



WorldExtend

WorldExtend Environment Preparation Guide

WorldExtend IronDoor™ Version 3.5

WorldExtend, LLC.

Published: March 2008

Abstract

This guide explains how to prepare your application environment for WorldExtend use. It explains the requirements for your running your applications and requirements for executing the WorldExtend IronDoor Agent.

The information contained in this document represents the current view of WorldExtend, LLC. on the issues discussed as of the date of publication. Because WorldExtend, LLC. must respond to changing market conditions, it should not be interpreted to be a commitment on the part of WorldExtend, LLC., and WorldExtend, LLC. cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. WORLDEXTEND, LLC. MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of WorldExtend, LLC..

WorldExtend, LLC. may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from WorldExtend, LLC., the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2008 WorldExtend, LLC.. All rights reserved.

WorldExtend, WorldExtend IronDoor, WE-PC are either registered trademarks or trademarks of WorldExtend, LLC. in the United States and/or other countries.

Microsoft, Windows, Terminal Services, and SQL Server are registered trademarks of the Microsoft Corporation. All other names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Preparing for WorldExtend

To help insure a successful deployment of WorldExtend, organizations must first prepare their corporate application environment for the deployment process. You should assess your application requirements and WorldExtend requirements and determine how they affect your organization. Before you can begin your deployment, you must gain some information about WorldExtend and perform some preparation tasks, including:

- Identifying the WorldExtend components
- Determining the WorldExtend hardware requirements
- Determining the WorldExtend software requirements
- Determining the WorldExtend network requirements
- Gathering the application attributes required by WorldExtend

The following sections provide you with some WorldExtend information and an easy-to-use checklist for preparing your application environment for WorldExtend.

WorldExtend IronDoor Products

IronDoor offers three (3) remote access products to enable your users to work remotely and support a centralized computing environment. Both products utilize the IronDoor Security Platform to ensure the highest level of security for your network and data resources.

1. **IronDoor VPN** – IronDoor VPN allows you to create encrypted SSH VPN tunnels between remote clients and your internal applications and data. No VPN hardware is required, just an IronDoor Agent and the WorldExtend Web Portal.
2. **IronDoor Desktop Access** – IronDoor allow your user to access their Windows and Linux based desktops from anywhere in the world.
3. **IronDoor Application Delivery** – The IronDoor Application Delivery platform enables your users to execute business-critical, server-based applications from anywhere in the world. These users can only view and execute the applications the IronDoor administrator assigns to them.

IronDoor Components

The IronDoor Security Platform consists of four (4) main components. This component-based, security platform gives you the flexibility and scalability you require for a complete enterprise solution.

1. **WorldExtend Server** – The WorldExtend Server is a managed, back-end computing environment that provides all of services necessary to enable secure remote access to your data and applications. It host the web services that the IronDoor Agent uses to initiate and validate incoming connections. The service is hosted in the WorldExtend datacenters, thus relieving you of the installation requirements and resources.
2. **WorldExtend Administrator** – The WorldExtend Administrator allows you to manage your remote users, applications, computers and IronDoor Agents. You can monitor real time user activity and connections. It is accessed via the WorldExtend Web Portal.
3. **WorldExtend Web Portal** – The WorldExtend Web Portal is your company-specific website where your users will launch their IronDoor VPN connections, managed applications and managed desktops.
4. **IronDoor Agent (IDA)** – The IronDoor Agent (IDA) is a Windows Service that acts as a secure gateway between remote clients and internal endpoints such as file systems, email servers, desktops and application servers. Just one IDA needs to reside on any Windows 2000, 2003, or XP computer within your network to provide access to any internal endpoint within that network.

The subcomponents are:

- a. **Connection Tester** – The Connection Tester allows you to enter your IDA port range and determine if your firewall is permitting access.

- b. **IronDoor Agent Configurator** – The IronDoor Agent Configurator enables you to tune your IDA for your needs. In most cases, the IDA is self-configurable so you will not need to use the IDA Configurator often.

- c. **IronDoor Updater** – The IronDoor Updater service communicates with the WorldExtend Server to determine if there are any software updates for the IronDoor Agent. Based on your settings within the WorldExtend Administrator, the Updater service will apply the updates when you want.
- d. **IronDoor Agent Monitor** – The IronDoor Agent Monitor allows you to manage the IronDoor Agent and IronDoor Updater services and apply software updates to the IronDoor Agent. The monitor runs as an icon in your Windows desktop systray area.

IronDoor Agent Requirements

This section lists the hardware, software, and network requirements for running the WorldExtend IronDoor Agent. Check entries as completed.

Hardware

You can install the WorldExtend IronDoor Agent (IDA) on the same Windows 2000 or Windows 2003 server that you are going to use to run your applications.

The following are the minimum requirements to run the IDA.

- 800 MHz Pentium III processor better
- At least 256 megabytes (MB) of RAM. 512 MB recommended

Software

The IDA currently requires the following operating systems and software:

- Windows XP SP2 or higher, Windows 2000 Server SP3 or higher, Windows Server 2003 SP1 or higher
- The Microsoft .NET Framework version 2.0. Available at: <http://support.microsoft.com>

Network

The IDA currently requires the following network and firewall configuration:

- An external TCP/IP address accessible over the public Internet. This does not have to be a “static” IP address.
- For an IDA configured as a Master or 0-Listener:
 - A firewall definition that makes “n” sequential ports available for the internal TCP/IP address assigned to the server that is hosting the IDA. The IDA will randomly select one of the “n” port numbers when establishing a WorldExtend connection.
Example: *Open 6 ports in the firewall, with port numbers 9000 through 9005 for IP 192.168.3.2*
 - A firewall definition that NAT's the external TCP/IP address to the internal TCP/IP address for those ports.
- For an IDA configured as a Secondary, no firewall changes are required.
- Run the WorldExtend Connection Tester to verify the network configuration.
- Log into the WorldExtend Administrator, display the IronDoor Agent Details form for the IDA, and use the Ping tool to test the connection from outside your network.

IronDoor VPN Requirements

This section lists the hardware, software, network, and application requirements if you are using IronDoor VPN Tunnels. Check entries as completed.

Hardware

Server

Within your corporate computing environment, you must install the WorldExtend IronDoor Agent (IDA). Please review the IDA requirements.

IDA hardware requirements completed.

For the internal endpoints of your IronDoor VPN (e.g. an email server, Intranet site, FTP server, etc.), you must adhere to the system requirements of the particular endpoint.

Endpoint hardware requirement completed.

Client

The IronDoor VPN runs as an ActiveX control within the end user's Microsoft Internet Explorer web browser. Please review the system requirements for Internet Explorer at:

<http://www.microsoft.com/windows/ie/ie6/evaluation/sysreqs/default.msp>

However, we recommend the following for your remote end users:

700 MHz Pentium processor or better

128 MB of RAM

Software

Server

Within your corporate computing environment, you must install the WorldExtend IronDoor Agent (IDA). Please review the IDA requirements.

- IDA software requirements completed.

For the internal endpoints of your IronDoor VPN (e.g. an email server, Intranet site, FTP server, etc.), you must adhere to the system requirements of the particular endpoint.

- Endpoint software requirement completed.

Client

The IronDoor VPN runs as an ActiveX control within the end user's Microsoft Internet Explorer web browser:

- Windows XP SP2 or higher, Windows 2000 SP3 or higher or Windows Server 2003 SP1 or higher
- Microsoft Internet Explorer 6.0 SP1 or higher.
- Internet Explorer options that allow signed Active X controls to be loaded. All WorldExtend ActiveX controls are digitally signed with our corporate certificates.
- If the Local Destination address of any of your IronDoor VPN tunnels will be a loopback address something other than 127.0.0.1 (e.g. 127.0.0.2), your Windows XP SP2 clients will require the Microsoft fix specified in Knowledge Base article KB884020.

Network

Server

Within your corporate computing environment, you must install the WorldExtend IronDoor Agent (IDA). Please review the IDA requirements.

- IDA network requirements completed.

For the internal endpoints of your IronDoor VPN (e.g. an email server, Intranet site, FTP server, etc.), you must adhere to the system requirements of the particular endpoint.

- Endpoint network requirement completed.

Client

The IronDoor VPN Active X control within Internet Explorer requires:

- An Internet connection to your WorldExtend Web Portal.
- A connection to your IronDoor Agent via either the Internet or internal LAN.
- Personal firewall definitions that allow outbound connections to the port range established in your IronDoor Agent definition within the WorldExtend Administrator.
- In order to use IronDoor VPN for Windows File Sharing, you must create a channel for port 139 (445 for Vista) and point the channel at a Microsoft Loopback adapter address. When the “Automatically install IronDoor Loopback Adapter” box is checked on you OU definition within the WorldExtend Administrator, the WorldExtend Initialization Control will automatically install a loopback adapter on the end user’s computer when they access the Web Portal for the first time. This installation will only occur if the user is logged into their computer with administrative authority. If you need to do this manually, please refer to Appendix B of this document.

Application/Desktop Publishing Requirements

This section lists the hardware, software, network, and application requirements for running applications using IronDoor. Check entries as completed.

Hardware

Server

Within your corporate computing environment, you must install the WorldExtend IronDoor Agent (IDA). Please review the IDA requirements.

IDA hardware requirements completed.

The specific hardware requirements for your corporate application environment are too complex for the scope of this document. Each individual software application has its own computing requirements; as does, the remote access infrastructure you plan to implement such as Microsoft Terminal Services, VNC, Telnet servers and FTP servers.

Please refer to your application vendor's documentation and website for capacity planning details.

- For Microsoft Terminal Services, visit <http://www.microsoft.com/windowsserver2003/technologies/terminalservices/default.aspx>
- For VNC, refer to the VNC vendor or the Linux operating system vendor.
- For Telnet, refer to the Telnet vendor or the operating system vendor.
- For FTP, refer to the individual FTP server vendor

Once you have reviewed the capacity planning requirements for your environment, check the box below.

Application hardware requirements completed.

Client

The various IronDoor remote access interfaces run as an ActiveX controls within the end user's Microsoft Internet Explorer web browser. Please review the system requirements for Internet Explorer at: <http://www.microsoft.com/windows/ie/ie6/evaluation/sysreqs/default.aspx>

However, we recommend the following for your remote end users:

- 700 MHz Pentium processor or better
- 128 MB of RAM

Software

Server

Within your corporate computing environment, you must install the WorldExtend IronDoor Agent (IDA). Please review the IDA requirements.

- IDA software requirements completed.

The specific software requirements for your corporate application environment are too complex for the scope of this document. Each individual software application has its own computing requirements; as does, the remote access infrastructure you plan to implement such as Microsoft Terminal Services, VNC, Telnet servers and FTP servers.

Please refer to your application vendor's documentation and website for capacity planning details.

- For Microsoft Terminal Services, visit <http://www.microsoft.com/windowsserver2003/technologies/terminalservices/default.msp>
- For VNC, refer to the VNC vendor or the Linux operating system vendor.
- For Telnet, refer to the Telnet vendor or the operating system vendor.
- For FTP, refer to the individual FTP server vendor

Once you have reviewed the capacity planning requirements for your environment, check the box below.

- Application software requirements completed.

Client

The various IronDoor remote access interfaces run as an ActiveX controls within the end user's Microsoft Internet Explorer web browser. Here are the software requirements for IronDoor:

- Windows XP SP2 or higher, Windows 2000 SP3 or higher or Windows Server 2003 SP1 or higher
- Microsoft Internet Explorer 6.0 SP1 or higher.
- Internet Explorer options that allow signed Active X controls to be loaded. All WorldExtend ActiveX controls are digitally signed with our corporate certificates.

Network

Server

Within your corporate computing environment, you must install the WorldExtend IronDoor Agent (IDA). Please review the IDA requirements.

- IDA network requirements completed.

The specific network requirements for your corporate application environment are too complex for the scope of this document. Each individual software application has its own computing requirements; as does, the remote access infrastructure you plan to implement such as Microsoft Terminal Services, VNC, Telnet servers and FTP servers.

Please refer to your application vendor's documentation and website for capacity planning details.

- For Microsoft Terminal Services, visit <http://www.microsoft.com/windowsserver2003/technologies/terminalservices/default.mspx>
- For VNC, refer to the VNC vendor or the Linux operating system vendor.
- For Telnet, refer to the Telnet vendor or the operating system vendor.
- For FTP, refer to the individual FTP server vendor

Once you have reviewed the capacity planning requirements for your environment, check the box below.

- Network requirements completed.

Client

The IronDoor Active X controls within Internet Explorer require:

- An Internet connection to your WorldExtend Web Portal.
- A connection to your IronDoor Agent via either the Internet or internal LAN.
- Personal firewall definitions that allow outbound connections to the port range established in your IronDoor Agent definition within the WorldExtend Administrator.

About Us

About WorldExtend, LLC.

Founded in 2005, WorldExtend, LLC. combines systems software expertise with practical experience in managing and operating mission-critical data centers. WorldExtend, LLC. is quickly becoming a leader in software platforms and systems that enable enterprises and service providers to successfully deploy and manage server-based computing.

About WorldExtend IronDoor

WorldExtend IronDoor™ is an advanced remote access security platform that seamlessly integrates our proprietary VPN and application delivery system, IronDoor™, with your internal computing environment to deliver fast, simple and secure access to information and applications. WorldExtend IronDoor enables administrators to quickly provide users access to applications and data from anywhere in the world using only their web browser.

Other sources of information

You can find more information, as follows:

WorldExtend, LLC.
131 Gaither Drive
Suite G
Mt. Laurel, NJ 08054

Web: www.worldextend.com
Email: info@worldextend.com

Phone: 866-999-7750
Fax: 856-234-6766