iTivity™

Internet-based remote
administration and support

User Guide

for iTivity Release 5.2

iTivity™

User Guide Edition - June 2009

iTivity Release 5.2

ACKNOWLEDGEMENTS

Licensing Information for OpenSSL Library

DIRECTLY TO DEATH, PERSONAL INJURY, OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE (“HIGH-RISK ACTIVITIES”). WIDGET WORKSHOP SPECIFICALLY DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS FOR HIGH-RISK ACTIVITIES.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED. IN NO EVENT SHALL
THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Visit the ACME Labs Java page for up-to-date versions of this and other fine Java utilities: http://www.acme.com/java/

The VNC system is free software; you can redistribute and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA, 02111-1307, USA.

For the latest source code, please check http:www.DevelopVNC.org/ or send email to feedback@developvnc.org.

If the source code for the VNC system is not available from the place whence you received this file, check http:www.uk.research.att.com/vnc or contact the authors on vnc@uk.research.att.com for information on obtaining it

Copyright Information for vncreflector:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR

SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Some iTivity components are available under the GPL. You may obtain the source code for those components here:

FTP://ftp.tridia.com/pub/gpl/

CONTENTS

Welcome to iTivity™

Thank you for choosing iTivity™, a powerful Internet-based solution for system administration and remote support.

At Tridia, our mission is to always exceed our customers' expectations by providing the absolute best software products backed by outstanding technical support and customer service. We take this mission very seriously and invite you to send your comments, compliments, or complaints to service@tridia.com.

WHAT IS ITIVITY?

iTivity is a software product that allows system administrators to deploy remote administration and viewing tools either within an intranet or safely across firewalls over the Internet. Deployment is simple; you can create custom installation files using a web-based wizard, and you can provide for one-click installation of end-user components from an e-mail or web page.

The iTivity solution is extremely economical because of its flexible licensing mechanism. The iAgent software that allows computers to be viewed or controlled remotely is distributed free of charge. iAgents can be downloaded and installed to an unlimited number of computers. You pay only for the number of connections that you need at a given time.

ITIVITY FEATURES

iTivity provides administrators and support engineers with tools to:

- View and remotely control Windows and UNIX/Linux computers
- Transfer files between remote computers
- Manage help desk requests
- Chat directly with users
- Control remote systems through TELNET

All connections are encrypted and make use of configurable authentication schemes including NTLM, LDAP or simple local password.

iTIVITY COMPONENTS

Figure 1 illustrates the major components of iTivity in a simple configuration used for remote support.

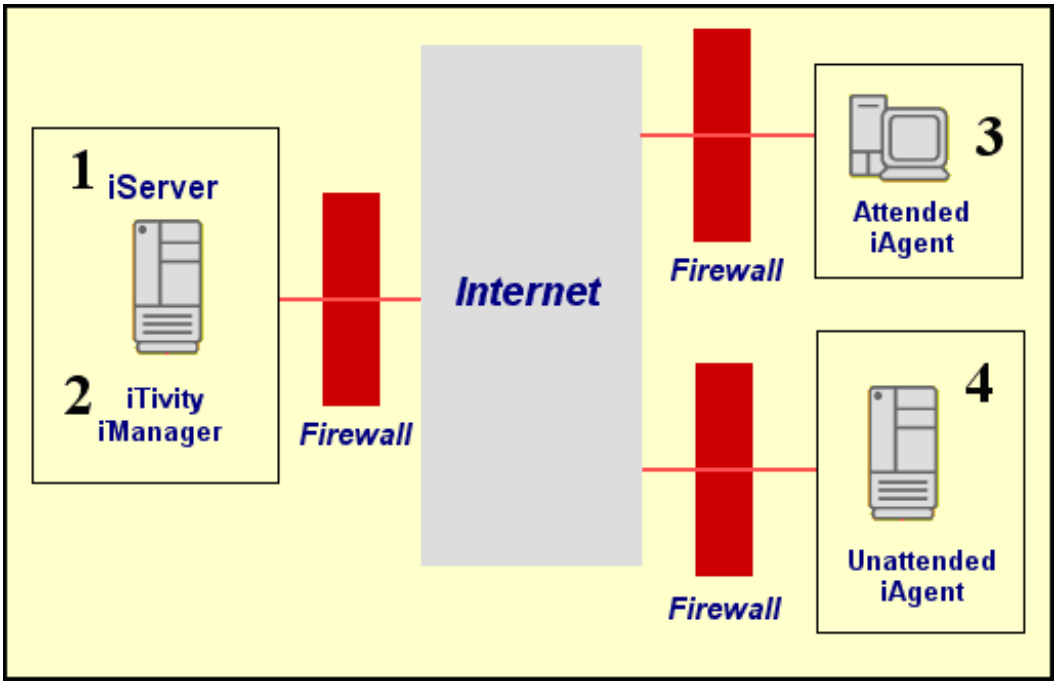


Figure 1: iTivity Components in a Remote Support Scenario

1. The **iServer** is the main engine of iTivity. The iServer creates and coordinates secure connections using 2048-bit encryption. The iServer software is available in Widows and Linux versions.

2. The **iTivity iManager** provides the interface for administrators and support personnel to view and manage remote computers and servers. The iTivity iManager can be installed on the same

computer as the iServer software or on another computer, either within or outside a firewall.

3. The **Attended iAgent** allows users of Windows computers to connect to an iServer and request support. The support request is then displayed in the iTivity iManager. The Attended iAgent also allows users to chat with an administrator who responds to their help request.

4. The **Unattended iAgent** provides for remote viewing and administration of Windows or UNIX/Linux systems. This iAgent provides a persistent, "always-on" connection. If the connection is lost, the iAgent automatically attempts to reconnect.

USING iTIVITY SECURELY OVER THE INTERNET

iTivity makes it possible to safely view and control remote computers behind firewalls.

Since the iServer only accepts secure (encrypted) connections through a user-configurable port, it can be placed safely in front of a firewall, in the network area often called a DMZ (Demilitarized Zone).

Alternately, the iServer can be placed behind a firewall. In this case, the administrator would need to open a single "pinhole" to allow iServer connections. Or, the administrator can configure the iServer to use port 443 (HTTP), which in most firewalls allows traffic by default. In this case, the firewall does not need to be reconfigured.

The iServer can accept connections from any iAgent computer behind the firewall, as long as the firewall allows outgoing TCP/IP connections.

Users running iTivity iManager, located inside or outside your network, can connect to the iServer, which in turn allows them to view its connected agents.

Figure 2 illustrates one typical usage scenario. An administrator with iTivity iManager installed on a laptop or home PC (1) uses the iServer to remotely view and control any number of Windows computers inside the firewall (2).

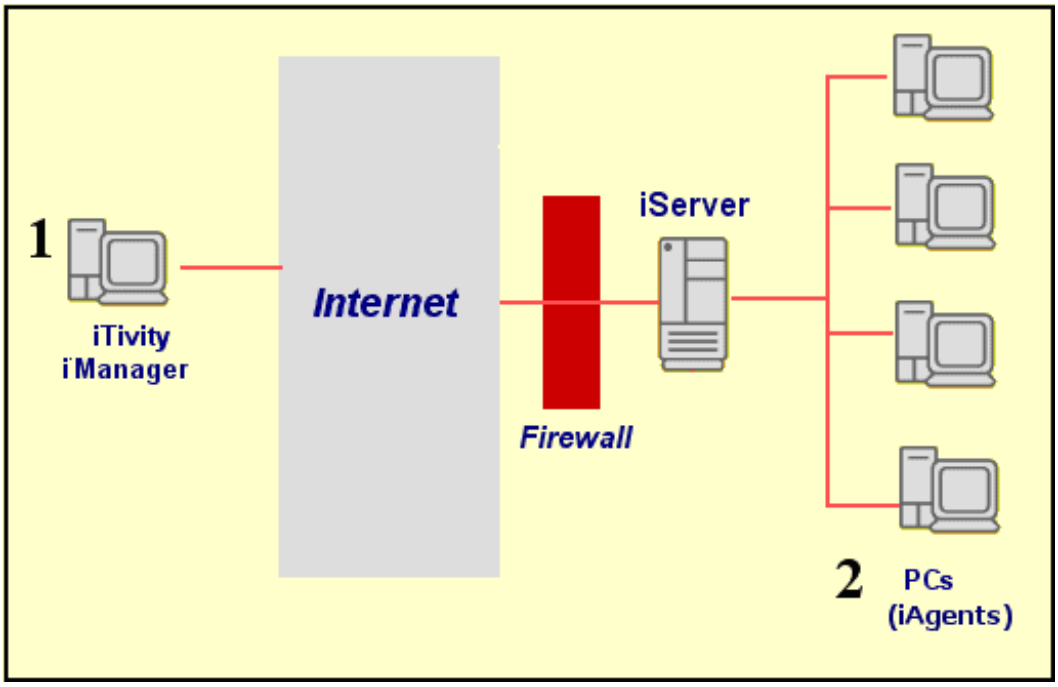


Figure2: iTivity Remote Support Example

DEPLOYING THE ITIVITY IAGENTS

Administrators can easily deploy iTivity iAgents to as many computers as needed. Customization is easy.

The administrator can place the iAgent distribution files on a web server, then send an e-mail containing a link for downloading the iAgent. The user receives the e-mail, clicks on the link, and the iAgent is downloaded and installed, safely and securely.

The administrator can configure how the iAgent will run once installed by setting configuration parameters in the HTML page that is used for downloading. This strategy allows for a uniform distribution policy. Exceptions can be made simply by copying and renaming the HTML file, then changing the configuration settings it contains. A new

customized iAgent can then be deployed by advertising the URL to the desired users.

The iAgents can also be installed via distribution EXE files downloaded from the Tridia web site. You can also build custom installation files for your iTivity modules using a simple wizard interface.

For More Information

For instructions on

- Installing the iAgents on Windows, see *Chapter 5*.
- Installing the Unattended iAgent on UNIX/Linux, see *Chapter 8*.
- Building Custom Installers, see *Appendix B*.

For additional information on planning and deploying iTivity, especially in enterprise environments, see the *iTivity Deployment Guide*.

iTIVITY LICENSING AND CONNECTIONS

This section contains information about the iTivity licensing. This information applies to the licensing of the iServer, as explained in *Sections 2.4* (Windows) and *2.10* (Linux).

iTivity licensing is based on an allowed number of iServer connections ("concurrent connections"). A licensed connection is consumed whenever an iManager connects to an iAgent for viewing or remote control. You can install any number of iManagers and iAgents. Your licensed connections are only consumed while an active connection exists between an iManager and iAgent.

Note: You can also license iAgents separately from the iServer, as described in sections 6.3.1 and 7.1.3. When an iAgent is licensed separately, its connection to an iServer does not count as one of the connections allowed by the iServer license. Contact Tridia for more information on this option.

USING THIS GUIDE

The User Guide has been organized by product module and function for easy use.

- *Chapter 1, System Administration with iTivity*, provides technical information to help administrators understand, plan, and deploy the iTivity software.
- *Chapter 2, Installing and Running the iServer*, provides complete information on the iServer component.
- *Chapter 3, Installing and Running the iTivity iManager*, contains setup and quick start information on the iManager component.
- *Chapter 4, Using the iTivity iManager*, provides complete instructions on all program menus and options.
- *Chapter 5, Installing the iTivity iAgents on Windows*, explains how to install and configure the Attended iAgent and Unattended iAgent on Windows.
- *Chapter 6, Using the Attended iAgent on Windows*, explains the iAgent features available to end-users for getting help.
- *Chapter 7, Using the Unattended iAgent on Windows*, explains the menu options available on the computer where the Unattended iAgent is installed.
- *Chapter 8, Installing and Running the Unattended iAgent on UNIX/Linux*, explains how to deploy, license and run the Unattended iAgent and related software on Linux and UNIX systems.
- *Appendix A, Using Silent Install for Automated Installation*, explains how to automate the installation of iTivity modules on Windows systems.

- *Appendix B, Creating Custom Installers*, explains how to create customized installation files for the iTivity modules on the Tridia support web site.

A *Glossary* and *Index* are also included.

THE iTIVITY DEPLOYMENT GUIDE

The *iTivity Deployment Guide* is intended for technical staff who will plan, install and configure the iTivity system. This guide includes details on system requirements, configuration recommendations and troubleshooting tips.

While some of the information applies to any iTivity implementation, the focus of this guide is on large, enterprise-scale deployments.

THE RELEASE NOTES

The "Readme" file containing the Release Notes for this version is located under **C:\Program Files\iTivity\README.txt**. (on Windows computers). These Release Notes are very important, since they contain specific information concerning the current release of this software.

The information contained in the Release Notes is typically not found in the User Guide. In many cases, the Release Notes information supersedes the information in the User Guide. Therefore, it is highly recommended that you read the Release Notes completely before installing or using iTivity.

iTIVITY PRODUCT SUPPORT

If you have a question or problem with the iTivity product, we encourage you to first review the User Guide, online help, and the www.tridia.com Web site for your solution.

If you still cannot find an answer, please contact Tridia directly for product support.

- Web site: support.tridia.com
- Telephone: 770-428-5000
- Toll free: 800-582-9337
- Fax: 770-428-5009

1 System Administration with iTivity

This chapter provides technical information for administrators to help you understand, plan, and deploy the iTivity software.

1.1 ENCRYPTION

All connections between the iTivity components are encrypted at all times, unless configured otherwise by the system administrator. The encryption used is 2048 bit RSA asymmetric key exchange with AES encryption using 256 bit bulk/session/symmetric keys.

When a connection is first established, the key exchange takes place and is done with a high level of security. Once the key exchange takes place, a lower (yet secure) encryption level is used in order to permit fast communication.

With the secure connection in place, FTP, chat, TELNET, remote control, and help desk requests are all safely encrypted.

1.2 AUTHENTICATION

1.2.1 Authentication Levels

Two levels of authentication are supported for iTivity connections, both of them configurable.

As shown in Figure 3, when attempting to access an iServer, a user of iTivity iManager must authenticate against the iServer (1). Then, when attempting to open a connection to view an iAgent computer attached to the iServer, the user can be required to authenticate a second time for that individual iAgent computer (2).

Note: No authentication is required by an iAgent connecting to the iServer.

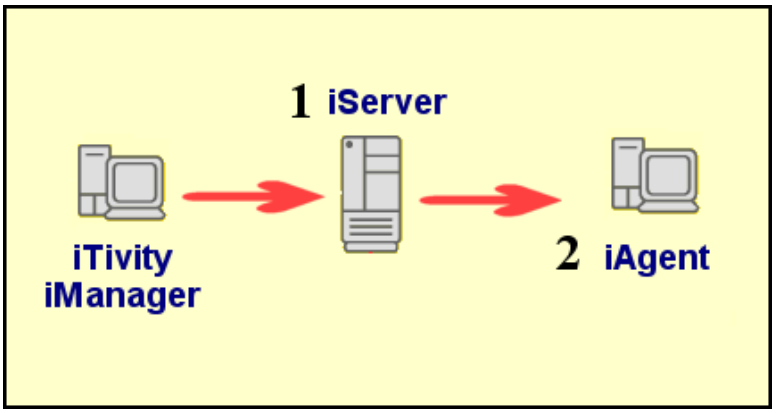


Figure 3: iTivity Authentication Levels

1.2.2 Supported Authentication Methods

Both authentication levels support these methods on Windows systems:

- NTLM
- LDAP
- Simple Password
- No Authentication Required

On UNIX/Linux systems, authentication is controlled by system user name and password. The UNIX/Linux permission group is controlled by the iServer and Unattended iAgent configuration files. See *Section 2.9, Configuring the iServer on Linux*, and *Section 8.4, Configuring the Unattended iAgent on UNIX/Linux.*

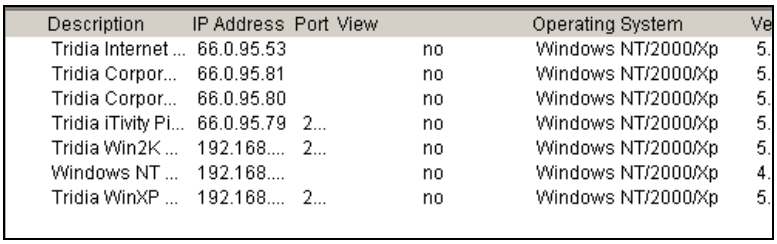
1.2.3 Authentication Strategies for the iServer

Consider the information in this section when deciding on the authentication method to use for your iServer.

Note: This section discusses iServer authentication on Windows. For information on the Linux iServer, see *Section 2.9, Configuring the iServer on Linux.*

WHY USE AUTHENTICATION FOR THE ISERVER?

Tridia recommends requiring authentication on the iServer because iTivity iManager displays sensitive information when it connects to an iServer.



Description	IP Address	Port	View		Operating System	Ve
Tridia Internet ...	66.0.95.53			no	Windows NT/2000/Xp	5.
Tridia Corpor...	66.0.95.81			no	Windows NT/2000/Xp	5.
Tridia Corpor...	66.0.95.80			no	Windows NT/2000/Xp	5.
Tridia iTivity Pi...	66.0.95.79	2...		no	Windows NT/2000/Xp	5.
Tridia Win2K ...	192.168....	2...		no	Windows NT/2000/Xp	5.
Windows NT ...	192.168....			no	Windows NT/2000/Xp	4.
Tridia WinXP ...	192.168....	2...		no	Windows NT/2000/Xp	5.

This information includes user names, computer IP addresses, operating system versions and so on. All of this information could potentially be useful to hackers.

NTLM AND LDAP

Both NTLM and LDAP provide a centralized user database. These authentication methods support permission groups that allow access to be granted precisely to one or more users or groups. Having a central user database can be a great advantage when managing staff turnover.

When **NTLM** is selected as the authentication method (during installation of the iServer), a Windows user group called *iTivityServerUsers* is created. Administrators can then add users to this group to allow them access to the iServer. Later, by removing a user or users from the iTivityServerUsers group, the administrator can render that user incapable of connecting to the iServer. Since iAgent computers can only be viewed through an iServer, they are protected from

unauthorized remote viewing. For Windows networks, Tridia recommends NTLM for this reason.

Under **LDAP**, the permission group is specified through the "ldapGroupURL" or authorization group object. This LDAP object is a group containing users or groups that are allowed to access the iServer. By adding or removing users or nested groups, you can easily and centrally control which LDAP users have permission to access iAgent systems via the iServer.

SIMPLE PASSWORD

As the name implies, the 'Simple Password' authentication method has the advantage of simplicity. For administrators who feel they have a secure environment or do not have an NTLM or LDAP background, the Simple Password may be chosen.

A possible drawback to using Simple Password is when staff changes occur. An administrator must then change the password on the iServer and reload the iServer Settings. (You can reload the settings on the iServer by choosing **Start > Programs > iTivity > Administrative Tools > Reload iTivity iServer Changes.**)

NO AUTHENTICATION REQUIRED

This option is provided for rare cases when an administrator might decide it is advantageous to allow access to the iServer without authenticating.

1.2.4 Authentication Strategies for iAgent Computers

Consider the information in this section when deciding on the authentication method to use for iAgent computers.

An *iAgent computer* is a machine with one of the iTivity iAgents installed. An iAgent computer must be connected to an iServer in order for it to be viewable by users of the iTivity iManager.

Various authentication strategies are available on Windows. Tridia recommends that a uniform authentication policy be established by the system administrator, to make it easy to remember and enforce.

For UNIX/Linux systems, Unattended iAgent authentication is controlled by system user name and password. The permission group is controlled by the Unattended iAgent configuration file. See *Section 8.4, Configuring the Unattended iAgent on UNIX/Linux*.

NTLM AND LDAP

The advantage of NTLM and LDAP is their use of a central user database.

- Under **NTLM**, each iAgent type has its own permission group. By default the Unattended iAgent uses **iTivityUnattendedUser***s* and the Attended iAgent uses **iTivityAttendedUsers**.
- Under **LDAP**, users are defined by the ldapGroupURL object.

With the central database, administrators can quickly prevent users from viewing computers remotely simply by removing them from the relevant user group (in NTLM) or object (LDAP). For example, if a user is no longer with the organization, or is no longer assigned to a help desk role, the administrator can go to the Domain Controller and remove that user from the permission group. The individual will no longer be able to view any iAgent through iTivity iManager.

One critical issue to keep in mind when using NTLM or LDAP for iAgent authentication is the context of the iAgent computer. The authentication server used by the iAgent computer will likely be local to that system. Therefore, the remote user will need a user id and password that is valid for the authentication context (domain or directory) of the iAgent system.

SIMPLE PASSWORD

With the Simple Password method, each iAgent computer has its own password, whether unique or otherwise. Administrators might choose the Simple Password method for iAgent authentication for several reasons:

- You might want to give the end user control over who can connect to their computer, by having them set their own Simple Password. Of course, the administrator or help desk user will have to be told what the password is before they could connect through iTivity iManager.
- The Simple Password method offers the advantage of simplicity. Also it might be preferred by an administrator who does not have an NTLM or LDAP background or does not have domain controllers or an LDAP server on the network.
- VARs (Value Added Resellers) might choose Simple Password if they need to support many users at widely dispersed locations. In this case, the NTLM or LDAP methods may be too difficult to implement. Or if the supported users work for different organizations, those organizations probably would not want to share authentication information. Note that it is perfectly possible for remote offices to use NTLM or LDAP. The NTLM or LDAP authentication server would simply have to reside on the same network as the iAgent computer.

NO AUTHENTICATION REQUIRED

Finally, the No Authentication Required option might be chosen to make iAgent computers more quickly accessible for viewing, provided that these computers do not require a secure login. Tridia does not recommend this option except in rare special circumstances.

USING MULTIPLE AUTHENTICATION METHODS

Another strategy is to use different authentication methods for different iAgent computers.

For example, a group of computers in the Accounting Department at a corporate headquarters might be assigned NTLM or LDAP authentication, while computers in remote field offices might use Simple Password. iTivity supports multiple methods to allow system administrators the greatest flexibility in configuring their networks.

1.2.5 Advanced Authentication

Starting with iTivity version 4.6, administrators can implement a more detailed security scheme. By setting up *permission groups* on the iServer and corresponding *support domains* on iAgent computers, you can limit users of iTivity iManager to viewing only a subset of the iAgents connected to your iServer. You can also precisely define the level of permissions these users have.

For complete information on advanced authentication, see the *iTivity Deployment Guide.*

1.3 CONFIGURING THE ISERVER ON THE NETWORK

1.3.1 Server Selection

The iServer software can be installed on a dedicated server or on a server already used for other functions. To ensure fast responses (low latency) the software should be installed on a lightly-loaded system or a dedicated server. Installing the iServer software on a system that is already experiencing heavy CPU or I/O loads will cause remote control sessions to respond too slowly.

1.3.2 iServer Placement

Some customers choose to set up the iServer in an area outside the firewall that is directly accessible via the Internet. (This area is often called the DMZ.) Since DMZ systems are also directly accessible from the organization's local network, this option may be the simplest to implement.

The iServer can also be placed behind a firewall, as long as port forwarding is enabled for the connection port types needed.

When port forwarding is used, the iAgents and iTivity iManager users must specify the public IP address of the firewall instead of the private IP address of the iServer system.

1.3.3 Port Configuration

In order for the iServer to be accessed and used via the Internet, there must be publicly visible Internet access to one or both of the connection ports.

- The *iAgent registration port* allows iAgent systems to register themselves with the iServer for remote access. It defaults to TCP port 23800.
- The *remote user view port* allows iTivity iManager users to view and control iAgent computers. This port defaults to TCP port 25800.

If only the iAgent registration port is accessible to the Internet, then iTivity iManager users can view iAgents over the Internet, but they themselves must be located on the iServer's local network.

If only the remote user view port is accessible to the Internet, then iTivity iManager users can connect from anywhere, but they can only access iAgent systems that reside on the same local network as the iServer.

To allow both iAgents and iTivity iManager users to connect from anywhere, configure both ports to be accessible via the Internet.

CHANGING THE IAGENT REGISTRATION PORT FOR ADDED SECURITY

For those customers deploying the iTivity iAgents into end-user environments with tight security restrictions, it may be helpful to change the iAgent registration port to TCP port 443. This port is more likely to be supported for outbound connections from the end user network.

This change must be implemented in both:

- The iServer configuration (on Windows: HKLM\Software\Tridia\iTivity\connector_ia\iasServerPort)
- The iAgent software setup, via the installation setting "varItivityConnectPort". See *Section 5.4, Editing the iAgent HTML Files* for information.

If these settings do not match, then the iAgent system will not be able to register and therefore will not appear in the iServer's list of connected computers in the iTivity Manger. If the iServer is positioned behind a firewall, then the port forwarding must accept the iAgent registration from port 443 on the public IP address of the firewall.

1.4 USING WEB-BASED INSTALLATION

1.4.1 Distributing iAgents via E-Mail

One of major advantages of iTivity is the ease of deployment of the iTivity iAgents. Through web-based, one-click install, system administrators can easily deploy the Attended iAgent and Unattended iAgent onto as many Windows computers as needed.

First, install the iAgents to a web server by installing the iTivity Support Module as described in *Section 5.3*. System administrators can then configure options for how the iAgents will work, simply by editing parameters in the delivered HTML files. This can include having the iAgent immediately connect to your specific iServer. See *Section 5.4, Editing the iAgent HTML Files,* for information.

Or, as an alternative, build custom installers for the iAgents on the Tridia support site, as explained in *Appendix B*. You can configure these installers with the options you need and place them on a web or ftp server for users to access.

After the iAgents are configured for deployment from a web or ftp server, the administrator can simply send an email to all users who need to have a particular iAgent installed. This email would contain instructions and a link to the proper download file.

When the email is received, the end-user simply clicks the link and the configured iTivity iAgent is installed automatically.

1.4.2 Other Distribution Options

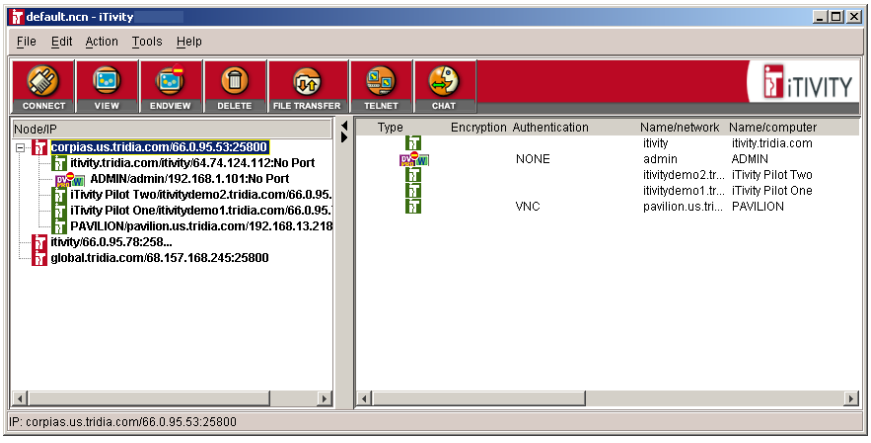
Email is not the only means of deployment. Administrators can also create their own web pages that in turn point to an iTivity iAgent deployment page. Users can click on links on these pages and the same installation process takes place as described above.

In an intranet situation, the intranet server might feature a support page. This page could list the different iTivity iAgent versions available and allow the end-user to choose the one that matches their situation.

Finally, if you are supporting computers without e-mail or web access, you can install the iAgents by copying the installation files over the local network.

1.5 iTivity iManager

The iTivity iManager provides the main user interface for administrators and support personnel. The iManager main window displays the configured iServers and any iAgent computers currently connected to them. While some organizations have only one iServer on their network, the iTivity iManager can connect to and list any number of iServers.



iTivity iManager stores its list of iServers in a **.ncn file**. You can add all of your iServers to this file, or you can have multiple files with different sets of iServers. By default, the iManager loads its last used '.ncn' file.

One good strategy is to store the .ncn file in a network directory. This allows all users of iTivity iManager to share the same iServer list.

A key feature of iTivity iManager is the Windows Explorer-like interface in the left pane of the main window. When you connect to an iServer, the list expands to show all iAgent computers currently connected to that iServer.

Also the right pane is populated with more detailed information about each registered iAgent computer, such as the operating system version, release number, service pack, etc. This information can be of value to a diagnostician attempting to solve a problem.

Description	IP Address	Port	View		Operating System	Ve
Tridia Internet ...	66.0.95.53			no	Windows NT/2000/Xp	5.
Tridia Corpor...	66.0.95.81			no	Windows NT/2000/Xp	5.
Tridia Corpor...	66.0.95.80			no	Windows NT/2000/Xp	5.
Tridia iTivity Pi...	66.0.95.79	2...		no	Windows NT/2000/Xp	5.
Tridia Win2K ...	192.168....	2...		no	Windows NT/2000/Xp	5.
Windows NT ...	192.168....			no	Windows NT/2000/Xp	4.
Tridia WinXP ...	192.168....	2...		no	Windows NT/2000/Xp	5.

Similar information for an iAgent computer is available by right-clicking on the computer in the list and choosing **Properties** from the popup menu.

When using the iManager, remember to select the iServer or connected iAgent computer in the left pane. The menu and tool bar options generally act on the selected item.

For complete instructions on the iTivity iManager interface and features, see *Chapter 4, Using iTivity iManager*.

1.5.1 Configuring iTivity WebTunnel

Beginning with iTivity v 5.2, the **iTivity WebTunnel** feature extends the viewing and remote control capabilities of iManager.

WebTunnel discovers available network applications running on a connected iAgent computer and provides remote access to those applications through an encrypted SSL connection. When an iAgent is connected to an iManager, you can see the network applications that are available to that iAgent system. WebTunnel works for both Windows and UNIX/Linux iAgent systems.

iTivity WebTunnel supports a number of well-known applications, such as Webmin, SWAT, VNC, RDP, Telnet and CUPS, preconfigured for your convenience. In addition, you can customize the iAgent to scan and report additional HTTP, HTTPS, RDP, VNC and Telnet based applications.

HOW ITIVITY WEBTUNNEL WORKS

The iAgent software scans the TCP ports on the iAgent computer. When an active TCP port is detected, the iAgent looks at the list of default applications (and optionally custom applications that you have added). If the discovered port number matches a port number in the application list, iTivity tunnels the application port.

A user running iManager sees the tunneled applications in the list, under the name of the connected iAgent. The user can double-click a tunneled application to begin a remote access session. In most cases, a web browser opens on the iManager computer to provide an interface to the web application over iTivity's secure connection.

In the example below, three tunneled applications are displayed in iManager, indicated by the globe icon.

DEFAULT APPLICATION SCAN LIST

The table shows the default application scan list and ports for Windows and UNIX/Linux iAgents.

Application	**Port**
Telnet Server	Port: 23
Standard Web Server (http)	Port: 80
Secure Web Server (https)	Port: 443
Remote Desktop Server (RDP)	Port: 3389
AppleShare IP Web Admin	Port: 311
FileMaker Web Application	Port: 591
CUPS – IPP	Port: 631
SWAT	Port: 901
Dell Web Admin	Port: 1278
HP Insight Manager	Port: 2381
Ruby Web Application	Port: 3000
Powerchute Network Shutdown	Port: 3052
Oracle Secure Web Server	Port: 4443
VMWare Server Console	Port: 8222
VMWare Secure Server Console	Port: 8333
Parallels Plesk Control Panel	Port: 8443

Application	Port
Eclipse IDE	Port: 9008
Websphere Admin Console	Port: 9090
Websphere Secure Admin Console	Port: 9043
Websphere Application Server	Port: 9080
Webmin	Port: 10000
Usermin	Port: 20000
Document Search – IMNSearch	Port: 49213

ADDING NETWORK APPLICATIONS TO THE SCAN LIST

For both Windows and UNIX/Linux iAgents, you can customize the scan list to add network applications and make them viewable in iManager.

WINDOWS APPLICATIONS

The list of applications an iAgent scans for is found in the Windows system registry.

For This iAgent...	Use This Key...
Attended iAgent	HKEY_LOCAL_MACHINE\Software\Tridia\iTivity\ processor_od\
Unattended iAgent	HKEY_LOCAL_MACHINE\Software\Tridia\iTivity\ processor_rc\

To add custom applications to the list, do the following:

1. Create a new registry key:

   HKEY_LOCAL_MACHINE\Software\Tridia\iTivity\processor_od\ customAppScan_1

2. Create the following registry values under the new customAppScan_1 key:

Value	Description
port= <tcp_port_number>	**Required**. Specifies the local TCP port number the iAgent will check for the presence of the application. If there is no program, application or daemon listening on this port, the iAgent will not report the availability to the iManager. If a listening program is found, then the application or service is reported back to the iManager for access by the iManager user. **Example**: port=80
protocol= <protocol_name>	**Required**. Application protocol. Currently supported protocols include, "http", "https", "telnet", "vnc" and "rdp". For web applications, the protocol should be either "http" or "https". **Example**: protocol=http
appname=<display_ name_for_service>	**Optional but recommended.** Specifies the user readable display name of the application or service. This name should have a clear meaning to the iManager user. **Example:** appname=Standard Web Server
session=[system_ session_name]	**Optional.** Some operating systems have platform specific session labels. This setting should declare the session in which the application or service is running, if any. Typical session names would include, "tty0", "pts/4", ":4", "tcp #7", etc. This setting is optional. **Example**: session = Service
path=[application_ path]	Specifies the path to the default page or landing page for the application. Typically only used for web/http applications.

3. After adding the custom registry updates, restart the iTivity iAgent to allow the scan to detect the custom applications.

UNIX/LINUX APPLICATIONS

The list of applications a UNIX/Linux iAgent scans for are defined in the iTivity iAgent configuration file. The default path and filename is

```
/etc/iTivity/iAgent.conf
```

To add a custom application to the scan list, you create a new **customAppScan definition** in the file. Add the following entries for each application you want to add. After editing and saving the file, restart the iAgent for the changes to take effect.

Entry `Processor_rc/customAppScan_1/port=<tcp_port_number>` **Example:** `port=80` **Description**: Specifies the local TCP port number the iAgent will check for the presence of the application. If there is no program, application or daemon listening on this port, the iAgent will not report the availability to the iManager. If a listening program is found, then the application or service is reported back to the iManager for access by the iManager user.
Entry `Processor_rc/customAppScan_1/protocol=<protocol_name>` **Example:** `protocol=http` **Description:** Required. Application protocol. Currently supported protocols include, "http", "https", "telnet", "vnc" and "rdp". For web applications, the protocol should be either "http" or "https".
Entry `Processor_rc/customAppScan_1/appname=<display_name_for_service>` **Example**: `/appname=Standard Web Server` **Description:** Optional but recommended. Specifies the user readable display name of the application or service. This name should have a clear meaning to the iManager user.

Entry

`Processor_rc/customAppScan_1/session=[system_session_name]`

Example: /session=Service

Description: Optional. Some operating systems have platform specific session labels. This setting should declare the session in which the application or service is running, if any. Typical session names would include, "tty0", "pts/4", ":4", "tcp #7", etc.

Entry

`Processor_rc/customAppScan_1/path=[application_path]`

Description: Specifies the path to the default page or landing page for the application. Typically only used for web/http applications.

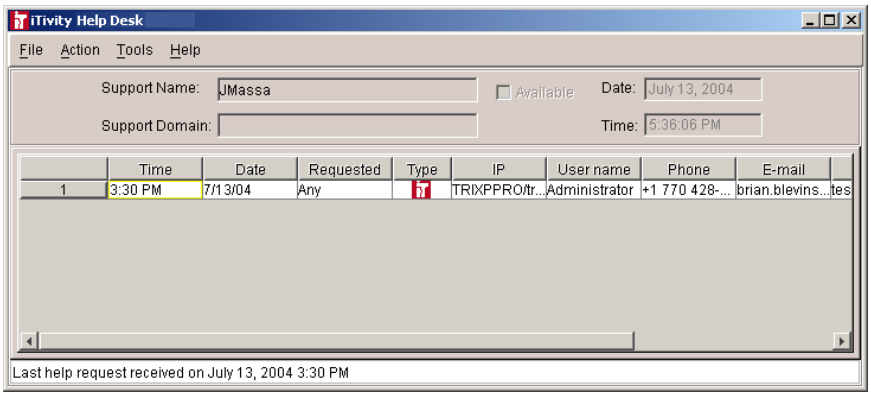
Example iAgent.conf file settings

This set of entries adds a web application called Acme Accounting Ace to the iAgent scan list.

```
# Check for Acme Accounting Ace.
Processor_rc/customAppScan_1/port=4242
Processor_rc/customAppScan_1/protocol=http
Processor_rc/customAppScan_1/appname=Acme Accounting Ace
Processor_rc/customAppScan_1/session=Service
Processor_rc/customAppScan_1/path=
```

1.6 HELP DESK WINDOW

The Help Desk window is launched from the iTivity iManager main window. With the Help Desk, administrators can easily monitor the help queue and provide help to any user at any time.



1.6.1 Using the Help Desk Window

The Help Desk window can be used by both support personnel and managers.

When you open the window it displays all users who have requested help. When their requests for help are answered, the users are automatically removed from the list. By observing the date and time help requests came in, a Help Desk manager can keep track and make sure that all requests are serviced in a timely fashion.

1.6.2 Using Announcement and Help Groups

The Help Desk feature uses the concept of Announcement’ and of help groups or 'Support Domains'.

A support person can open the Help Desk window and ‘announce’ that he or she is ready to provide help.

By filling in a **Support Domain** on the **Announce Help** dialog, the support person indicates that they belong to a specific help desk group.

For example, a help desk manager could decide to assign team members to an ‘Accounting Help Desk’ group and a ‘Marketing Help Desk’ group. Users in the accounting department could then be instructed to request help only from members of the Accounting Help Desk group.