any such changes without notice. Neither Avigilon Corporation nor any of its affiliated companies: (1) guarantees the completeness or accuracy of the information contained in this document; or (2) is responsible for your use of, or reliance on, the information. Avigilon Corporation shall not be responsible for any losses or damages (including consequential damages) caused by reliance on the information presented herein.

Avigilon Corporation
avigilon.com

INT-ACM-AA-IP-A

Revision: 3 - EN

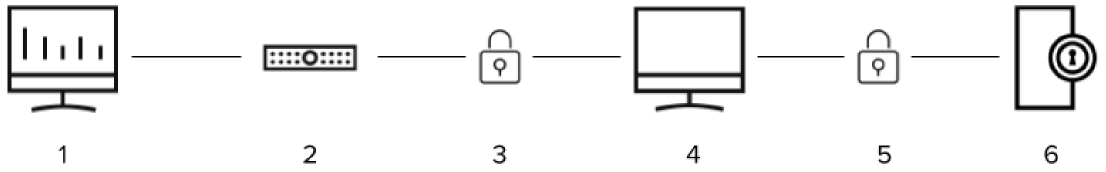
20230307

Table of Contents

Before You Start

Use the Access Control Manager (ACM) system integration with the ASSA ABLOY Door Service Router (DSR) and Lock Control Tool (LCT) to install and configure ASSA ABLOY IP-enabled locks and doors, and then manage user access in the ACM system.

System Overview



1	ACM applications, including identity (badging), administration, video surveillance and alarm monitoring
2	ACM appliance
3	Encrypted connection provided by the ACM appliance certificate and ASSA ABLOY DSR server configuration using Transport Layer Security (TLS)
4	ASSA ABLOY Door Service Router server, DSR Support Tool and Lock Configuration Tool applications
5	Encrypted connection provided by LCT network configuration
6	ASSA ABLOY IP-enabled external powered (hard powered) PoE locks and battery-powered Wi-Fi locks Typically, Wi-Fi locks are battery-powered (referred to as the Battery Powered lock type in ACM), and if configured with an external power supply, can have the real-time communication capabilities of hard-powered PoE locks (referred to as the External Powered lock type in ACM).

Prerequisites

Register for an account on the Avigilon Partner Portal (avigilon.com/software-downloads) to ensure you can download the required ACM software, ASSA ABLOY software and embedded documentation.

System Requirements

- ACM 6.18.0 release
- DSR 8.0, installer version 8.0.13.0 or newer
    - Administrator account to complete the DSR-related procedures in this guide
    - DSR software system requirements
- LCT installer version 4.0.55.0 or newer

For More Information

- ACM 6.18.0 Release Notes
  (avigilon.com/support/access-control/acm6/)
- ACM User Guide*
  (avigilon.com/support/access-control/acm6/)
- DSR (Door Service Router) Software Installation Manual
  (see the DSR installer in the Avigilon Partner Portal)
- DSR Support Tool User Manual*
- Lock Configuration Tool User Manual*

*Click the **?** icon in the respective software to access online documentation.

Step 1: Install and Configure the DSR

To install and configure the DSR, which includes the DSR server and DSR Support Tool:

1. Download the zipped file for the `DSRInstaller8.0.13.0.exe` and *DSR (Door Service Router) Software Installation Manual* from the Avigilon Partner Portal.
2. Run the installer as the Administrator and follow the wizard workflow and installation manual.

   Note: The installer version replaces the installed Oracle® Java 8 with JRE8 (Java SE Runtime Environment 8) after completion of the installation on the Microsoft™ Windows™ machine.

   a. Create separate accounts for the DSR Support Tool Configuration and DSR Database Configuration when prompted.

   b. Set up the encrypted connection with the ACM system for the DSR Server Configuration when prompted:

      - In the **WS Encryption** field, select **False**.
      - In the **TLS/SSL Security** field, select **True**.

        Important: The encrypted connection must be enabled in the DSR Support Tool.

      - In **Access Data Port** field, enter the port number used for communication between the DSR and the ACM system. Make sure a firewall inbound traffic rule is created for the port.
      - In the **Lock Port** field, enter the port number used for communication between the DSR and the lock.
      - In the **Security Valve** field, enter a list of the IP addresses or hostnames, separated by a pipe (|) character, corresponding to the machine that the DSR is running on and the ACM appliance that can access the DSR Support Tool:

        `127.0.0.1|0:0:0:0:0:0:0:1|`*`ACM_appliance_IPaddress_1`*|*`ACM_appliance_IPaddress_2`*

        Important: The default DSR address in the above is required. It is the same address that is entered in the DSR panel configuration in the ACM system.

Note: If you are configuring replication and failover of the ACM application, enter multiple IP addresses for the ACM appliances.

3. After you install the DSR server and DSR Support Tool:
    a. Log in to the browser-based DSR Support Tool that was configured in the **Security Valve** field.

       Example: `https://127.0.0.1:8080/dsrsupport`
    b. Download the DSR Support Tool user manual from the **?** icon.
    c. Use the tool to view locks that are provisioned in the LCT application.

Step 2: Update the Windows Hosts File

To update the Windows host file on the machine where the DSR server is installed:

1. Open the `C:\Windows\System32\drivers\etc\hosts` file.
2. Add an entry for your ACM appliance in *`ACM_appliance_IPaddress ACM_appliance_hostname`* format.

   ```
   nnn.n.n.n ACM_hostname
   ```

3. If required, repeat the above steps for each ACM appliance in a replication set.
4. On your desktop, start a Windows PowerShell (Admin) session:
   1. Flush the cache.

      ```
      cd 'C:\Windows\System32\drivers\etc'
      ipconfig /flushdns
      ```

      A success message is displayed.
   2. Ping the hostname of the ACM appliance.

      ```
      ping ACM_appliance_IPaddress
      ```

      Replies and ping stats are displayed.

Step 3: Update the ACM Appliance Certificate

To update and install the ACM appliance certificate:

1. In the ACM system:

   a. Create an ACM appliance certificate from ⚙ >**Appliance**.

   b. Enter the hostname of the ACM appliance (for example, `acm-2`) in the **Organization Unit Name**, **Common Name** and **Subject Alternative Name (FQDN)** fields.

   c. Save the settings.

   For more information, click the **?** icon.

2. In your browser:

   a. Click the site connection icon and export the ACM appliance certificate to a file format that is supported by your browser.

   b. Rename the exported file to a `.csr` filename.

   Example: `Base64 Encoded X.509 (*.cer)` to `*.csr`

3. If required, repeat the above steps for each ACM appliance in a replication set.

4. On your desktop, start a Windows PowerShell (Admin) session:

   a. Type `cd 'C:\Program Files\jre8\lib\security\'`.

   b. Update the `alias` parameter with the hostname of the ACM appliance (or multiple ACM appliances if deploying an appliance in a replication set) and the `file` parameter with the path to the `.csr` certificate:

   ```
   keytool -importcert -alias ACM_appliance_hostname_1 ACM_appliance_
   hostname_2 ACM_appliance_hostname_n -file ACM_certificate_pathname -
   keystore .\jssecacerts
   ```

   Example: `keytool -importcert -alias acm-1 acm-2 acm-n -file C:\tmp\acm-2.csr -keystore .\jssecacerts`

   c. Enter your keystore password.

   d. Type `yes` to trust the certificate.

Step 4: Install and Configure the LCT and ASSA ABLOY Locks

To install and configure the LCT and ASSA ABLOY locks:

1. Download the zipped file for the `LCTInstaller4.0.55.0.exe` and *Lock Configuration Tool User Manual* from the Avigilon Partner Portal.
2. Run the installer and follow the wizard workflow and installation manual.
3. After you have installed the LCT, log in and complete lock configuration:
   a. Click the **Create** button to create a new configuration file and save the settings.

      Note: Store the **Site Name** and **Administrator Password** in a secure location.

      For more information, click the **?** icon.

   b. Click the **Create New Profile** button to set up the communication between a group of locks and the DSR:
      - On the Details tab, select the **Set as default** and **Privacy** checkboxes and save the settings.
      - On the Network Setup tab, enter the **IP Address** of the DSR machine and **Port**.

        Note: Make sure the **Use alternate PoE communication** checkbox is not selected to avoid connection issues with the locks.

        For Battery Powered lock only. Enter the lock credentials in the WiFi Manager middle panel.

        Important: The encrypted connection between the lock and Wi-Fi network must be configured in the middle panel.

        Save the settings.
      - On the Reader Setup tab, select **multiCLASS Reader**, **iCLASS/iCLASS SE** and **HID Prox** for each Card Type.

        Leave **Application** as the Card Data Type. Save the settings.

      Note: Store the LCT configuration file in a secure location.

4. On your Windows machine, make sure the firewall can support inbound traffic on the port used for communication between the lock and DSR.
5. Using a Mini USB cable, connect the lock to your workstation:
    a. On the Lock Configuration tab of the LCT, the lock should automatically be detected as plugged in.

    > **Note:** To prevent issues in lock operation, make sure the lock has sufficient battery power in case you need to disconnect the USB cable.

    b. Click the settings icon button.

    c. On the Firmware Upgrade tab, if needed, click the **Upload Firmware** button. The lock Comm and Tamper light will blink during the firmware upgrade until it completes. After several minutes, the lock is displayed in the Lock Configuration list.

    d. On the Configuration tab, enter the **Lock Name** and click the **Configure** button to save the settings.

    > **Tip:** A recommended practice is to name the lock using the *MODEL_NUMBER-MAC_ADDRESS* format.

    The lock is now connected to the DSR.
6. In the DSR Support Tool, select **Facility View**. The status and details of the provisioned lock are automatically displayed.

Step 5: Integrate the ACM System and DSR

To integrate the ACM system and DSR:

1. For the DSR Support Tool:
   a. On your Windows machine:
      - Make sure the firewall can support inbound traffic on the port used for communication between the DSR and ACM system.
      - Make sure to register the ACM hostname with the DNS server.

        If the ACM hostname is not registered to the DNS server, add `ACM`*`appliance_IPaddress ACMappliance_hostname`* to the `hosts` file (assuming Windows 10):

        `C:\Windows\System32\drivers\etc\hosts`

   b. On the main menu of the DSR Support Tool, select **Configuration Settings** > **Server Settings** > **WS Encryption & Port Configuration** and make sure the following settings are selected.
      - In the **WS Encryption** field, select **False**.
      - In the **TLS/SSL Security** field, select **True**.

        Important: The encrypted connection must be enabled in the DSR Support Tool.

      - In the **Sentinel-Bit** field, select **False**.
      - In **Access Data Port** field, enter the port number used for communication between the DSRand the ACM system. Make sure a firewall inbound traffic rule is created for the port.
      - In the **Lock Port** field, enter the port number used for communication between the DSR and the lock.
      - In the **Security Valve** field, enter a list of the IP addresses or hostnames, separated by a pipe (|) character, corresponding to the machine that the DSR is running on and the ACM appliance that can access the DSR Support Tool:

        `127.0.0.1|0:0:0:0:0:0:0:1|`*`ACM_appliance_IPaddress_1|ACM_appliance_IPaddress_2`*

        Important: The default DSR address in the above is required. It is the same address that is entered in the DSR panel configuration in the ACM system.

        Note: If you are configuring replication and failover of the ACM application, enter multiple IP addresses for the ACM appliances.

c. Save any changes.

d. On the main menu of the DSR Support Tool, select **Configuration Settings** > **Controller Settings** > **Device Specific Commands** > **Custom Settings**.

   - On the Filters tab, make sure the **USER** event filter is not selected.

e. Save the setting.

2. In the ACM application:

   a. Create an **Assa Abloy** panel from **Physical Access** > **Panels**.

   b. On the Host tab, enter the IP address of the DSR machine (see the Security Valve field) in the **IP Address** field.

   c. Save the setting.

   For more information about the other fields, click the **?** icon.

Troubleshooting

If the following troubleshooting solutions do not resolve the issue, contact Avigilon Technical Support: **avigilon.com/support**.

DSR does not install or start up

To resolve the issue, do any of the following:

- Some versions of Oracle JRE can cause DSR installation and/or startup issues. Refer to the DSR software requirements for the supported JRE version before reinstalling the DSR software.