INSTALLING AVALANCHE

This paper describes how to perform a first-time installation of Avalanche 6.1.

If you are currently running a version of Avalanche earlier than 6.0, find the Upgrading to Avalanche 6.1 instructions on the Wavelink Web site.

To install Avalanche:

1   Review the Avalanche 6.1 System Requirements on the Wavelink website and ensure your environment meets minimum system requirements.

2   Download the Avalanche installer. To obtain the Avalanche installer, contact your Wavelink Sales representative.

3   Install Microsoft SQL Server. For detailed steps that describe installing SQL Server 2008 R2 for Avalanche, see the Wavelink Community article Setting up SQL Server 2008 R2 Express. For general information about installing SQL Server, see Setting Up Microsoft SQL Server (1).

4   Run the Avalanche installer. For information about running the installer, see Running the Avalanche Installer (3).

5   If you plan to connect iOS, Android, or Windows Phone 8 devices to Avalanche, set up the certificates and keys necessary to secure communication. For information about setting up secure communications for Avalanche, see Enabling Secure Communication (5).

6   Activate licenses for Avalanche. For information about licensing, see Licensing Avalanche in the Avalanche online help.

7   Connect devices to the Avalanche Server. To watch a video about connecting Smart devices, see the videos on YouTube: Connecting an Android Device to Avalanche or Connecting an iOS Device to Avalanche.

> ⓘ You must set up secure communication before you can connect Android, iOS, or Windows Phone 8 and 8.1 devices to Avalanche.

SETTING UP MICROSOFT SQL SERVER

As part of the installation process, you must set up databases with Microsoft SQL Server to store and access device information.

Avalanche 6.1 can use the following database platforms:

- SQL Server 2008

- SQL Server 2012

If you install the Express edition, you must use Microsoft SQL Server Express with Tools.

Microsoft SQL Server Express with Tools is available for free commercial use, but comes with hardware limitations that govern the number of CPU cores, memory, and hard drive space that can be used per instance. If you use a different version of SQL Server, you are responsible for all licensing and fees associated.

The steps below are an overview of what you must do to install SQL Server. For detailed steps about installing SQL Server, see the Wavelink Community article Setting up SQL Server 2008 R2 Express.

To set up SQL Server:

1 Install Microsoft SQL Server 2008 or 2012. Instructions for doing this can be found on the Microsoft Developer Network Web site.

Ensure you use **Mixed Mode** authentication. Avalanche supports Microsoft SQL Server's Default instance as well as any custom instances.

2 After completing the installation, open SQL Server Management Studio and log in.

3 Navigate to **Security > Logins** and select **New Login** from the context menu.

4 Enter a username.

5 Select the **SQL Server authentication** option.

6 Enter the database password and confirm it.

7 Clear the **Enforce password expiration** option.

8 Click **OK**.

9 Right-click on the new login and select **Properties**.

10 Click **Server Roles**.

11 Select **dbcreator**.

12 Click **OK**.

13 Navigate to **SQL Server Network Configuration > Protocols**.

14 Locate your server and right-click to select **Enable TCP/IP**. Dismiss the warning dialog box that pops up.

15 Double-click **TCP/IP** and click on the IP Addresses tab.

16 Scroll to IPAll and enter `1433` for the **TCP Dynamic Ports** field.

17 Click **OK**. Dismiss the warning dialog box that pops up.

18 Navigate to SQL Server Services, right-click your server, and click **Restart**.

You do not need to create the databases before you install Avalanche; the databases will be created when you run the Avalanche installer.

In some circumstances, communicating with database requires that you must enable TCP/IP for your instance and set it to port 1433 from SQL Server Configuration Manager. This port will also need to be opened through your network and computer firewalls. If you use named instances, you must also open port 1434.

ALLOWING REMOTE ACCESS TO THE DATABASE

If you install Microsoft SQL Server on the same computer as Avalanche, you do not need to configure the server for remote access. However, if your database server is on a different machine from where you will upgrade Avalanche, it must be configured to allow remote access.

To configure the Microsoft SQL Server database for remote access:

1 Launch SQL Server Management Studio.

2 In Object Explorer, right-click on your server and select **Properties**.

3 Click **Connections**.

4 Under Remote server connections, select **Allow remote connections to this server**.

5 Click **OK** to save the changes. Changing this setting does not require restarting the server.

6 Ensure TCP/IP protocols are enabled and your firewall is set to allow port 1433.

RUNNING THE AVALANCHE INSTALLER

The Avalanche installer is designed to include all components of the service, including the Web Console, device servers, certificate manager, and Remote Control server. This installer allows you to create all services on the same computer through one installation process. If you want to install the device servers on separate computers, see Installing Device Servers (5).

Avalanche installs its own JRE and changes the JRE_HOME system variable. If you have a JRE already installed, it is not affected by Avalanche. However, any program using the JRE_HOME variable will be redirected to use the Avalanche JRE.

> ⓘ The Web Console can be installed individually through the Select Components screen of the installer by clearing **Mobile Device Server**, **Smart Device Server**, and then **Enterprise Server**.

> ⓘ Do not perform a new install of Avalanche 6.1 on the same machine as any previous versions of Avalanche. This will result in system errors that prevent the existing installation from working correctly.

To install Avalanche:

1 Double-click the Avalanche installer.

2 Select a language and click **OK**.

3 Review the Pre-Install checklist and then click **Next** to continue.

4 Browse to your preferred install destination directory and click **Next**.

5 Select **New Installation** as the installation type.

6 The Select Components screen appears. Select which components you want included on the installation and click **Next**.

7 Enter the SQL Server credentials and click **Next**. The **Main DB Name** defaults to `Avalanche` and the **Stats DB Name** to `AvaStats`. If you use a named instance instead of the default MSSQLSERVER instance, select the checkbox for **Use Named Instance** and enter the name of your custom instance.

> ⓘ The **Hostname** is the IP address or hostname of the machine running SQL Server. The username and password were set during the Microsoft SQL Server installation process. The port used by Avalanche is 1433.

8 When prompted, click **Yes** to create the enterprise server and statistics server databases.

9 By default, Wavelink creates shortcuts in the Windows Start menu. Click **Next** to accept the shortcut, or modify it as desired and then click **Next**.

10 Click **Next** to begin the installation.

11 Click **Finish** to complete the installation.

INSTALLING DEVICE SERVERS

If you want to run your mobile device servers and Smart device server on machines separate from your enterprise server, use the device server installer.

Avalanche 6.1 only allows you to install one Smart device server, whereas you can create as many mobile device servers as needed.

To install a device server:

1 Double-click the device server installer to start the installation process.

2 Browse to your preferred install destination directory and click **Next** to continue.

3 Click **Next** to create a Start Menu folder.

4 Enter an **Avalanche Address** in the form of a hostname or IP address to identify and connect to the enterprise server's computer.

5 Click **Next** to begin the installation process.

6 Click **Finish** to complete the installation.

ENABLING SECURE COMMUNICATION

There are several connections used by Avalanche that can be secured using encryption methods. They include:

- Securing the connection between Android, iOS, or Windows Phone 8 devices and the Smart device server. This step is mandatory if you are going to connect Smart devices to Avalanche. This requires an SSL certificate, a GCM API for Android devices, and an APNS certificate for iOS devices.

- Securing the connection between the Avalanche Console (a web browser) and the Avalanche web server. This step is optional, and requires an SSL certificate.

- Securing the connection between AIDC devices and the Avalanche Remote Control server and viewer. This step is required if you have Avalanche Remote Control installed and you have secured the Avalanche Console. This step requires an SSL certificate.

For information on establishing secure communication for Avalanche, see the following topics:

- APNS Certificate for iOS

- GCM for Android

- SSL Certificates

APNS CERTIFICATE FOR IOS

Avalanche requires the use of an Apple Push Notification Service (APNS) certificate in order to manage iOS devices. You need your own certificate to ensure secure communication between iOS devices and your servers.

APNS certificates enable Avalanche's Smart Device Server to communicate with your iOS device over the wirelessly. Wavelink cannot submit or obtain APNS certificates for or on behalf of your organization.

After obtaining an APNS certificate, you must also obtain an SSL certificate for communication encryption between servers.

To complete this process, you must have an Apple ID.

To generate a CSR through Wavelink:

1   Navigate to `apnsportal.wavelink.com`.

2   Click **Start**.

3   Perform the steps indicated to create a private key and certificate.

4   Click **Next**.

5   Perform the steps indicated to upload the certificate and download a Wavelink-signed certificate.

6   Open another browser tab and navigate to `https://identity.apple.com/pushcert`.

7   Enter your Apple ID and password to sign in.

8   Select **Create a certificate**.

9   From the Create a New Push Certificate page, browse and upload your signed certificate file.

    The Apple Push Certificates Portal appears with the status **Confirmation**.

10 Click **Continue**.

11 Click **Download**.

    The `MDM_ LANDESK Software, Inc_Certificate.pem` certificate downloads.

12 From the `apnsportal.wavelink.com` browser tab, click **Next**.

13 Perform the steps indicated to export the signed certificate to PKCS #12 format.

14 Navigate to **Tools > System Settings**.

15 In the **SmartDevice Server** section, click **Add** under the Apple iOS heading.

16 Locate the signed certificate file and click **Open**.

17 Enter the pass phrase associated with the certificate.

18 Click **Save**.

Your iOS devices are now able to use the Apple Push Notification service through Avalanche. You must also have an SSL certificate for the Smart device server in order to connect iOS devices.

GCM FOR ANDROID

Installing Avalanche with Android Smart devices requires the use of Google Cloud Messaging (GCM) for managing Android devices.

GCM support enables Avalanche's smart device server to communicate to your device wirelessly. Wavelink cannot provide, submit, or obtain these communication credentials for or on behalf of your organization.

To complete this process, you must have a Gmail account.

In order to successfully implement GCM on a Smart Device Server, you must obtain a project ID and API key to authenticate your server as an acceptable originating entity for data communications.

To generate the GCM credentials needed:

1 Navigate to the Google Developers Console website:

`https://cloud.google.com/console`

2 Click **Create Project**.

3 Enter a project name and click **Create**.

A page appears that displays the project ID. Write down the project ID, as this will be needed to complete the GCM setup in Avalanche.

4 On the left, click **APIs & auth**.

5 Activate the **Google Cloud Messaging for Android** toggle.

6 Navigate to **APIs & auth > Credentials**.

7 In the Public API access section, click **Create new key**.

8 Click **Server key**.

9 Supply an IP address for your server. Providing an IP address is optional. Not specifying an address allows the API key to function on any server regardless of its IP address.

10 Click **Create**.

The page refreshes with the generated server API key.

11 From the Avalanche Console, navigate to **Tools > System Settings**.

12 In the **SmartDevice Server** section, enter the **Google Project Number** and **API key** you received in the Google Developers Console.

13 Click **Save**.

Your Android devices are now able to use Google Cloud service through Avalanche. You must also have an SSL certificate for the Smart device server in order to connect Android devices.

SSL CERTIFICATES

You should obtain an SSL certificate for these situations:

- If you have Android, iOS, or Windows Phone 8 devices that you want to connect to Avalanche, you must have an SSL certificate. Connecting Smart devices also requires a GCM API for Android devices, and an APNS certificate for iOS devices.

- If you want to secure the connection between the Avalanche Console (a web browser) and the Avalanche web server. This step is optional. If you do not use an SSL certificate for the web server, it connects to the browser and devices using Hypertext Transfer Protocol (HTTP), which is not encrypted.

- If you want to secure the connection between the Avalanche Remote Control server and the Remote Control viewer. This step is optional. The connection between the server and devices is automatically secured using PSK and does not require an SSL certificate.

When you use Avalanche with an SSL certificate for a secure connection, Wavelink strongly recommends that you purchase a certificate through a third-party certificate authority (such as Verisign). If you install the Avalanche web server, Smart device server, or Remote Control server on different systems, you need either a wildcard certificate or a certificate for each system where those Avalanche components are installed.

> These instructions explain how to manipulate certificates using OpenSSL. Wavelink does not include OpenSSL with Avalanche. The install files can be found on the OpenSSL Web site. If you want to use a different tool, refer to the user guide for that tool for the process of creating a certificate request or self-signed certificate.

See the following sections for information on setting up SSL certificates for Avalanche:

- Creating a Certificate Request for a Certificate Authority

- Converting a Certificate

- Importing Certificates for the Smart Device Server

- Configuring Tomcat to Use an SSL Certificate

- Importing the Certificate for Remote Control

If you choose to use self-signed certificates in order to set up a demo environment, see Creating a Self-Signed Certificate (14) for more information about self-signed certificates. Wavelink strongly recommends using a certificate from a certificate authority for a production environment.

CREATING A CERTIFICATE REQUEST FOR A CERTIFICATE AUTHORITY

These instructions explain how to generate a certificate signing request using OpenSSL. Wavelink does not include OpenSSL with Avalanche or install it for you. You can find a version of OpenSSL that runs on Windows through the OpenSSL Web site.

Wavelink strongly recommends using a certificate signed by a certificate authority. Utilizing a certificate authority like Verisign tells clients that your server information was verified by a trusted source and is authentic.

ⓘ   If you plan to enroll Windows Phone 8 devices, do not create wildcard certificates.

Wavelink recommends that you backup all certificate files after you have implemented your certificate.

To generate a private key for the certificate:

1   From a command line, navigate to:

```
[OpenSSL installation directory]\bin
```

2   Use the command:

```
openssl genrsa -des3 -out privateKey.key 2048
```

3   At the prompt **Enter pass phrase for privateKey.key**, type a pass phrase. When prompted, re-enter the pass phrase. The pass phrase is arbitrary, but should be noted for future reference.

ⓘ   If you get a message that says "`WARNING: can't open config file: /usr/local/ssl/openssl.cfg`", you need to set the configuration file

location. From the command prompt, use the following command:

```
set OPENSSL_CONF=[OpenSSL installation directory]
\bin\openssl.cfg
```

If OpenSSL created the privateKey.key file anyway, delete it. Then repeat steps 2 and 3.

4 Use the command:

```
openssl req -new -key privateKey.key -out CACert.csr
```

5 At the prompts, enter all requested information. For the Common Name, provide the fully qualified domain name of the computer where you plan to install the certificate. The domain name used should be one that your company owns. Add a DNS entry if needed to resolve this computer.

An example of generating a CSR:

```
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Some-State]:Utah
Locality Name (eg, city) [Newbury]:Midvale
Organization Name (eg, company) [My Company Ltd]:Wavelink Corporation
Organizational Unit Name (eg, section) []:Engineering
Common Name (eg, your name or your server's hostname)
[]:avaself.wavelink.com
Email Address []:support@wavelink.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []: avalanche
An optional company name []: Wavelink Corporation
```

When you apply to a certificate authority for an SSL web server certificate, you will need to submit the CACert.csr file that is generated by this process.

When sending the CSR to the certificate authority, request that the signed certificate be sent back as a PKCS #12 file. Before you use the certificate with Avalanche, you need to import the private key into the certificate file. For information about converting the certificate into PKCS #12 or importing the private key, see Converting a Certificate (10).

CONVERTING A CERTIFICATE

In order to use an SSL certificate for the Avalanche Console, Remote Control, or the Smart Device Server, the certificate must be in PKCS #12 format and include the private key. Even if the certificate authority gave you a .p12 file, you must import the private key into the .p12 file before you can use it with Avalanche.

To export a certificate to PKCS #12:

1 From a command line, navigate to:

```
[OpenSSL installation directory]\bin
```

2 Use the command:

```
openssl pkcs12 -export -out certificate.p12 -inkey privateKey.key -in
ca.pem
```

Where `privateKey.key` is the name of the key you created (either before creating the CSR, or when you generated a self-signed certificate), and `ca.pem` is the name of the certificate you are converting.

> ⓘ If you submitted a certificate signing request to a certificate authority and they sent back the certificate chain separate from the certificate, add `-certfile intcert.crt` to the end of the command, where `intcert.crt` is the name of the intermediate certificate.

3 Enter the pass phrase associated with the private key. Self-signed certificates created using the command given in Creating a Self-Signed Certificate (14) will not request a pass phrase.

4 Enter an export password. Verify the export password again.

The PKCS #12 file is created in the OpenSSL installation directory.

For information on importing the new certificate to a Smart device server, see Importing Certificates for the Smart Device Server (11).

For information on configuring the Avalanche web server to use the certificate, see Configuring Tomcat to Use an SSL Certificate (12).

For information on using a certificate for Avalanche Remote Control, see Importing the Certificate for Remote Control (13).

IMPORTING CERTIFICATES FOR THE SMART DEVICE SERVER

After obtaining a SSL certificate, import it into Avalanche using the Console so that the Smart device server can use it.

> ⓘ The certificate must be in PKCS #12 format. If the certificate is in a different format, see Converting a Certificate (10).

To complete the setup:

1 From the Avalanche Console, navigate to **Tools > System Settings**.

2 In the HTTPS Configuration section, click **Add**.

3 Locate the `certificate.p12` file and click **Open**.

4 Enter the pass phrase associated with the certificate. When the pass phrase is entered correctly, the Common Name is displayed in the **SDS Public Address** text box.

5 If the certificate is a wildcard certificate (uses a * in the Common Name), type the server address in the **SDS Public Address** text box.

6 Click **Save** at the top right of the page.

7 Perform a deployment from My Enterprise.

After you have set up the APNS certificate, GCM key, and the SSL certificate, communication between Smart devices and the Smart device server is enabled and you can enroll devices. You should import your licenses before attempting to connect devices.

CONFIGURING TOMCAT TO USE AN SSL CERTIFICATE

Once you have a PKCS #12 certificate, you can configure the Avalanche web server, Tomcat, to use encrypt traffic between the Console and the Avalanche server. This requires modifying the `server.xml` file and then restarting the Tomcat server.

To activate SSL for Tomcat:

1 Navigate to

```
[Avalanche installation directory]\Wavelink\Avalanche\apache-tomcat-
7.0.35\conf
```

and open the `server.xml` file with a text editor such as Notepad.

2 Find

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true" clientAuth="false"
sslProtocol="TLS" />
```

3 Remove the comment markers <!-- and --> so that the section is not commented out.

4 Replace the section to contain the following information:

```
<Connector port="8443"
protocol="org.apache.coyote.http11.Http11NioProtocol" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true" clientAuth="false"
sslProtocol="TLS" keystoreFile="C:/Program
Files/Wavelink/certificate.p12" keystorePass="password"
keystoreType="PKCS12" />
```

Where the `keystoreFile` value is the path to the certificate and the `keystorePass` value is the password you entered when creating the certificate. In the path to the certificate, use forward slashes.

5 Save your changes to the file.

6   Restart the Tomcat service.

Once you have generated a certificate, activated SSL for Tomcat, and restarted the Tomcat server, you can access the Web Console over an HTTPS connection.

To access the Web Console over a secure connection:

- In the address field of your browser, type:

    ```
    https://[DNS name or IP address of Avalanche]:8443/AvalancheWeb
    ```

IMPORTING THE CERTIFICATE FOR REMOTE CONTROL

The certificate must be stored in a Java keystore file named `keystore.jks` in order for Remote Control to use it, and then you need to modify the Remote Control `server.properties` file.

To import a certificate from OpenSSL to the keystore:

1   Copy the PKCS #12 certificate file to:

    ```
    [Avalanche installation directory]\Avalanche\jre\bin
    ```

2   From a command line, navigate to the same directory and use the command:

    ```
    keytool -importkeystore -srckeystore certificate.p12 -srcstoretype
    PKCS12 -deststoretype JKS -destkeystore keystore.jks
    ```

   where `certificate.p12` is the name of the certificate.

3   Enter a destination keystore password and verify it.

4   Enter the pass phrase associated with the certificate.

5   Copy the JKS certificate to the following location:

    ```
    [Avalanche installation directory]\Wavelink\Avalanche\RemoteControl\cfg
    ```

6   In this directory, open the `server.properties` file with a text editor such as Notepad.

7   Change this line:

    ```
    Global.Script.Edit.User = all
    ```

   to

    ```
    Global.Script.Edit.User = amcadmin
    ```

8   Add the following lines to the end of the file:

    ```
    AMC.Server.Type = 2
    Web.HTTPS.Enable = 1
    ```

```
Web.SSL.KeyPassword = password

Web.SSL.KeyStore = cfg/keystore

Web.SSL.MaxIdleTime = 60000

Web.SSL.Port = 8900
```

where `password` is the password associated with the SSL certificate.

9 Save the server.properties file.

10 Restart the Remote Control Server.

CREATING A SELF-SIGNED CERTIFICATE

These instructions explain how to generate a self-signed certificate using OpenSSL. Wavelink does not include OpenSSL with Avalanche. The install files can be found on the OpenSSL Web site. If you want to use a different tool, refer to the user guide for that tool.

Wavelink strongly recommends you use certificates from a certificate authority to secure communications for Avalanche. Using self-signed certificates may cause the following issues:

- If you use a self-signed certificate for the Web Console, a web browser may not recognize the certificate and displays warning messages that the site is not trusted. The browser may require you to make an exception in order to connect. The connection will be encrypted, however.

- If you use a self-signed certificate for the Smart Device Server, Android devices will refuse to enroll because they do not recognize the certificate. For devices running Android 4.0 or newer, you can install the self-signed certificate on each device. Devices running a version of Android older than 4.0 will not connect to a server that uses self-signed certificates. To install the certificate on the Android device, open a browser on the device and navigate to the iOS enrollment page after you have the certificate set up. On the page, tap **Trust this Server** and download the certificate. Once the certificate is downloaded, you can close the browser.

For instructions on obtaining a certificate from a certificate authority, see Creating a Certificate Request for a Certificate Authority (9).

> The file names given in these instructions, such as `privateKey.key` and `ca.pem`, are required if you are using the certificate for the Smart device server.

When creating a certificate you will need to provide a Common Name (such as an IP address), organizational unit, organization, city, state, and country code when creating your certificate.

1 From a command line, navigate to:

```
[OpenSSL installation directory]\bin
```

2 Use the command:

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
privateKey.key -out ca.pem
```

3 At the prompts, enter all requested information. For the Common Name, provide the fully qualified domain name of the computer where you plan to install the certificate. The domain name used should be one that your company owns. Add a DNS entry if needed to resolve this computer.

An example of generating a self-signed certificate:

```
Country Name (2 letter code) []:US
State or Province Name (full name) []:Utah
Locality Name (eg, city) []:Midvale
Organization Name (eg, company) []:Wavelink Corporation
Organizational Unit Name (eg, section) []:Engineering
Common Name (eg, your name or your server's hostname)
[]:avaself.wavelink.com
Email Address []:support@wavelink.com
```

The certificate `ca.pem` is created in the `\bin` directory.

In order to import the certificate and use the certificate for the Console and Avalanche Remote Control, you need to convert it to PKCS #12 format. For information on converting the certificate, see Converting a Certificate (10).

Wavelink Corporation
USA and Canada: 1.888.697.WAVE (9283)
Outside the USA and Canada: + 800 WAVELINK (9283 5465)
www.wavelink.com