Security Considerations for ITScriptNet™ OMNI Communications

Overview

If your organization has specific security requirements for applications running on your network, you might be interested in information about how ITScriptNet OMNI communicates. This document discusses common security issues.

Versions

The content of this document applies to ITScriptNet OMNI versions up to and including V3.1. Future versions may make changes that will be reflected in updates to this document.

Communications

ITScriptNet OMNI uses a proprietary protocol over TCP/IP. Typically, ITScriptNet OMNI communicates on IP Port 61200, although this port can be configured to any available port.

ITScriptNet OMNI communications are not encrypted, but some content may be compressed. From a security standpoint, however, you can consider the communications to be plain-text.

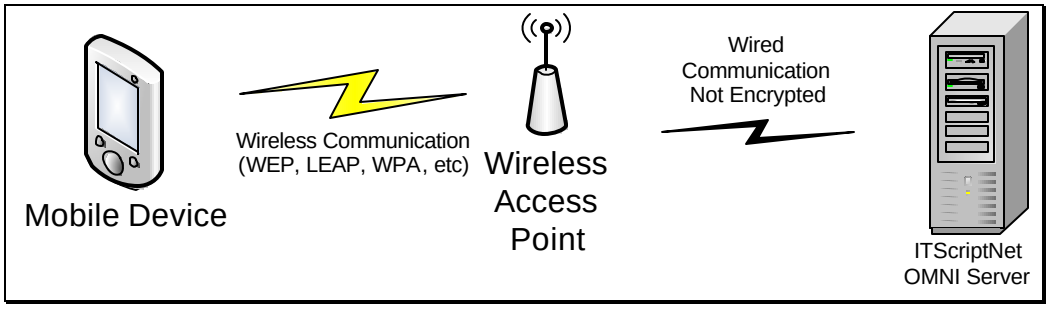
A portable device can communicate with an OMNI server in several ways. The most common include:

1) WiFi connection within an organization. Typically the OMNI Server is located in the same facility as the Wireless network.
2) ActiveSync connection to a local PC. The OMNI Server is running on the PC that the device is connected to, and communications is typically USB, although Serial, IrDA, and BlueTooth connections are possible.
3) ActiveSync connection to a remote PC. Since ActiveSync can provide a network connection pass-through, a portable device connected via ActiveSync to a remote PC can make a connection to an OMNI server running on a different PC. This is true as long as the OMNI server is reachable over the network from the ActiveSync PC.
4) Wide-Area connections. The Portable Device can have a wide-area connection, such as a GPRS connection to the internet. The OMNI Server can be located within a private network if the firewall is properly configured to allow OMNI traffic from the Internet to be forwarded to the OMNI Server.

Note: The use of the term 'ActiveSync connection' also includes Mobile Device Center connections to Windows Vista or Windows 7. The communications is the same for all of these connections.

The security considerations for each of these common configurations are discussed in more detail below.

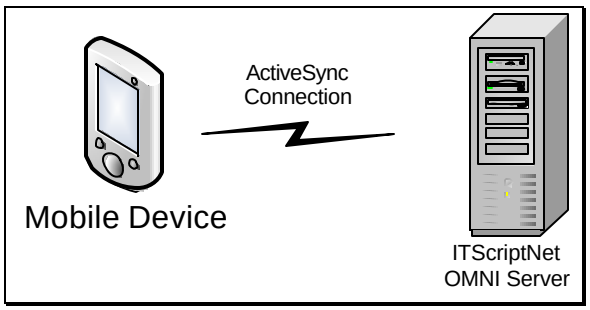
WiFi within an Organization



For organizations that are located within a single facility, the same Wireless Security that is used for the rest of the corporate network is generally sufficient for ITScriptNet OMNI. Windows CE and Windows Mobile devices support the common Wireless security protocols such as WEP, LEAP, WPA, etc. This provides enough security to prevent outside access to the data on the wireless network.

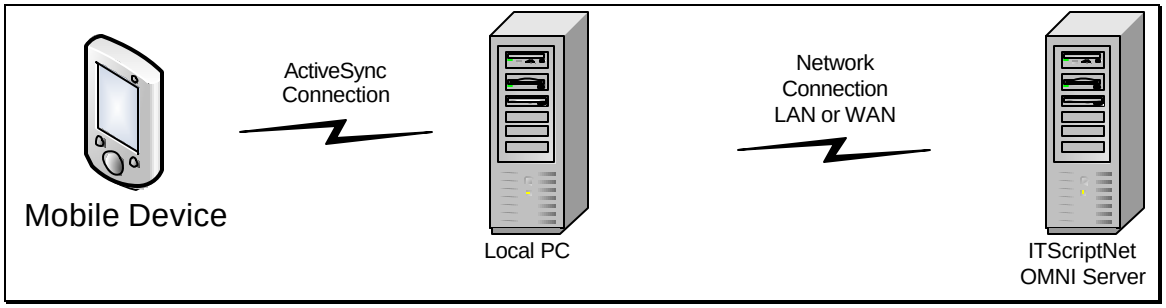
Some organizations require that all traffic on the wired and wireless networks be encrypted. ITScriptNet does not provide end-to-end encryption between the server and device. In these cases, a VPN would be required. There are third-party VPN clients for Windows CE and Windows Mobile that can be used.

ActiveSync Connection to a Local PC



In this scenario, the Mobile Device is directly connected to the PC running the OMNI Server software. The device would typically be connected USB, although other connection types are possible. Since eavesdropping on a direct USB connection is unlikely, additional encryption is probably not necessary.

ActiveSync Connection to a Remote PC



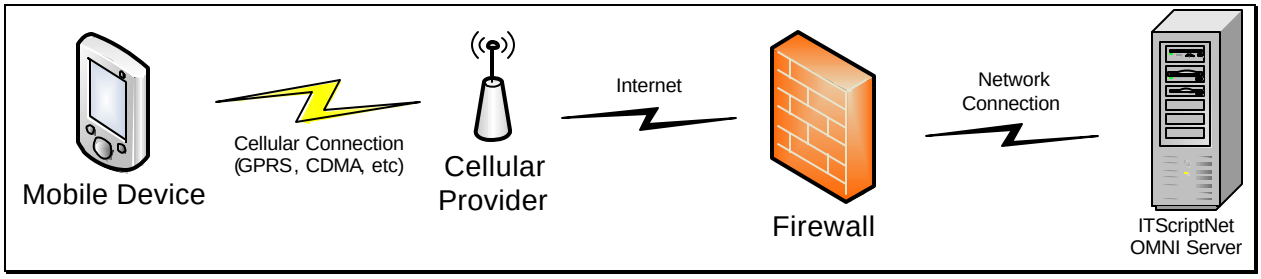
In this configuration, the Mobile Device is directly connected to a local PC with ActiveSync, and uses the ActiveSync pass-through to reach the OMNI Server which is located on another server.

The device would typically be connected to the local PC via USB, although other connection types are possible. Since eavesdropping on a direct USB connection is unlikely, additional encryption is probably not necessary for this portion of the link.

If the remote OMNI Server is located on the same wired network as the Local PC (for example within the same facility), then additional encryption is probably not needed. However, if your organization requires all traffic to be encrypted, then you may need to consider a VPN connection from the Mobile Device to the OMNI Server.

If the Remote OMNI Server is located across a WAN link from the Local PC, then there is typically a VPN already established from the local site to the remote site. This provides encryption of the traffic from the local to the remote facility, and may be sufficient.

Wide Area Connections



If the Mobile device is using a Wide Area connection ("outside the four walls"), there are two common configurations that can be used.

1) Forward the ITScriptNet TCP/IP Port through the firewall. In this scenario, the device connects to the Internet using the Wide-Area connection (GPRS, CDMA, etc), and attempts to connect to

the external IP Address of the firewall. The firewall is configured to forward traffic on the OMNI port to the private network address of the OMNI Server. In this way, only the OMNI traffic is allowed onto the network. The OMNI traffic is not encrypted in this scenario.

2) Establish a VPN connection from the Mobile Device to a VPN Server Firewall. This gives the Mobile Device access to the private network, while encrypting all traffic between the Mobile Device and the VPN server. Traffic on the private network is still not encrypted. In addition, port forwarding is typically not required, as the VPN connection gives the Mobile Device access to the private network.

Other Considerations

In addition to the communications between the Mobile Device and the OMNI Server PC, there may be other aspects of a data collection system to be aware of. For example, the OMNI Server may connect to a database server to update collected data or retrieve validation information. ITScriptNet OMNI does not encrypt this type of communications, but the database provider may be able to.