CONFIGURING ENHANCED SECURITY OPTIONS FOR REMOTE CONTROL

Avalanche Remote Control 4.1.3 can be configured to use AES encryption between the device and the server, and SSL encryption between the server and the Remote Control Viewer or web browser. You may choose to implement one or both types of encryption depending on your environment. If you use SSL encryption, you must use either a self-signed certificate or a certificate issued by a certificate authority.

This paper contains the following tasks:

- Using Remote Control with AES Encryption
- Configuring the Remote Control Server for SSL

USING REMOTE CONTROL WITH AES ENCRYPTION

To use AES encryption between the device and the Remote Control Server, configure the server and the Client with the same passphrase. The passphrase can include ASCII symbols and uppercase and lowercase letters. Do not use two consecutive spaces in a passphrase.

NOTE: The following provides instructions on configuring the Client package from the Java Console. The task can also be accomplished from the Web Console.

To configure the Remote Control package:

1 On the **Profiles** tab, select the software profile that has the Remote Control package.

2 From the Software Packages area of the **Software Profile** tab, select the package and click **Configure**. The *Configure Software Package* dialog box appears.

3 From the available list, double-click **Client Configuration**. The *Remote Control Client Configuration* dialog box appears.

4 Enable the **Use Encryption** check box in the upper right corner.

5 Type the passphrase you want to use for encryption in the **Passphrase** text box.

6 Click **OK**.

7 Deploy the package.

To configure the Remote Control server:

1. Access the Remote Control Console by opening a web browser and typing the URL in an address bar. If you have not configured SSL, the URL is: `http://<IP address or Domain Name>:1900/app/setup_logon.vm`. If you have configured SSL, use the URL provided in the SSL instructions.

2. Log in using the credentials you provided during installation.

3. In the System Menu, click **Server Setup**.

4. Click the **Encryption** tab.

5. Enable the **Use Encryption** check box.

6. Type the passphrase you want to use for encryption in the Passphrase text box.

7. Click **Save**.

8. Restart the Remote Control server.

CONFIGURING THE REMOTE CONTROL SERVER FOR SSL

The Remote Control Server can be configured to use SSL for connections between the server and a browser, so when you use the Remote Control Console, the connection is encrypted. It also encrypts connections between the viewer and the server. In order to use SSL, you must have a certificate and a private key.

If you intend to use Remote Control with an SSL certificate for a secure connection, you can either purchase a certificate through a third-party Certificate Authority (such as Verisign) OR create a self-signed certificate.

NOTE: If you create a self-signed certificate, web browsers may not initially recognize the certificate and display warning messages that the site is not trusted. They may require you to make an exception in order to connect. The connection will be encrypted, however.

To configure Remote Control for SSL, complete one of the following tasks:

- Implementing a Certificate from a Certificate Authority
- Implementing a Self-Signed Certificate

IMPLEMENTING A CERTIFICATE FROM A CERTIFICATE AUTHORITY

You can use Remote Control with a certificate from a Certificate Authority. Remote Control requires that the certificate be imported into the Java keystore. The steps may vary depending on the certificate authority vendor.

Wavelink strongly recommends that you backup the keystore and certificate files after you have implemented your certificate.

The steps provided below use the Java keytool utility. The following tasks are necessary to implementing an SSL certificate from a certificate authority:

- Creating a Keystore
- Generating the Certificate Signing Request
- Importing the Certificate
- Configuring Remote Control to Use SSL
- Accessing the Remote Control Console over a Secure Connection
- Configuring the Package with the Server Address

Creating a Keystore

To create a keystore for the certificate, use the keytool.exe utility. You will need to provide a domain name (Common Name), organizational unit, organization, city, state, and country code. You will also need to provide a keystore name and passwords for the keystore and alias. These should be noted for future reference.

To generate a keystore for the certificate:

1 From a command line, navigate to:

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

where `[RC installation directory]` is the directory where Remote Control is installed.

2 Use the command:

```
keytool -genkey -alias rcselfcert -keyalg RSA -keystore keystore
```

3 At the prompt **Enter keystore password**, type the keystore password. When prompted, re-enter the password.

4 At the prompt **What is your first and last name**, type the domain name. The domain name you enter should be the domain name for the server where Remote Control is installed. Wavelink recommends using the fully qualified domain name unless you plan to use a wildcard certificate.

NOTE: Remote Control will not function if the domain name on the certificate is incorrect.

5. At the prompts, enter your organizational unit, organization, city, state, and the country code.

6. When you are prompted to review your information, type `yes` to confirm that it is correct. If you type `no`, you will be guided through the prompts again.

7. At the prompt **Enter key password for <rcselfcert>**, press `Return` to use the same password for the key.

8. The certificate and keystore are created.

An example of generating a keystore:

```
Enter keystore password: avalanche
Re-enter new password: avalanche
What is your first and last name?[Unknown]: domain.wavelink.com
What is the name of your organizational unit?[Unknown]:
Engineering
What is the name of your organization?[Unknown]: Wavelink
Corporation
What is the name of your City or Locality?[Unknown]: Midvale
What is the name of your State or Province?[Unknown]: Utah
What is the two-letter country code for this unit?[Unknown]: US
Is CN=domain.wavelink.com, OU=Engineering, O=Wavelink Corporation,
L=Midvale, ST=Utah, C=US correct?[no]: yes
Enter key password for <rcselfcert>(RETURN if same as keystore
password):
```

Generating the Certificate Signing Request

Once you have created the keystore, you can use the keytool.exe utility to generate a certificate signing request (`certreq.csr`) file to send to a certificate authority.

To generate a certificate signing request:

1. From a command line, navigate to:

```
[Remote Control installation directory]\jre\bin
```

2. Use the command:

```
keytool -certreq -keyalg RSA -alias rcselfcert -file certreq.csr
-keystore "[Remote Control installation
directory]\JRE\bin\keystore"
```

3. Enter your keystore password.

When you apply to a certificate authority for an SSL web server certificate, you will need to submit the `certreq.csr` file. This file should be created in the `[Remote Control installation directory]\jre\bin` folder.

Importing the Certificate

When you acquire your certificate and any intermediate certificates from the certificate authority, import them into the keystore. Depending on the format of the files, you may need to convert them to a format that the keystore will recognize. Copy the file or files to the `[Remote Control installation directory]\JRE\bin` directory before you import.

NOTE: If you generated the CSR from the computer where Remote Control is installed, the keystore will already have the private key. If you need to import the private key to a different keystore or if you need to combine the certificate file and intermediate certificates, use a tool such as OpenSSL to convert the files to a single file in PKCS12 format before importing the file to the keystore.

To import a certificate:

1 From a command line, navigate to:

```
[Remote Control installation directory]\JRE\bin
```

2 Use the command:

```
keytool -import -alias amccert -keystore keystore -trustcacerts -
file example.cer
```

NOTE: As an example, `example.cer` is used as the filename. Replace this with the name of your certificate file.

3 Enter your keystore password.

The certificate is added to the keystore. After you have imported the certificate, copy the keystore file (named `keystore`) to the `Remote Control 4.1\cfg` directory.

Configuring Remote Control to Use SSL

Once you have generated a certificate, configure Remote Control with the keystore information. Modify the `server.properties` file and then restart the Remote Control server. If you do not want the password in clear text, obfuscate the password using the provided instructions.

NOTE: The properties file is case-sensitive.

To activate SSL for Remote Control:

1 Navigate to:

```
[RC Install location]\cfg
```

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

2. If the key password and the keystore password are the same, insert the following lines:

```
Web.HTTP.Enable = 0
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 for both the key and keystore.

Or, if the key password and keystore password are different, insert the following lines:

```
Web.HTTP.Enable = 0
Web.HTTPS.Enable = 1
Web.SSL.KeyPassword = [key password]
Web.SSL.Password = [keystore password]
Web.SSL.KeyStore = cfg/keystore
Web.SSL.MaxIdleTime = 60000
Web.SSL.Port = 8900
```

Where `[key password]` and `[keystore password]` are your passwords for the key and keystore.

3. Save your changes to the file.

4. Restart the Remote Control service.

To obfuscate a password:

1. From a command line, navigate to:

```
[Remote Control installation location]\lib
```

2. Use the command:

```
java.exe -cp jetty-6.1.24.jar;jetty-util-6.1.24.jar
org.mortbay.jetty.security.Password [password]
```

where `[password]` is the password you want obfuscated.

The command will generate an obfuscated password that begins `OBF:`. Use the entire line as a password in the `server.properties` file. For example:

```
Web.SSL.KeyPassword = OBF:1vgt1t331vg1
```

Accessing the Remote Control Console over a Secure Connection

Once you have imported the certificate, copied the keystore file to the Remote Control cfg directory, and configured and restarted Remote Control, you can access the Console over a https connection.

To access the Remote Control Console over a secure connection:

- In the address field of your browser, type:

```
https://<Domain Name>:8900/app/setup_logon.vm
```

Configuring the Package with the Server Address

In order to connect to a device after configuring the server to use SSL, you must configure the Remote Control package with the new server port and protocol.

NOTE: This document provides instructions on configuring the package from the Java Console. The task can also be accomplished from the Web Console.

To configure the package with the server address:

1. On the **Profiles** tab, select the software profile that has the Remote Control package.
2. From the Software Packages area of the **Software Profile** tab, select the package and click **Configure**. The *Configure Software Package* dialog box appears.
3. From the available list, double-click **Server Location**. The *Remote Control Server Location* dialog box appears.
4. In the Server text box, type the address and port for the Remote Control server, including the https protocol. For example:

   ```
   https://servername.headquarters.yourcompany.com:8900
   ```

5. Click **OK**.

   The software package is ready for synchronization.

IMPLEMENTING A SELF-SIGNED CERTIFICATE

These instructions explain how to generate and use a self-signed certificate for Remote Control. If you choose not to use a Certificate Authority, you can still use a https connection to connect to the Web Console by creating your own certificate.

NOTE: Internet browsers may not recognize a self-signed certificate as trusted and display warnings before allowing you access.

Wavelink strongly recommends backing up the server configuration and keystore files after you have implemented a self-signed certificate.

This section contains the following tasks for implementing a self-signed certificate:

- Generating a Certificate
- Configuring Remote Control to Use SSL
- Accessing the Remote Control Console over a Secure Connection
- Configuring the Package with the Server Address

Generating a Certificate

To create a self-signed certificate, use the keytool.exe utility. You will need to provide the domain name (Common Name), organizational unit, organization, city, state, and country code when creating your certificate. You will also need to provide a keystore name and a password for the keystore and key. These should be noted for future reference.

To generate a self-signed certificate:

1 From a command line, navigate to:

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

where `[RC installation directory]` is the directory where Remote Control is installed.

2 Use the command:

```
keytool -genkey -alias rcselfcert -keyalg RSA -keystore keystore
```

3 At the prompt **Enter keystore password**, type the keystore password. When prompted, re-enter the password.

4 At the prompt **What is your first and last name**, type the domain name. The domain name you enter should be the domain name for the server where Remote Control is installed. Wavelink recommends using the fully qualified domain name unless you plan to use a wildcard certificate.

NOTE: Remote Control will not function if the domain name on the certificate is incorrect.

5 At the prompts, enter your organizational unit, organization, city, state, and the country code.

6 When you are prompted to review your information, type `yes` to confirm that it is correct. If you type `no`, you will be guided through the prompts again.

7 At the prompt **Enter key password for <rcselfcert>**, press `Return` to use the same password for the key.

8 The certificate and keystore are created. Copy the keystore file (named `keystore`) to the `Remote Control 4.1/cfg` directory.

An example of generating a self-signed certificate:

```
Enter keystore password: avalanche
Re-enter new password: avalanche
What is your first and last name?[Unknown]: domain.wavelink.com
What is the name of your organizational unit?[Unknown]:
Engineering
What is the name of your organization?[Unknown]: Wavelink
Corporation
What is the name of your City or Locality?[Unknown]: Midvale
What is the name of your State or Province?[Unknown]: Utah
What is the two-letter country code for this unit?[Unknown]: US
Is CN=domain.wavelink.com, OU=Engineering, O=Wavelink Corporation,
L=Midvale, ST=Utah, C=US correct?[no]: yes
Enter key password for <rcselfcert>(RETURN if same as keystore
password):
```

Configuring Remote Control to Use SSL

Once you have generated a certificate, configure Remote Control with the keystore information. Modify the `server.properties` file and then restart the Remote Control server. If you do not want the password in clear text, obfuscate the password using the provided instructions.

NOTE: The properties file is case-sensitive.

To activate SSL for Remote Control:

1 Navigate to

```
[RC Install location]\cfg
```

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

2 If the key password and the keystore password are the same, insert the following lines:

```
Web.HTTP.Enable = 0
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 for both the key and keystore.

Or, if the key password and keystore password are different, insert the following lines:

```
Web.HTTP.Enable = 0
Web.HTTPS.Enable = 1
Web.SSL.KeyPassword = [key password]
Web.SSL.Password = [keystore password]
Web.SSL.KeyStore = cfg/keystore
Web.SSL.MaxIdleTime = 60000
Web.SSL.Port = 8900
```

Where `[key password]` and `[keystore password]` are your passwords for the key and keystore.

3. Save your changes to the file.

4. Restart the Remote Control service.

To obfuscate a password:

1. From a command line, navigate to:

   ```
   [Remote Control installation location]\lib
   ```

2. Use the command:

   ```
   java.exe -cp jetty-6.1.24.jar;jetty-util-6.1.24.jar
   org.mortbay.jetty.security.Password [password]
   ```

   where `[password]` is the password you want obfuscated.

3. The command will generate an obfuscated password that begins `OBF:`. Use the entire line as a password in the `server.properties` file. For example:

   ```
   Web.SSL.KeyPassword = OBF:1vgt1t331vg1
   ```

Accessing the Remote Control Console over a Secure Connection

Once you have generated a certificate, copied the keystore file to the Remote Control cfg directory, and configured and restarted Remote Control, you can access the Console over a https connection.

To access the Remote Control Console over a secure connection:

- In the address field of your browser, type:

  ```
  https://<Domain Name>:8900/app/setup_logon.vm
  ```

Configuring the Package with the Server Address

In order to connect to a device after configuring the server to use SSL, you must configure the Remote Control package with the new server port and protocol.

NOTE: This document provides instructions on configuring the package from the Java Console. The task can also be accomplished from the Web Console.

To configure the package with the server address:

1. On the **Profiles** tab, select the software profile that has the Remote Control package.
2. From the Software Packages area of the **Software Profile** tab, select the package and click **Configure**. The *Configure Software Package* dialog box appears.
3. From the available list, double-click **Server Location**. The *Remote Control Server Location* dialog box appears.
4. In the Server text box, type the address and port for the Remote Control server, including the https protocol. For example:

   ```
   https://servername.headquarters.yourcompany.com:8900
   ```

5. Click **OK**.

   The software package is ready for synchronization.

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