Background scanning in ACTIVE Net

(v7)

ACTIVE Network, LLC

ACTIVE Network, LLC
Dallas Corporate Office
717 N. Harwood Street, Suite 2500
Dallas, Texas 75201

About ACTIVE Network, LLC

ACTIVE Network, LLC is a technology and media company that helps millions of people find and register for things to do and helps organizations increase participation in their activities and events.

For more information about ACTIVE Network, LLC products and services, please visit ACTIVEnetwork.com.

If you have any questions about the features included in these release notes, please contact the ACTIVE Net Support team using the information below.

Phone: 1-800-663-4991

Email: activenetsupport@activenetwork.com

Website: http://support.activenetwork.com/activenet

Table of contents

Overview

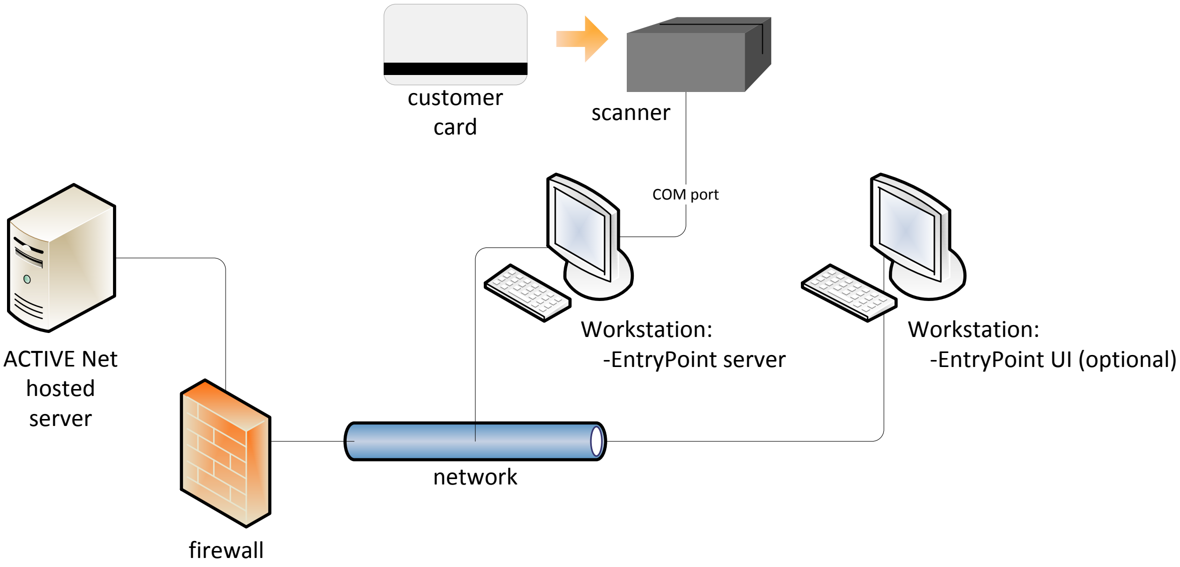
This document describes the prerequisites that you must have in place in order to configure and run background scanning in ACTIVE Net. It lists different scanning methods and describes supported scanning hardware. The document also summarizes how to install the EntryPoint server and UI applications, and how to configure your ports and network to enable background scanning.

Scanning methods and hardware

Scanning methods

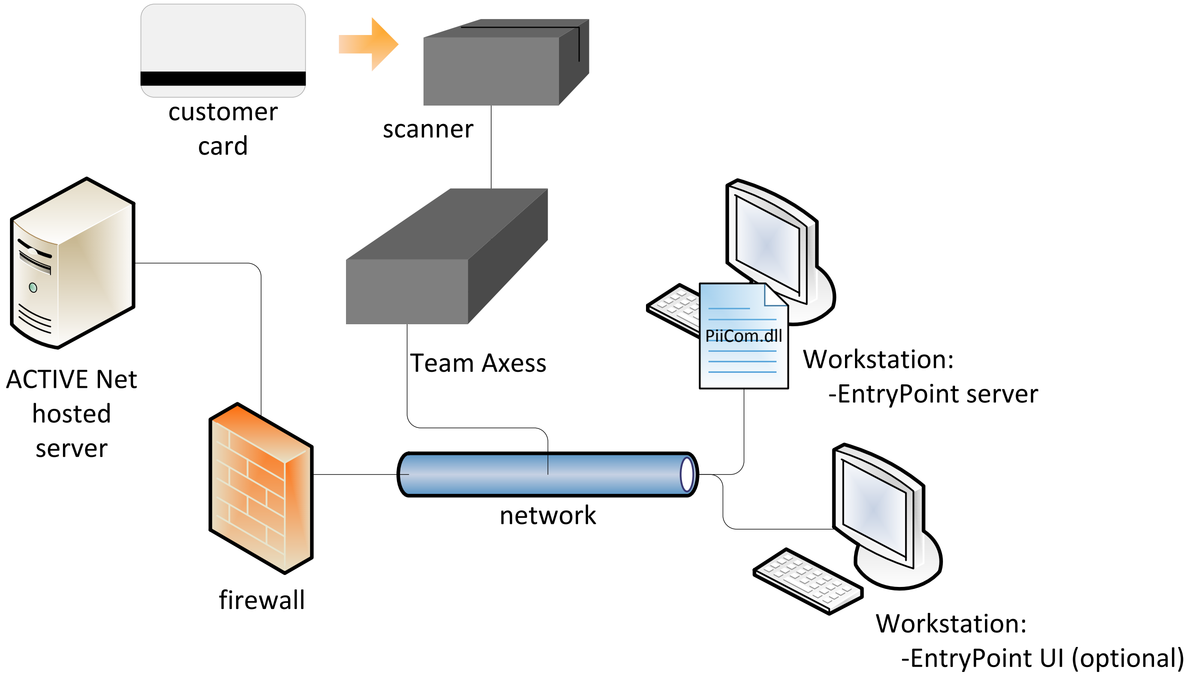
There are three methods of background scanning, depending on your hardware:

Serial



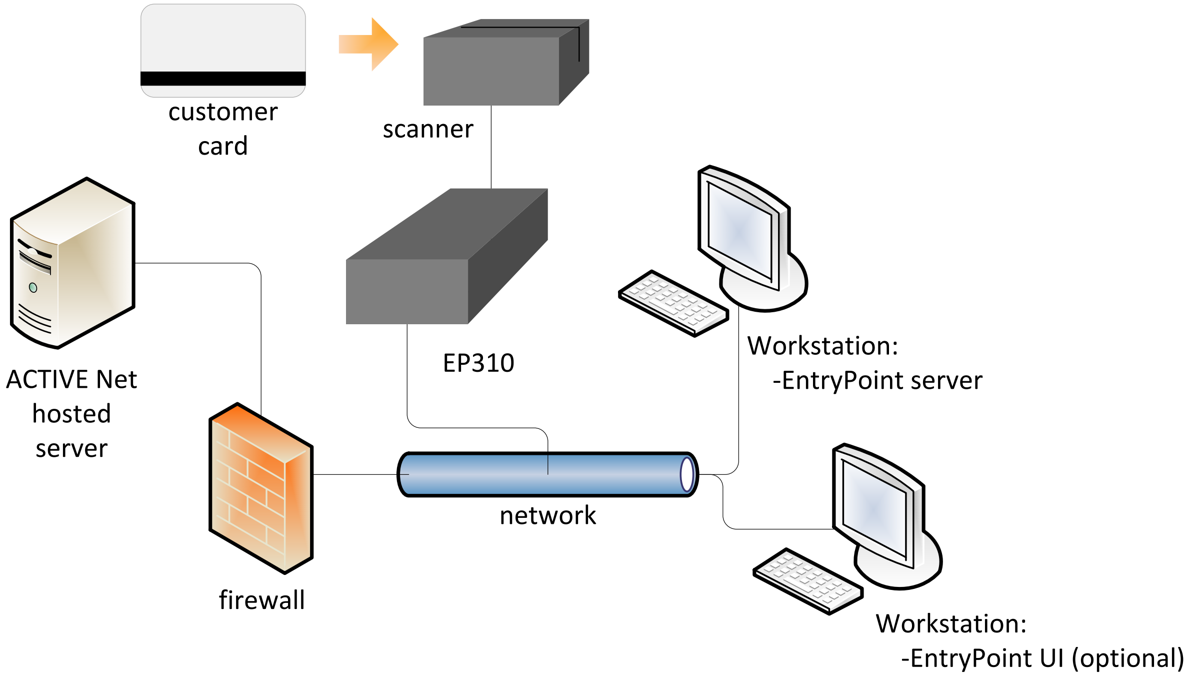
If you use a serial scanner, then the scanner is connected directly to the EntryPoint server workstation though a COM port.

Team Axess



If your hardware is from Team Axess, then the scanner is connected to a Team Axess device that is itself connected to the network. The EntryPoint server application uses the PiiCom.dll file on the EntryPoint server workstation to communicate with the scanner.

EP310



If your hardware is EP310, then the scanner is connected to an EP310 device that has its own IP address and port. The EntryPoint server machine uses this information to communicate with the scanner across your network.

Supported serial scanners

The following serial scanners are supported for background scanning:

- Orbit 7120
- Genesis 7580G-2
- WCR3227-633C
- WCR3237-633U
- IDMB-337112B

Note: Background scanning is supported for serial and USB-RS232 scanners, but not for USB keyboard or wedge scanners.

The following serial scanners are not supported:

- IDMB-334112B
- IDMB-334133B
- Voyager 9520/9540
- Symbol LS4208
- Devices with PS/2 (6 pin) connections.

Note: We do not support USB to serial hardware adapters.

Supported USB scanners for serial scanning

Many scanners used in serial scanning are actually USB scanners that use manufacturer-supplied serial emulation drivers. If you have obtained a USB scanner with a serial emulation driver from the ACTIVE Network, then it is supported.

Separate entry points required for multiple serial scanners

If you want to use multiple serial scanners, then you must configure separate entry points for each scanner in ACTIVE Net. Each entry point must have its own instance of the EntryPoint server running.

Multiple scanners required for multiple types of scans

If you are using a serial scanner for background scanning and validation, then you cannot also use it for other types of scanning, such as scanning a client's card to bring them up in ACTIVE Net for a transaction. The EntryPoint server that listens for background scanning events is constantly running, so it can't be interrupted to make other types of scans. If you want to do other types of scans while also running background scanning, then you must use more than one scanner.

No support for customers with multiple passes

ACTIVE Net does not support scanning multiple passes for a single customer through background scanning. In the standard validation interface (non-background scanning), staff can manually select from multiple passes to validate whenever a customer with more than one pass attempts to scan. When scanning happens in the background, however, then staff are not given the opportunity to select the correct pass that should be scanned at any given time.

For example, if a customer with multiple passes attempts to scan their card on a scanner that is running in the background, then the background scanning process automatically validates only the pass that has been specified as the default for that customer—staff are not given the opportunity to select a non-default pass. If no default pass has been specified for this customer, then the background scanning process automatically validates the pass that was purchased most recently.

Optional gatekickers

Gatekickers are optional to the background scanning process when using serial scanners. They are not required if you just want to have the EntryPoint UI open on a separate monitor so that your staff can quickly glance over and visually confirm whenever a valid or invalid scan is made, without interrupting their work flow.

Setting up the EntryPoint server and UI

Installing the EntryPoint server

First select a workstation to host the EntryPoint server. For the serial scanning method, this should be the same machine that your scanner is connected to. For other scanning methods, this workstation does not need to be connected to the scanner. You can use this machine for other things while the EntryPoint server is running, such as working in ACTIVE Net.

To install and run the EntryPoint server application, follow the steps below on the workstation that you want to use as your EntryPoint server:

1. Use a web browser to go to http://activenet.active.com/entrypoint.
2. In the **Entrypoint Server** section, click **EntryPoint.exe**.
3. Save and run the **EntryPoint.exe** file.

Once you have installed the EntryPoint server, it runs as a background service in Windows.

Note: The EntryPoint server uses an ACTIVE Net user account to communicate with ACTIVE Net (this account is specified in the EntryPoint server setup). Ensure that this user account has admin privileges in ACTIVE Net.

Installing the EntryPoint UI

The EntryPoint UI is an optional visual interface that you can install on another workstation. It is optional because background scanning and validation will still happen as long as the EntryPoint server is running, whether or not you are also running the EntryPoint UI.

To install and run the EntryPoint UI application, follow the steps below on the workstation that you want to use to run the EntryPoint UI:

1. Use a web browser to go to http://activenet.active.com/entrypoint.
2. In the **Entrypoint UI** section, click **EntryPointUI.exe**.
3. Save and run the **EntryPointUI.exe** file.

Ports and network configuration

ACTIVE net background scanning requires communication between the EntryPoint server and the EntryPoint UI workstation (if applicable), and between the EntryPoint server and the ACTIVE Net hosted server across your network. Background scanning will not function properly unless specific ports are open on your EntryPoint server workstation and network.

Configuration of the EntryPoint server workstation

The EntryPoint server machine uses webservices to communicate with the ACTIVE Net hosted server using http or https. Keep ports 80 and 443 open to enable this communication.

Select a specific port number that the EntryPoint server will use to communicate with the EntryPoint UI. The default recommended port number is 4000. Specify this port number when you configure both the EntryPoint server and the EntryPoint UI. This port must remain open on the EntryPoint server workstation and over the network.

Note: Port 80 is typically reserved for internet communications, so do not select this port number in the EntryPoint server and UI configuration.

Configuration of the EntryPoint UI workstation

On the EntryPoint UI workstation, Windows randomly assigns ports when communicating with the EntryPoint server. Because of this, you must keep all network ports open on the EntryPoint UI machine.

Troubleshooting

If your EntryPoint server is unable to connect to the web service on the ACTIVE Net hosted server, try the following troubleshooting strategies:

- First, make sure you have a recent version of Java 7 installed, which comes with the latest security certificates.
- If installing a recent version of Java 7 does not resolve the connection issue, then run a java utility that tests whether your EntryPoint server can connect to another server using SSL. See the Appendix of this document for complete steps describing how to run this utility.

  If you see a **Successfully connected** message, then the utility is able to connect using SSL. If the utility can successfully connect but the EntryPoint server cannot connect on its own, then further troubleshooting may be required to identify the issue with the EntryPoint connection. Contact your ACTIVE Net representative for more information.

  If you see an error message, then the utility was not able to connect using SSL. Continue with the steps below.
- If the java utility was not able to connect to another server using SSL, try manually installing the necessary security certificate using the following instructions:

  1. Go to the web service URL at https://activenettr012.active.com/phoenixtrainer/servlet/services/ActiveNetEntryPointWS?WSDL using a browser such as Internet Explorer or Google Chrome.

     The browser will display a message warning you about the certificate. Click **View Certificate** and install the certificate. Ignore any warning messages.

     Note: If you are using Internet Explorer, open the certificate in Administrator mode (right-click on the Internet Explorer menu link and click **Run as Administrator**). Otherwise, the **Copy to File** button in step #3 below will be disabled.
  2. The browser should now display a lock in the address bar (in Chrome the lock appears to the left of the URL, in Internet Explorer the lock appears to the right).

     If you are using Chrome, click the lock, change to the Connection tab, and click **Certificate information**.

     If you are using Internet Explorer, click the lock and then click the option to **View Certificates** in the menu that appears.

3. In the **Certificate** window that appears, change to the **Details** tab and click **Copy to File**.

   This will lead you through steps to save the certificate to file. Make sure you leave the default option to save in DER encoded format, and save the file somewhere accessible with the default extension **.cer** (for example: **d:\temp\active.cer**).

4. Open a CMD window and run the following command (where `<java path>` is the actual path to where the Java JRE is installed, and `<certificate>` is the path and file name where the certificate was exported to (wrapped in quotes if the path contains a space):

   ```
   <java path>\bin\keytool.exe -import -noprompt -trustcacerts -
   alias activenettr012 -file <certificate> -keystore <java
   path>\lib\security\cacerts -storepass changeit
   ```

Appendix: Running the Java utility

Use the following steps to create a file that you can run to test your server's ability to connect with the ACTIVE Net web service:

1. Copy and paste the following code into a new text file:

```
import javax.net.ssl.SSLSocket;
import javax.net.ssl.SSLSocketFactory;
import java.io.*;

public class SSLPoke {
    public static void main(String[] args) {
              if (args.length != 2) {
                     System.out.println("Usage: "+SSLPoke.class.getName()+"
<host> <port>");
                     System.exit(1);
              }
              try {
                     SSLSocketFactory sslsocketfactory = (SSLSocketFactory)
SSLSocketFactory.getDefault();
                     SSLSocket sslsocket = (SSLSocket)
sslsocketfactory.createSocket(args[0], Integer.parseInt(args[1]));

                     InputStream in = sslsocket.getInputStream();
                     OutputStream out = sslsocket.getOutputStream();

                     // Write a test byte to get a reaction :)
                     out.write(1);

                     while (in.available() > 0) {
                            System.out.print(in.read());
                     }
                     System.out.println("Successfully connected");

              } catch (Exception exception) {
                     exception.printStackTrace();
              }
       }
}
```

2. Save the file with the name **SSLPoke.java**.
3. Open a CMD window.
4. Change to the folder where you saved the file.
5. Run the following command:

   ```
   javac SSLPoke.java
   ```

6. Run the following command:

   ```
   javaSSLPoke activenettr012.active.com 443
   ```

   Note: Replace **activenettr012.active.com** with the appropriate server name to match the web service URL that you are trying to connect to.