Datum Trusted Time™ 2000 05 10 11:07:32

SyncServer™

SyncServer User Guide

Installation, Configuration, and Operation

SS v1.2, Doc v1.2

datum

Trusted Time Division

SyncServer User Guide

Installation, Configuration, and Operation

SS v1.2, Doc v1.2

DATUM INC. – Trusted Time Division
10 Maguire Road, S120, Lexington, Massachusetts, 02421
Voice: +1 (781) 372-3600 Fax: +1 (781) 372-3651
www.datum.com/tt

Datum Trusted Time™ SyncServer™

END USER LICENSE AGREEMENT

READ BEFORE USING:
THIS DOCUMENT IS A LEGAL AGREEMENT BETWEEN YOU, THE LICENSEE, AND DATUM INC.
OPENING THIS PACKAGE AND USING THE SOFTWARE CONSTITUTES ACCEPTANCE OF THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY RETURN THE ENTIRE PACKAGE, INCLUDING THE HARDWARE AND OTHER ITEMS, IN THEIR ORIGINAL PACKAGE.

1. License to the Software. In consideration of payment of the license fee, which is part of the price paid for this product, and subject to the terms and conditions of this Agreement, Datum Inc. (“Datum”) grants to Licensee a limited, revocable, non-exclusive, nontransferable license to internally use the Datum Trusted Time SyncServer software (the “Software”), in binary executable form on Datum SyncServer hardware only and solely for the purpose as provided in the accompanying documentation. Licensee may make one (1) copy of the Software for backup or archival purposes; provided, that such copy is subject to this Agreement and contains all proprietary notices. Licensee may not make any other copies of the Software or any part thereof without the prior permission of Datum.

2. Ownership of Intellectual Property. This Agreement is for licensing of the Software only, and does not transfer to Licensee any Datum Technology (as defined below). Title to, ownership of and all interests in the Datum Technology shall be and at all times remain with Datum or its designees, as applicable. All rights not expressly licensed herein are reserved to Datum. “Datum Technology” means all patents, patent applications, copyrights, copyright applications, trade secrets, knowhow, inventions, software and any other intellectual property or information developed or owned by Datum, or any corrections, bug fixes, enhancements, updates, modifications (including custom modifications) or derivative works thereof, underlying, relating to or derived from the Software or accompanying documentation.

3. Restrictions on Use. Licensee may not, and may not permit or cause others to do, any of the following:

(i) alter or modify, or create derivative works from the Software or the accompanying documentation;

(ii) publish, rent, sell, loan, lease, distribute, redistribute, transmit, license, sublicense or otherwise transfer or assign the Software or the accompanying documentation whether by operation of law or otherwise, with or without consideration, and through any means;

(iii) translate, decipher, reverse assemble, reverse compile or reverse engineer the Software, or otherwise attempt to discover any source code or underlying Datum Technology;

(iv) publish or provide any results of any test runs, accounts or other information regarding the Software to any third party without Datum’s prior written consent; or

(v) delete, remove or obscure any proprietary notices on the Software or accompanying documentation.

4. Support and Maintenance. This Agreement does not provide to Licensee any support or maintenance of the Software or any other services (such as time calibration services). In the event Licensee desires such services, it shall enter into a separate Technical Services Agreement with Datum or a third party authorized in writing by Datum.

5. Acknowledgments. Licensee expressly acknowledges that Licensee is solely responsible for any use of the Software, and such use will be entirely at Licensee’s own risk. Licensee agrees to backup data and take all appropriate measures to protect programs and data. Licensee agrees that the Software shall not be used for or in connection with any illegal purpose (including but not limited to intellectual property infringement or fraud).

6. Limited Warranty; Warranty Disclaimer.

(i) Datum warrants that it knows of no third party copyright, United States trademark, trade secret, or United States patent that is infringed by the Software.

(ii) Datum warrants that the Software will perform substantially as specified in product data sheets.

(iii) Notwithstanding the foregoing, Datum shall not be responsible in any way for any portion of software prepared by or added to the Software by the Licensee or any third party.

THE FOREGOING WARRANTIES SHALL BE IMMEDIATELY VOID IN THE EVENT LICENSEE MODIFIES THE SOFTWARE OR USES THE SOFTWARE IN ANY MANNER NOT PROVIDED FOR OR PERMITTED BY THE ACCOMPANYING DOCUMENTATION AND DATUM’S PUBLISHED SPECIFICATIONS.

DATUM HEREBY EXPRESSLY DISCLAIMS ANY WARRANTY THAT LICENSEE’S USE OF THE SOFTWARE WILL BE UNINTERRUPTED OR THAT THE OPERATION OF THE SOFTWARE WILL BE ERROR-FREE OR SECURE. DATUM FURTHER DISCLAIMS ALL WARRANTIES, EXPRESS (OTHER THAN EXPRESSLY SET FORTH IN THIS SECTION 6) OR IMPLIED, RELATING TO THE SOFTWARE OR ACCOMPANYING DOCUMENTATION INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES AGAINST INFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY AND FITNESS FOR A

PARTICULAR PURPOSE. LICENSEE ASSUMES ALL RISK OF THE USE, QUALITY, AND PERFORMANCE OF THE SOFTWARE.

7. LIMITATION OF LIABILITY. IN NO EVENT SHALL DATUM OR ITS AFFILIATES, OR ANY OF THEIR DIRECTORS, OFFICERS, EMPLOYEES AND AGENTS BE RESPONSIBLE OR LIABLE FOR ANY LOST PROFITS, LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE, LOSS OF INFORMATION, LOSS OF DATA, OR ANY OTHER INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, EXEMPLARY, PUNITIVE OR OTHER DAMAGES (EVEN IF DATUM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER THEORY ARISING OUT OF OR RELATING IN ANY WAY TO THE SOFTWARE OR ANY OTHER SUBJECT MATTER OF THIS AGREEMENT. IN NO EVENT SHALL DATUM'S LIABILITY EXCEED THE AMOUNT, IF ANY, OF THE LICENSE FEES THAT LICENSEE HAS ACTUALLY PAID TO DATUM. LICENSEE'S SOLE REMEDY FOR BREACH OF THE LIMITED WARRANTY ABOVE IS TO TERMINATE THIS AGREEMENT PURSUANT TO SECTION 19.

8. Nondisclosure. Licensee shall not disclose to any third party and shall use reasonable efforts to maintain the security of any information provided by Datum to Licensee, whether verbal or in writing, that is identified as confidential or that by its nature should reasonably be understood to be confidential. This Section 8 shall not apply to information that is or becomes publicly known through no wrongful act of Licensee.

9. Indemnification. Licensee shall defend, indemnify and hold Datum harmless against any and all claims, damages, losses, costs or other expenses (including reasonable attorneys' fees) that arise directly or indirectly out of Licensee's willful misconduct or unpermitted use of the Software.

10. Nonassignability. Neither Licensee's rights nor Licensee's obligations arising under this Agreement are assignable or otherwise transferable by Licensee (whether voluntarily or by operation of law) unless Datum provides its prior written consent and the assignee agrees to be bound by this Agreement. Subject to the provisions of this Section 10, this Agreement shall inure to the benefit of and be binding upon each of the parties hereto and their respective permitted successors and assigns.

11. Government Entities. If Licensee is licensing the Software on behalf of any unit or agency of the United States Government, the following applies: The Software and any Datum Technology is provided with RESTRICTED RIGHTS. Use, duplication or disclosure by the Government is subject to restrictions as set forth in Subparagraphs (a) through (d) of the Commercial Computer-Restricted Rights clause at FAR 52.227-19 when applicable, or in Subparagraph 252.227-7013 (c)(1)(ii) of the Rights in Technical Data and Computer Software at DFARS, and in similar clauses in the NASA FAR Supplement. Contractor/manufacturer is Datum Inc., 9975 Toledo Way, Irvine, California, 92618-1605, Tel: (949) 598-7500, Fax: (949) 598-7555.

12. Applicable Law and Forum. This Agreement shall be governed by the laws of the State of California, exclusive of its choice of law rules. Each party to this Agreement hereby submits to the exclusive jurisdiction of the state and federal courts sitting in the County of Orange in the State of California for the purpose of resolving any dispute arising under or relating to this Agreement, and each party hereby waives any jurisdictional, venue or inconvenient forum objections to such courts. In any action to enforce this Agreement, the prevailing party will be entitled to costs and attorneys' fees.

13. Entire Agreement. The terms of this Agreement shall be the final expression of their agreement with respect to the subject matter hereof and may not be contradicted by evidence of any prior or contemporaneous agreement. Any modifications of this Agreement must be in writing and signed by both parties hereto. In the event that any of the provisions of this Agreement shall be held by a court or other tribunal of competent jurisdiction to be unenforceable, such provisions shall be limited or eliminated to the minimum extent necessary so that this Agreement shall otherwise remain in full force and effect and enforceable. No waiver of any breach of this Agreement shall be effective unless made in writing and signed by an authorized representative of the waiving party.

14. Equitable Relief. Licensee acknowledges and agrees that, due to the unique nature of the Datum Technology, there can be no adequate remedy at law for any breach of its obligations hereunder and such breach will cause irreparable harm to Datum, and therefore Datum shall be entitled to injunctions and other appropriate equitable relief in addition to whatever remedies it may have at law.

15. Export Controls. Licensee acknowledges that the Software may not be downloaded, transferred or otherwise exported or re-exported (i) into (or to a national or resident of) Cuba, Iran, Iraq, Libya, North Korea, Sudan, Syria or any other country to which the United States has embargoed goods; or (ii) to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Commerce Department's Table of Denial Orders. Licensee represents and warrants that he/she/it is not located in, under the control of, or a national or resident of any such country or on any such list.

16. Taxes. Licensee will pay all federal, state and local sales, personal property, ad valorem and any other taxes (but not including Licensee's income taxes) arising as a result of this Agreement.

17. Notice. Unless herein provided otherwise, any notices required or permitted under this Agreement shall be sent to the other party by registered or certified mail or by express, overnight delivery, addressed to the address on the first page of this Agreement (or at such other address previously provided in accordance with this Section 17).

18. Counterparts. This Agreement may be executed in one or more counterparts, each constituting an original, and when taken together shall be deemed one and the same instrument.

19. Termination. This Agreement shall be effective upon the date on which the Software is made available to Licensee. This Agreement may be terminated as follows: (i) by Datum, for any reason, by providing thirty (30) days advance written notice to the Licensee or (ii) by Datum immediately upon notice to Licensee in the event of any breach by Licensee of the terms of this Agreement or upon Licensee's insolvency, bankruptcy, suspension of business, assignment of assets for the benefit of creditors, voluntary dissolution, or appointment of a trustee for all or any substantial portion of Licensee's assets. In the event that this Agreement is terminated for any reason, Licensee shall not be entitled to any refund or credit of fees paid or payable hereunder. The following provisions shall survive expiration or termination of this Agreement: Sections 2, 3, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 19, 20 and 21. Upon expiration or termination of this Agreement, Licensee will immediately destroy or erase all copies of the Software and any Datum Technology and, upon Datum's request, promptly confirm destruction of same by signing and returning to Datum an "affidavit of destruction" acceptable to Datum.

20. Relationship of Parties. The parties to this Agreement are independent contractors. No joint venture, agency or partnership, express or implied, is granted under this Agreement.

21. Headings. The headings used in this Agreement are for convenience only and shall not be considered in construing or interpreting this Agreement.

DATUM INC. – Trusted Time Division
10 Maguire Road, S120, Lexington, Massachusetts, 02421
Voice: +1 (781) 372-3600 Fax: +1 (781) 372-3651
www.datum.com/tt

Datum Trusted Time™ SyncServer™

Trusted Time and SyncServer are trademarks of Datum, Inc.

TT-SYNCSERVER S100 HARDWARE LIMITED WARRANTY

In consideration of payment of the purchase price for the Trusted Time™ SyncServer™ S100 (the "SyncServer"), and subject to the terms and considerations set forth herein, Datum Inc. ("Datum") provides the following limited warranty to the original purchaser from Datum or an authorized representative of Datum ("Purchaser") of this SyncServer.

1. Limited Warranty; Warranty Disclaimer.

1.1 Parts. Subject to the terms and conditions set forth herein, Datum shall repair or replace, at Datum's sole discretion, any CRU (1.3 below), or SyncServer unit that fails to adhere to published specifications for the SyncServer for a period of two (2) years from the date of purchase of this SyncServer (the "Warranty Period"), as set forth below. Such CRUs, or SyncServer units shall be repaired or replaced on an exchange basis by either Datum or an authorized representative of Datum, in each case at the sole discretion of Datum either at Purchaser's location or a location designated by Datum.

(a) In the event warranty service involves the exchange of a CRU or SyncServer unit, the item Datum or its authorized representative replaces becomes its property and the replacement becomes Purchaser's property. The replacement may not be new, but will be in good working order and at least functionally equivalent to the item replaced. The replacement assumes the warranty service status of the replaced item.

1.2 Labor. Subject to the terms and conditions set forth herein, below, during the Warranty Period, all labor performed by Datum in connection with Datum's obligations pursuant to Section 1.1 above, shall be at no charge to Purchaser. Any labor performed by Datum after the Warranty Period shall be at the Datum's then current rates. Datum shall not be responsible for any labor performed by Purchaser or on Purchaser's behalf for replacement or repair of CRUs or SyncServer units.

1.3 Shipping. Customer shall prepay shipping charges and shall pay all duties and taxes for products

returned for warranty. Datum will pay shipping charges for the return of products to the purchaser. All returned

products must first have a return authorization number.

1.4 Customer Replaceable Units. Certain parts of Datum SyncServers are designated as "Customer Replaceable Units" or "CRUs" (e.g. memory, certain PCI Cards, or hard disk drives). In the event Datum ships a CRU to Purchaser in replacement of a defective CRU, Purchaser shall replace the defective CRU with the replacement CRU. Purchaser shall return all defective CRUs to Datum within thirty (30) days of Purchaser's receipt of the replacement CRU.

1.5 Limitations. This warranty does not apply to (a) SyncServers which have been incorrectly installed or maintained, (b) SyncServers which have been repaired or modified or used in conjunction with thirdparty equipment or software not authorized or intended by Datum, (c) SyncServers subject to unusual physical, thermal, or electrical stress, improper installation, misuse, abuse, accident or negligence in use, storage, transportation or handling, or (d) SyncServers considered consumable items or items requiring repair or replacement due to normal wear and tear (if any).

1.6 DISCLAIMER. DATUM HEREBY EXPRESSLY DISCLAIMS ANY WARRANTY THAT PURCHASER'S USE OF THE SYNCSERVER WILL BE UNINTERRUPTED OR THAT THE OPERATION OF THE SYNCSERVER WILL BE ERROR-FREE OR SECURE. DATUM FURTHER DISCLAIMS ALL WARRANTIES, EXPRESS (OTHER THAN EXPRESSLY SET FORTH IN THIS SECTION 1) OR IMPLIED, RELATING TO THE SYNCSERVER OR ACCOMPANYING DOCUMENTATION INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES AGAINST INFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. ANY TECHNICAL OR OTHER SUPPORT PROVIDED FOR THE SYNCSERVER WILL BE PROVIDED WITHOUT WARRANTIES OF ANY KIND. PURCHASER ASSUMES ALL RISK OF THE USE, QUALITY, AND PERFORMANCE OF THE SYNCSERVER. PURCHASER HEREBY ACKNOWLEDGES THAT NEITHER DATUM NOR ITS AUTHORIZED REPRESENTATIVES ARE RESPONSIBLE FOR ANY OF PURCHASER'S CONFIDENTIAL, PROPRIETARY OR PERSONAL INFORMATION CONTAINED IN A SYNCSERVER WHICH PURCHASER RETURNS TO DATUM OR ITS AUTHORIZED REPRESENTATIVE FOR ANY REASON. PURCHASER IS ADVISED TO REMOVE ALL SUCH INFORMATION FROM THE SYNCSERVER PRIOR TO ITS RETURN.

2. LIMITATION OF LIABILITY. IN NO EVENT SHALL DATUM OR ITS AFFILIATES, OR ANY OF THEIR DIRECTORS, OFFICERS, EMPLOYEES AND AGENTS BE RESPONSIBLE OR LIABLE FOR ANY LOST PROFITS, LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE, LOSS OF INFORMATION, LOSS OF DATA, OR ANY OTHER INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, EXEMPLARY, PUNITIVE OR OTHER DAMAGES (EVEN IF DATUM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER THEORY ARISING OUT OF OR RELATING IN ANY WAY TO THE SYNCSERVER OR ANY OTHER SUBJECT MATTER OF THIS AGREEMENT. IN NO EVENT SHALL DATUM'S LIABILITY EXCEED THE AMOUNT, IF ANY, OF THE PURCHASE PRICE THAT PURCHASER HAS ACTUALLY PAID TO DATUM. PURCHASER'S SOLE REMEDY FOR BREACH OF THE LIMITED WARRANTY ABOVE IS LIMITED TO DATUM'S REPAIR OR REPLACEMENT (AT DATUM'S SOLE

OPTION) OF THE SYNCSERVER OR PART THEREOF. IN THE EVENT THE REMEDIES PROVIDED FAIL OF THEIR ESSENTIAL PURPOSE, DATUM SHALL HAVE THE RIGHT BUT NOT THE OBLIGATION TO REFUND THE MONEY PAID FOR THE PARTICULAR SYNCSERVER LESS A REASONABLE AMOUNT FOR ITS USE.

3. Purchaser’s Representations and Obligations. Prior to obtaining any services from Datum pursuant to Section 1 above, Purchaser represents that it will fulfill the obligations set forth in this Section 3.

(a) Purchaser has downloaded designated SyncServer Code and Licensed Internal Code updates from a Datum Internet web site or from other electronic media in accordance with instructions provided by Datum.

(b) Purchaser has removed all features, parts, options, alterations, and attachments not under warranty service. Purchaser represents that all removed items are genuine and unaltered.

(c) Purchaser represents that the SyncServer is free of any legal obligations or restrictions that prevent its exchange.

(d) Purchaser has obtained authorization, to Datum’s satisfaction, from the owner of the SyncServer, if other than Purchaser, to have Datum or Datum’s authorized representative service the SyncServer.

(e) Purchaser shall, as applicable:

(i) follow the problem determination, problem analysis, and service request procedures that Datum or its authorized representative provides;

(ii) secure all programs, data, and funds contained in the SyncServer;

(iii) provide Datum or its authorized representative with sufficient, free, and safe access to Purchaser’s facilities to permit them to fulfill their obligations; and

(iv) inform Datum or its authorized representative of changes in a SyncServer’s location.

4. Customer Service Number. Please contact Datum at (+1) 781-372-3675 for warranty service.

TRUSTED TIME™ SYNCSERVER™ S100 USER GUIDE

SS v1.2, Doc v1.2

TABLE OF CONTENTS

Introduction

Trusted Time™ SyncServer™ S100

Introduction and Welcome

Welcome to the The Trusted Time SyncServer S100, providing secure synchronization to UTC time. It is an NTP-based network appliance that acquires time and keeps it secure as it distributes the time over the network. It acquires time either from a non-network source or from another SyncServer, and delivers it to computers and other devices on a network.

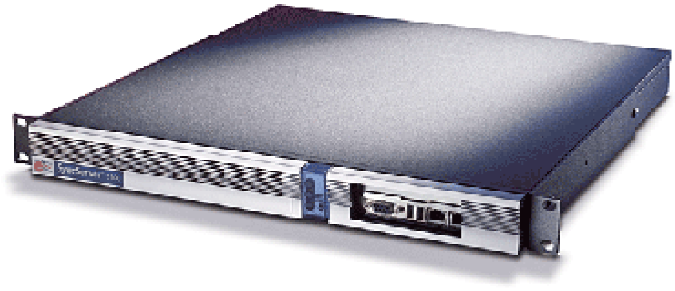


Figure I-1: SyncServer S100

About This Book

This User Guide describes the installation and operation of the Trusted Time SyncServer Model S100.

Additional copies of this *User Guide* are available through your Datum Trusted Time Division contact.

For SyncServer Users

This information is written for network administrators familiar with network configuration and operations.

Conventions Used

The most common conventions used here are:

Conventions Used

Term	Definition
Bold	**Boldface** type is used for menu and command names; field, tab, and button labels; and special terms.
Courier	The Courier typeface is used to designate file names, folder names, and URLs.
⚠	The warning symbol alerts the user to information that if improperly used could be harmful to people, equipment, or data.

Product Details

Details about the physical description and operating environment of the SyncServer S100 are found in Appendix A, SyncServer Product Specifications on page 101 of this *User Guide*.

Details about SyncServer operations are in Chapter 3 - The Web-Based Interface, as well as Chapter 2 - Getting Started: Installation, and Chapter 4 - SyncServer Operations and Time-Related Protocols.

Technical Support

Technical support for your S100 is available through Datum Trusted Time Division at ttsupport@datum.com, or at (1) (781) 372-3600.

About Time

This section describes world standards in time, and defines some time-distribution concepts.

Time Standards

The international time standard is called Coordinated Universal Time or, more commonly, UTC. This standard was agreed upon in 1972 by worldwide representatives within the International Telecommunications Union; today, the Internet Engineering Task Force (IETF) sets standards based on the 1972 work. Today UTC is coordinated by the world's International Bureau of Weights and Measures, or BIPM. (The designations "UTC" and "BIPM" were chosen as a compromise among all the countries' abbreviations for the terms.)

The global availability and precision of UTC time makes it the ideal source of time for trusted time.

SyncServer uses UTC as its time standard.

Global Positioning System (GPS)

The U.S. Department of Defense Global Positioning System (GPS) is a constellation of 24 satellites that each orbit twice a day; their orbits are inclined 56 degrees to the equator. These satellites transmit signals that are used by the GPS receivers to very precisely determine the position and time.

The orbits of these satellites and the offset (relative to international standard time, UTC) of their on-board cesium atomic clocks is precisely tracked by the U.S. Air Force control network. Position and time correction information is uplinked from the ground control stations and maintained in the satellites in what are termed *ephemeris tables,* or tables of data that describe the satellite's position when compared to specified coordinates. Each satellite transmission reports the satellite's current position, GPS time, and the offset of the satellite's clock relative to UTC, international standard time.

SyncServer uses GPS to obtain time.

Stratum Levels

Years ago, the Internet Engineering Task Force (IETF) established standards for Network Time Protocol (NTP), standards still used today in IETF RFC 1305. These hold that the source of time for each server is defined by a number called its **stratum**. The highest level is 0; Stratum 0 devices, such as GPS or radio clocks, are connected to a primary time reference, such as the national atomic clock. Each level "away" from this primary time reference adds on another number. The Stratum of a primary server, which gets its time from, for example, a GPS, is assigned as 1.

Devices that get their time from a Stratum 1 primary server via NTP are Stratum 2, Stratum 3, and so forth. A Stratum 2 or 3 Server simultaneously acts as a client, deriving its time via an NTP process with a Stratum 1 (or 2) Server, and acts as a server for clients further down the hierarchy.

Here is a summary:

Table I-1: Stratum Levels: Summary

Stratum Level	Significance
Stratum 0	Connected to a primary time reference, this device—usually a GPS or radio clock—is synchronized to national standard time.
Stratum 1	A Stratum 1 time server derives time from a Stratum 0 time source
Stratum 2...n	A Stratum 2 (and so on) device derives its time from a Stratum 1 server, or other Stratum 2...n device via NTP.

Obviously, the further away a network is from the primary source, the higher the possibility of signal degradation because of variations in communication paths and the stability of the local clock.

SyncServer can be a Stratum 1 device, as well as Stratum 2 or 3.

Time Synchronization and Business

Reliable time synchronization is essential for doing business today.

Ensuring all components of a network are synchronized to the global UTC time standard is critical for accurate time stamps, operational logs, and security applications. Many complex data processing tasks are dependent upon precise event sequences that are, in turn, dependent upon each sequence having a correct time tag.

By using something other than a dedicated time server, problems can arise, such as:

- Security risks: Users who retrieve time from an outside source, such as the Internet, are going outside your firewall.
- Bandwidth consumption: By attempting to synchronize time by using WAN (wide area network) links, users are consuming expensive bandwidth, which can also degrade time accuracy.
- Lost time: If your network synchronization relies on only one source for time reference, your network can be seriously compromised if that one connection is lost.

How SyncServer Solves the Problem

SyncServer sets system time by providing a single, unbiased time reference that draws from one or more sources. All your computer networks are securely synchronized against this time reference. SyncServer has the unique advantage of having its own high performance crystal. This way, you make sure NTP clients always receive accurate time, even if the GPS or other external time references become temporarily unavailable.

A SyncServer, using its internal GPS receiver, operates as a Stratum 1 time server, with accuracy to the nearest microsecond relative to UTC as maintained by the U.S. Naval Observatory, one of the National Measurement Institutes (NMIs) in the U.S.

Time is distributed within the network using the Network Time Protocol (NTP), and between multiple sites. The result is that with SyncServer, network users can get time without breaching your firewall.

Full specifications are found in SyncServer Product Specifications.

About Trusted Time

SyncServer is a member of the Trusted Time™ family of products. The following section is background information about Trusted Time.

National Measurement Institutes

Trusted Time products synchronize to UTC. This time standard is maintained by the International Bureau of Weights and Measures (BIPM). By international agreement, each country's National Measurement Institute (NMI) maintains audit records of their synchronization with BIPM UTC, thus providing verifiable sources of UTC within their countries. NMI clocks are disciplined to be within microseconds of UTC time.

Table I-2: Examples of NMIs

Country	Name of NMI	Abbreviation
United States	National Institute of Standards and Technology	NIST
France	Laboratoire Primaire du Temps et des Fréquences	LPTF
United Kingdom	National Physical Laboratory	NPL
Japan	Communications Research Laboratory	CRL

Secure Time Distribution

Most time-distribution solutions today ignore both the issues of *time source trust* and the *universal nature of time*.

Trusted Time products are capable of securely and verifiably distributing time from a country's legal time source down to the local applications themselves. SyncServer products offer secure time.

For more on how SyncServer works, please see Chapter 1, SyncServer: The Technology.

Chapter 1

SyncServer: The Technology

Overview

This chapter gives a review of the SyncServer S100 technology within the context of the Trusted Time Infrastructure.

There is additional information in Appendix A, SyncServer Product Specifications, on page 101.

SyncServer Product Overview

The Trusted Time SyncServer S100 is a network time server that synchronizes *secure* network time. The following sections describe SyncServer technology.

Sources of Time

SyncServer obtains time either from a non-network source or from another SyncServer, and delivers it to computers and other devices on a network.

It acquires UTC (Universal Coordinated Time) from GPS signals, or by dialup to the National Institute of Standards and Technology (in the U.S.) or other UTC source. If you have several SyncServers on your network, only a few SyncServers need acquire UTC directly. They can then distribute that time to other SyncServers.

On the Network

Clients on a network synchronize with an external time source using NTP, the Network Time Protocol, to exchange packets of time. SyncServer implements NTP Version 4. This prevents hackers from spoofing time packets and using NTP to gain access to your systems. Unlike previous versions, NTP Version 4 implements asymmetric encryption. This is the same technique used by secure web sites to protect credit card numbers and other sensitive information from unintended interception.

SyncServer also supports SNMP (Simple Network Management Protocol) for easy integration into your existing management hierarchy.

Web-based Access

SyncServer S100 management is web-based. Using a standard browser, you will set up and configure all SyncServers from any point on the Internet/World Wide Web.

See Chapter 2 for more about this web access.

There is a detailed section about this web-based interface in Chapter 3, The Web-Based Interface.

Time Distribution Model

Network time distribution systems usually use a hierarchical time distribution model, as illustrated in Figure 1-1 here, and which shows where SyncServer can fit in.

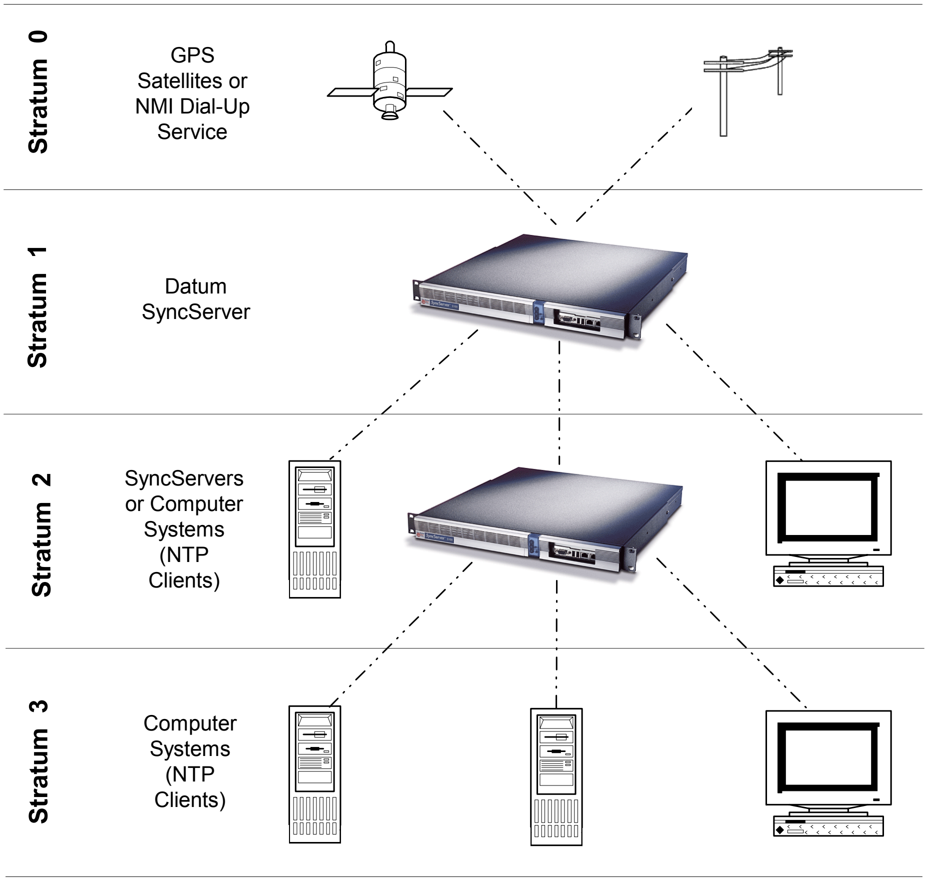

Stratum 0
GPS Satellites or NMI Dial-Up Service
Stratum 1
Datum SyncServer
Stratum 2
SyncServers or Computer Systems (NTP Clients)
Stratum 3
Computer Systems (NTP Clients)

Figure 1-1: SyncServer in the Time Distribution Hierarchy

In hierarchical systems, the primary time source clocks are considered Stratum 0 (zero) which includes GPS satellites, National Institute of Standards and Technology (NIST), or other national time standards organizations.

The SyncServer acts as a Stratum 1 time server that derives its time from the GPS satellites and distributes this time through TCP/IP network to the computers. The client computers may act as Stratum 2 time servers and distribute time to Stratum 3 computers, as shown.

How SyncServer Works

The following describes the "big picture" about how SyncServer acquires and secures time.

More details are found in Chapters 2 and 3.

SyncServer and Time Distribution

Time is distributed over an IP network by Network Time Protocol (NTP), Simple Network Time Protocol (SNTP), Time Protocol, and Daytime Protocol over TCP/IP.

SyncServers can be distributed throughout a LAN or intranet. Also, a single GPS antenna is all that is required to acquire UTC time for an array of SyncServers, making the network less vulnerable to damage or attack.

Once the SyncServer is locked with its time source, it will continuously provide time even if the timing signal is lost. If the GPS time signal is lost, the NTP message returned by the SyncServer will indicate—via the Reference Timestamp—when it last obtained time updates from the timing signal.

The SyncServer maintains the year value as a four-digit number. It also recognizes leap years and the introduction of leap seconds.

SyncServer and Client Software

Client software must be installed on the client machines before NTP can synchronize the time with the SyncServer's clock.

The clients that need to be synchronized should be running a copy of the public domain NTP daemon or other equivalent client software. If an NTP daemon is not available for your system, you can obtain a copy of RFC 1305 or 2030 from the Network Information Center (NIC) at `http://www.rfc.net/rfc1305.html`, in order to implement an NTP daemon for your system.

And you can obtain the DatumTime™ client for Windows at `http://www.datum.com/tt/pages/trustedtime/datumtime.html.`

Details about installing DatumTime are found in Chapter 2, Installing the DatumTime™ Client Software.

SyncServer and NTPv4's Security Features

NTP is the de facto standard of communicating time in IP network environments. Developed at the University of Delaware in the United States, NTP is public domain software. It can provide time without opening the NTP port and exposing the firewall to possible intrusion. The SyncServer supports NTP v4 (Secure NTP), and can support NTPv2 and v3, as well.

SyncServer generates keys which take the form of a file composed of random numerical sequences. These key files which are recognized by the cryptographic authentication components of NTP. These keys are symmetric, or private (in NTPv3 and v4), and asymmetric or public or Autokey (NTPv4); Autokey protocol, therefore, can recognize the key files as well. The contents of the key files include the public/private key pair, a certificate request, a certificate, and Diffie-Hellman parameters.

Digitally signed public certificates are required by the Autokey protocol. As you can see by looking at the interface at NTP Advanced: Keys/Certificates, you must provide what are called “credentials”, such as the host name, the name of the person responsible, and so forth. All of this data goes into your certificate request (X.509) to a trusted certificate Authority (CA). The CA can be an outside trust authority, such as VeriSign, or the device can certify itself. The S100 itself is “self-signed”, or shipped to you with an authenticated certificate. The S100 CA digitally signs (authenticates) the request and sends it back, along with the certificate, to the person requesting it.

More details of the NTP protocol and synchronization techniques can be found in the Help file included with the interface, or at:

- `http://www.ntp.org`
- `http://www.ietf.org/rfc/rfc1305.txt`

SyncServer and the Global Positioning System

The Global Positioning System (GPS) receiver in your SyncServer tracks the 24 GPS satellites as they pass overhead.

The SyncServer also determines the range of the satellite in relation to its antenna. There are four unknowns about location of the satellite, and what they roughly represent, which when resolved will help you position the SyncServer antenna:

- x, or latitude
- y, or longitude
- z, or altitude
- t, or time

Knowing the range from one satellite places you on a sphere. Two satellites show the intersection of two spheres, roughly a circle. Three satellites show two points. And four satellites show the complete four-variable solution.

However, once x, y, and z are known, only one satellite is needed to solve for time (t). This is because the receiver has tracked at least four satellites and has positioned itself.

Thus the SyncServer antenna still works—and SyncServer can still source time—in areas with a somewhat restricted view of the sky, such as in cities.

The time is expressed as the number of weeks since midnight, January 6, 1980 (GPS Week) and the number of seconds in the week. These two values are transmitted as binary integers from the satellites and converted into conventional date or day by the GPS receiver.

Chapter 2

Getting Started: Installation

Overview

Installation, setup, and getting started with the SyncServer S100 are reviewed in this section. Datum recommends you review Chapter 3, The Web-Based Interface before beginning your installation so that you are already familiar with the references to the interface once you begin to use it.

Getting Up and Running

The following sections describe what you need to begin installing your SyncServer.

Basic Steps

This is what you'll be doing to install your SyncServer:

1. Set up the hardware and make all connections (*Optional:* For GPS, install antenna)
2. Using the serial cable, establish the S100's IP address
3. Test for NTP functionality
4. Using the web-based interface, choose and configure the time source

Unpacking Your SyncServer

Unpack and inspect each item in the box. If there is any damage, or any items are missing, please contact Datum at (781) 372-3600 immediately.

The following items should be included:

Table 2-1: SyncServer and Accessories

For the SyncServer-Dialup/ACTS	For the SyncServer-GPS
SyncServer S100	SyncServer S100
A/C Power Cord with US-style wall plug	A/C Power Cord with US-style wall plug
CD with NTP Clients, DatumTime™ software, User Guide PDF	CD with NTP Clients, DatumTime™ software, User Guide PDF.
Six-foot RS-232 Cable	Six-foot RS-232 Cable
Phone cord	Phone cord
	Bullet Antenna
	Antenna Mast -aluminum mast threaded to screw into the bottom of antenna
	Mounting Bracket Hardware - for attaching mast to railing
	50-foot RG58 (Belden 8240 or equivalent) cable

The following illustration shows you these components.

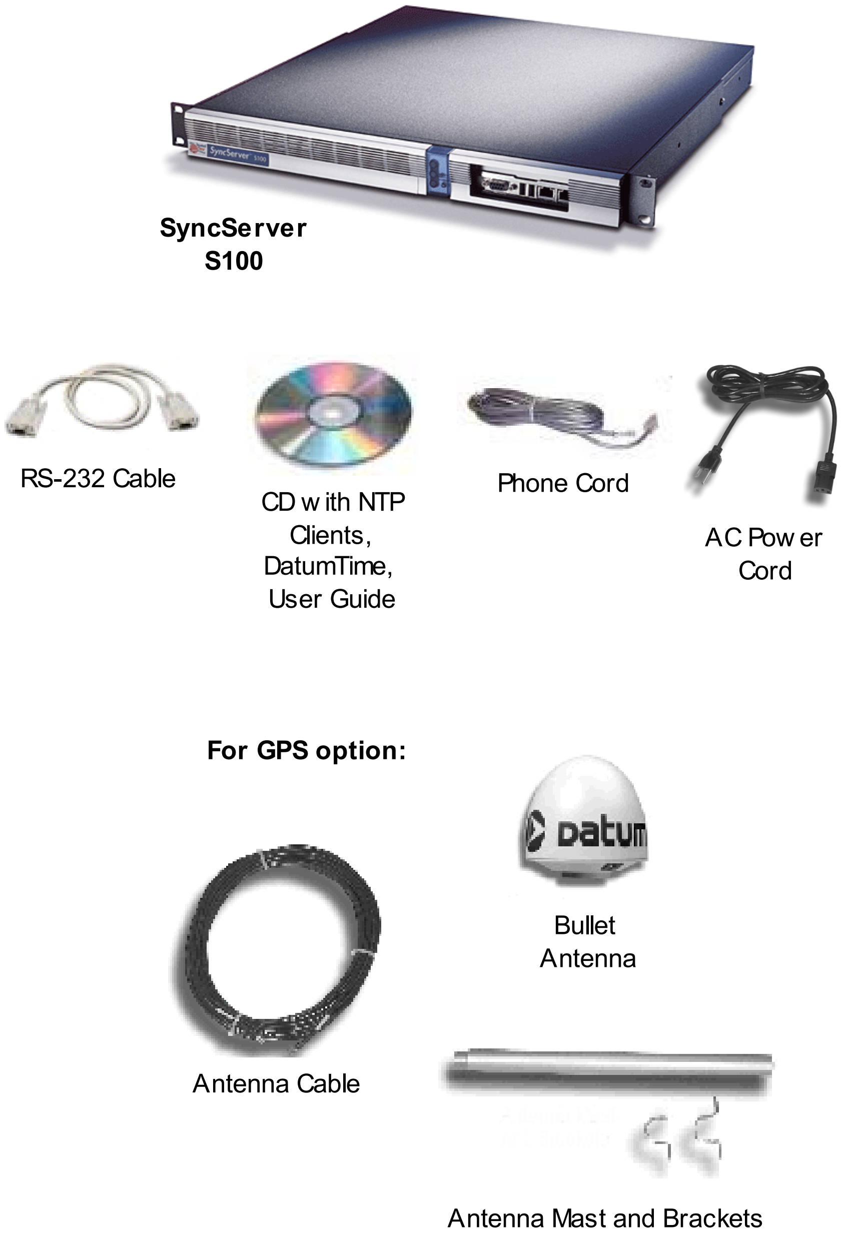


Figure 2-1: SyncServer and Accessories

Installing Your SyncServer

The S100 should be installed in a physically secure location with strong physical access controls.

Datum recommends that you read the operating environment requirements and other specifications in *Appendix A,* SyncServer Specifications, before you get started.

⚠	**WARNING!** *To prevent electrical shock or injury, DO NOT remove the SyncServer cover.* *Dangerous voltages exist within this enclosure!*

Rack Mounting

The S100 is designed for mounting in a standard 19-inch (48.26 cm) rack.

NOTE: It is important to keep the fan inlet and outlet areas clear, to maintain air flow. Also, if the unit is installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may become greater than that of the room, so allow for this. Be sure that the ambient temperature is no higher than 50°C/122°F. And make sure the unit is properly balanced and grounded.

Primary Power Connection

The SyncServer uses external AC power.

The unit has a power cable with a PH-386, IEC 320-C-13 three-conductor female connector on the computer end of the cable. The other end of the cable has a NEMA 6-15P grounding plug (US Standard, 15-amp, 125-volt, straight-blade plug).

Making All Connections

This is the front panel of the SyncServer S100. Use this illustration as a reference when you install your SyncServer.

Use your standard PC workstation to configure your SyncServer.

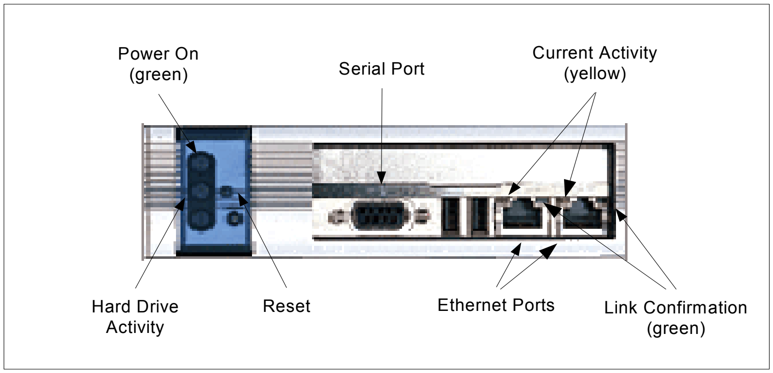


Figure 2-2 S100 Front Panel Close-up

Setting Up the Hardware

Your SyncServer is not yet powered on.

On the Front

See Figure 2-2 for details.

1. **Connect** the 9-pin serial cable from the PC workstation to the SyncServer serial port. You are doing this so that you can configure the SyncServer by using the PC; see Establishing A Serial Connection in the next section.
2. **Connect** the RJ45-terminated Ethernet cable to one or both network ports on the SyncServer.

NOTE: If only one network connection is required, it must use the *left* Ethernet port (**eth0**).

On the Back

The back panel of the S100 has the power port and power switch.

1. **Connect** the power cable to the SyncServer.
2. *Optional:* Install GPS Antenna by connecting it to the card in the back of the S100.

Installing the GPS Antenna

If you are installing a SyncServer with GPS option, a bullet antenna is provided. The bullet antenna provided with the SyncServer GPS version comes with a weatherproof housing, suitable for permanent installation in an outdoor location.

Best Antenna Location: The Global Positioning System (GPS) of 24 satellites are in orbits inclined 56 degrees to the equator, each orbiting the earth twice a day. This angle means that the further north you are in the northern hemisphere, the more probable it is that satellites will be passing to the south of you. And if you are in the southern hemisphere, the satellites will be passing to the north of you. Please consider this as you install your antenna.

The antenna should be located with an unobstructed, clear view of the sky for optimum tracking conditions. The antenna can receive satellite signals through glass, canvas, or thin fiberglass. The satellite signals cannot penetrate foliage, or dense wood or metal structures. The antenna's operation is not affected if it is partially covered with snow, provided the snow is dry and does not form a continuous ice sheet on the surface. The shape of the bullet antenna is designed to prevent accumulation of rain, snow, or ice on its surface.

The GPS transmission is a 1.5 GHz (Ll Band) spread-spectrum signal. Being spread-spectrum means it is relatively immune to interference. But high energy sources, especially those with significant in-band energy, can swamp the receiver's radio frequency (RF) processing circuitry. In addition, it is difficult to operate GPS at power substations or in close proximity to high-voltage 60 Hz sources. Datum offers an optional high gain antenna that is useful in these heavy interference situations. Still, it is best to locate the antenna away from radiating sources so you can avoid degradation in antenna performance.

⚠	**WARNING:** *Do not* cut the cable to a shorter length. Instead, bundle any excess cable. Correct antenna cable length—even if you do not "use it all"—is critical to proper SyncServer operation, which should have a gain within the range of 15dB–25dB.

Outdoors: Install the antenna, using the mast and mounting brackets, with a clear view of the sky, and away from radio frequency interference. It should be mounted vertically, in a location with an unobstructed view of 30° of the horizon. Be sure to position it at least two meters from other active receiving antennas, and shield it from transmitting antennas.

Indoors: While Datum does not recommend indoor installations, we understand that this may be the only option available to some customers. In such a case, it is best to temporarily install the antenna along a window to verify performance, before making such a configuration permanent.

Install the antenna by placing it near a window with a clear view of the sky, and away from radio frequency interference. Make sure it is as vertical as possible. Reflective window coatings will not only reflect sunlight, but the GPS signal as well. You can expect lower performance if you have reflective or heavy tinting on your office windows.

To install the GPS antenna:

□ Slide the antenna mounting pole down over the antenna cable so that the cable passes through the center of the pole.

□ Take the end of the cable that has passed through the pole and screw the antenna onto the cable by turning the antenna.

□ Screw the antenna down on the mounting pole by turning the pole.

□ Use the saddle straps to mount the antenna mast in an area where the antenna has a 30° view of the horizon.

□ After running the cable from the SyncServer location to the antenna, attach the cable to the antenna.

For additional information, ask your Datum representative for the *GPS Antenna Mounting Guide*.

3. *Optional:* Connect the modem phone line to the card on the back of the S100.
4. *Optional:* Connect the chassis ground and install nut (not provided).
5. On the back panel of the SyncServer, **turn on** the Power switch. The Power LED (green) in the front panel comes on. When the hard drive is active, a red LED light comes on.

Establishing A Serial Connection

This step is necessary so you can establish the SyncServer's IP address. The only time you will need to make a serial connection with the SyncServer is now, during setup. Once the SyncServer has an IP address, you will use the web-based interface.

The following instructions assume you are using Windows.

1. On the PC you are using the manage the S100, click **Start->Programs->Accessories->HyperTerminal.**
2. Double-click `Hypertrm.exe`.
3. In the **Connection Description** dialog's **Name** field, enter `SyncServer1` (for example).
4. Click **OK**.
5. In the **Connect to** dialog, select the **com Port number** of the comm port you are plugged into.
6. Click **OK**.

7. In the **Com1 Properties** dialog, enter the following Port Settings information:

Port Setting:	Enter:
Bits per second:	115.2kbps or higher
Data bits:	8
Parity:	none
Stop bits:	1
Flow Control:	Hardware

8. Click **OK**.
9. Select **File->Properties**. The **Properties** dialog opens. Click the **Settings** tab. Be sure the **Telnet Terminal ID** is set at *ANSI*.
10. Click **OK**.

To set the IP address:

1. Login with the user ID of **`root`** and use the default password **`datum`**.

NOTE: For security purposes, the **`root`**, or **superuser**, password should immediately be changed by using the **`passwd`** utility.

2. In HyperTerminal, type in the **`netconfig`** command. Enter the correct information.
3. Next, type the **`reboot` command**. The SyncServer reboots.

Your SyncServer now has an IP address.

Testing Network Functionality

Now ensure that your network is functioning correctly.

Checking to See if the SyncServer is On the Network

To check the functionality of the network, first check the Ethernet connection between the client computer and the SyncServer:

1. Call up the client computer's command prompt.
2. Enter ping command to verify that the SyncServer is visible on the network.

   Example: **ping** xxx.xxx.xxx.xxx (the address you entered in To set the IP address:, above).
3. Press **Enter**

   If there is an affirmative response, the SyncServer is visible to the network.

NOTE: If there is no response, then troubleshoot and fix the connection problem before proceding with the next steps.

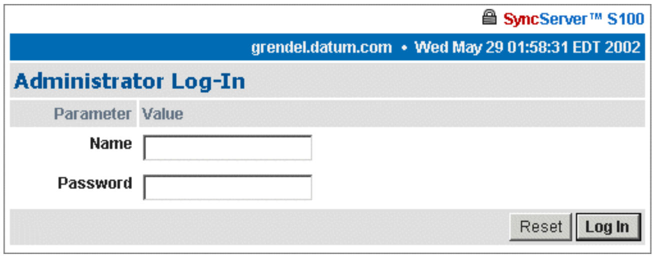
How to Acquire Time

With SyncServer, you can choose your source of secure time.

Each of the time references described in this section is configured by using the web-based interface's **Config Wizard**.

First, log on.

Logging On



SyncServer™ S100

grendel.datum.com • Wed May 29 01:58:31 EDT 2002

Administrator Log-In

Parameter	Value
Name	
Password	

Figure 2-3 Logging In

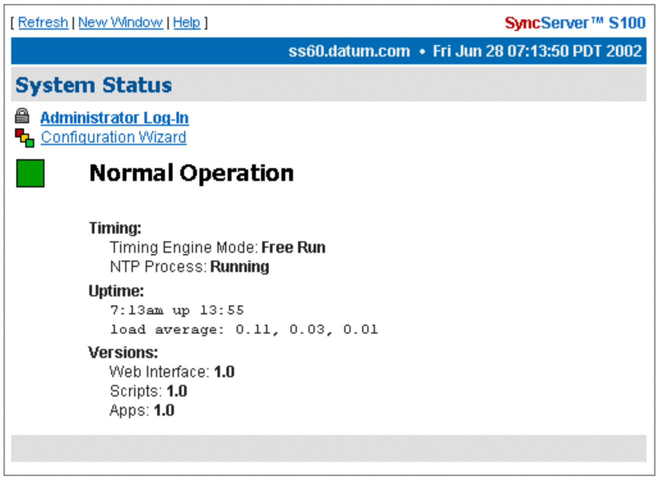
Here is how to log in to the web-based interface:

Using your browser, this dialog displays once you click on the link to or icon for your SyncServer S100.

Enter the default user name, **`admin`**, and default password, **`datum`**.

You may log off by clicking **Log Out** at the top of each screen in the interface. More about logging off can be found in Chapter 3, Logging Off.

Assuming this is the first time you have logged in, you now see the System Status screen.



[Refresh | New Window | Help] SyncServer™ S100

ss60.datum.com • Fri Jun 28 07:13:50 PDT 2002

System Status

Administrator Log-In
Configuration Wizard

🟩 Normal Operation

Timing:
Timing Engine Mode: **Free Run**
NTP Process: **Running**

Uptime:

```
7:13am up 13:55
load average: 0.11, 0.03, 0.01
```

Versions:
Web Interface: **1.0**
Scripts: **1.0**
Apps: **1.0**

Figure 2-4: Checking the System Status

The *System Status* screen gives you the status of your SyncServer’s timing, uptime, and versions.

The color of the box on the left side of the screen is your guide. It follows the traffic light convention:

- Green = Normal Operation: SyncServer up and running with the correct time
- Amber = Unsatisfactory: Some settings still need attention before secure time can be issued
- Red = Unsatisfactory: System not yet ready to issue time

Log-ins after this first log-in will bring you to the last screen you accessed in your most recent session.

The Config Wizard

Using your browser, follow this easy-to-direct sequence of dialogs to configure your SyncServer's source of time. You will need the wizard only once, unless you change the time source for your S100.

Every screen in the wizard lets you start over, reset, or (for a screen in a sequence) go back to the previous screen.

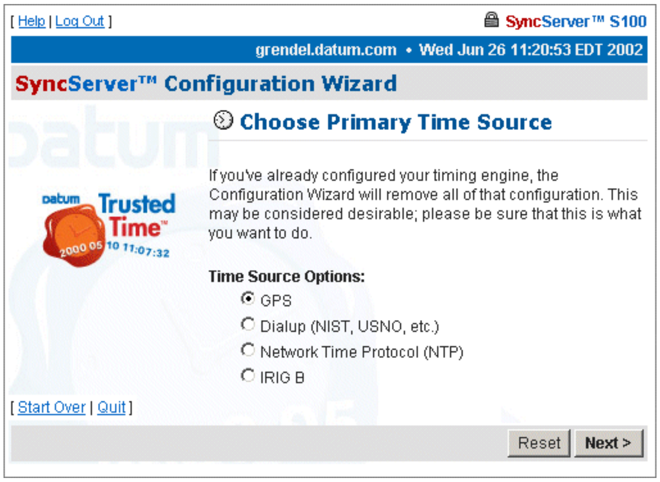
NOTE: When within the Config Wizard, do not use your browser's *back* button but use the Wizard's instead: < Back

Choose Your Time Source

The first dialog in the ConfigWizard asks you to choose the source of time.

The choices are:

- GPS
- Dialup (to NIST, for example)
- Network Time Protocol (NTP)
- IRIG B



[Help | Log Out] SyncServer™ S100

grendel.datum.com • Wed Jun 26 11:20:53 EDT 2002

SyncServer™ Configuration Wizard

Choose Primary Time Source

If you've already configured your timing engine, the Configuration Wizard will remove all of that configuration. This may be considered desirable; please be sure that this is what you want to do.

Time Source Options:

● GPS
○ Dialup (NIST, USNO, etc.)
○ Network Time Protocol (NTP)
○ IRIG B

[Start Over | Quit]

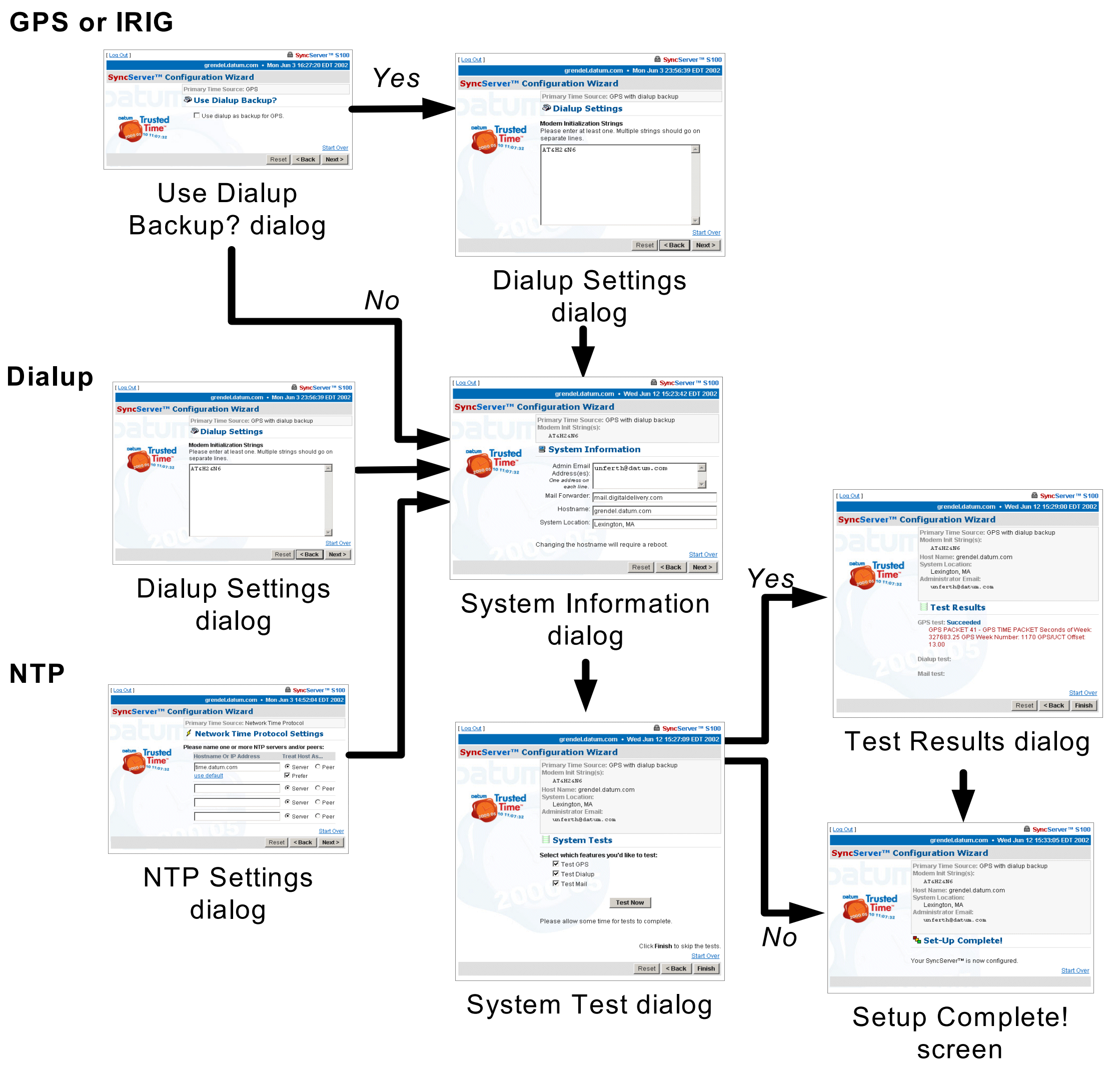
Figure 2-5: Choose Your Time Source

Warning:

If you've already configured your timing engine, the Configuration Wizard will remove all of that configuration. This may be considered desirable; please be sure that this is what you want to do.

The following graphic shows the route you take once you choose the time-source option you prefer.

Configuring Your SyncServer's Time Source



grendel.datum.com • Mon Jun 3 16:27:20 EDT 2002

Primary Time Source: GPS

Use Dialup Backup?

□ Use dialup as backup for GPS.

grendel.datum.com • Mon Jun 3 23:56:39 EDT 2002

Primary Time Source: GPS with dialup backup

Dialup Settings

Modem Initialization Strings
Please enter at least one. Multiple strings should go on separate lines.

AT&H2&N6

grendel.datum.com • Wed Jun 12 15:23:42 EDT 2002

Primary Time Source: GPS with dialup backup
Modem Init String(s):
AT&H2&N6

System Information

Admin Email Address(es): *One address on each line.* unferth@datum.com
Mail Forwarder: mail.digitaldelivery.com
Hostname: grendel.datum.com
System Location: Lexington, MA

Changing the hostname will require a reboot.

grendel.datum.com • Mon Jun 3 14:52:04 EDT 2002

Primary Time Source: Network Time Protocol

Network Time Protocol Settings

Please name one or more NTP servers and/or peers:

Hostname Or IP Address	Treat Host As...
time.datum.com use default	● Server ○ Peer ☑ Prefer
	● Server ○ Peer
	● Server ○ Peer
	● Server ○ Peer

grendel.datum.com • Wed Jun 12 15:27:09 EDT 2002

Primary Time Source: GPS with dialup backup
Modem Init String(s):
AT&H2&N6
Host Name: grendel.datum.com
System Location:
Lexington, MA
Administrator Email:
unferth@datum.com

System Tests

Select which features you'd like to test:
☑ Test GPS
☑ Test Dialup
☑ Test Mail

Please allow some time for tests to complete.

Click **Finish** to skip the tests.

grendel.datum.com • Wed Jun 12 15:29:00 EDT 2002

Primary Time Source: GPS with dialup backup
Modem Init String(s):
AT&H2&N6
Host Name: grendel.datum.com
System Location:
Lexington, MA
Administrator Email:
unferth@datum.com

Test Results

GPS test: Succeeded
GPS PACKET 41 - GPS TIME PACKET Seconds of Week: 327683.25 GPS Week Number: 1170 GPS/UCT Offset: 13.00

Dialup test:

Mail test:

grendel.datum.com • Wed Jun 12 15:33:05 EDT 2002

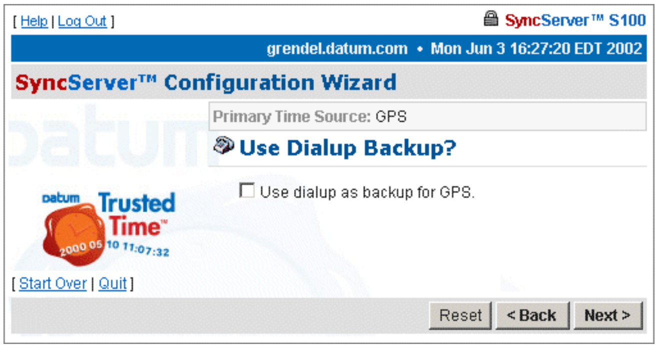
Primary Time Source: GPS with dialup backup
Modem Init String(s):
AT&H2&N6
Host Name: grendel.datum.com
System Location:
Lexington, MA
Administrator Email:
unferth@datum.com

Set-Up Complete!

Your SyncServer™ is now configured.

Figure 2-6: Configuring the Time Source

GPS



grendel.datum.com • Mon Jun 3 16:27:20 EDT 2002

SyncServer™ Configuration Wizard

Primary Time Source: GPS

Use Dialup Backup?

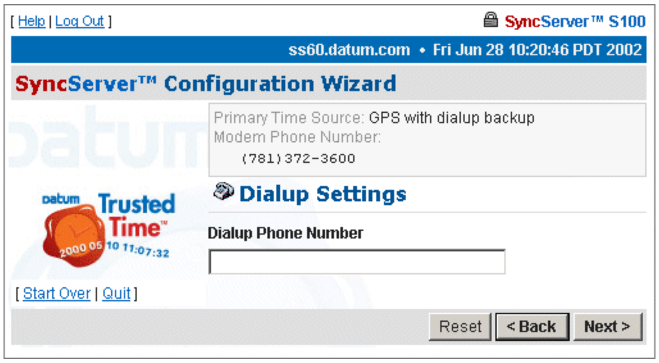
□ Use dialup as backup for GPS.

Figure 2-7: Dialog Backup

If you choose **GPS** and click **Next**, the *Dialup Backup* dialog displays.If you wish to use dialup as a backup time source to GPS, click the checkbox next to **Use dialup as backup to GPS**, then click the **Next** button.

If you do not want to back up your GPS time source with dialup, leave the checkbox unselected, and click **Next**, which will open the System Information dialog.

If you do check **Use dialup as backup for GPS**, this *Dialup Settings* dialog displays.



ss60.datum.com • Fri Jun 28 10:20:46 PDT 2002

SyncServer™ Configuration Wizard

Primary Time Source: GPS with dialup backup
Modem Phone Number:
(781) 372-3600

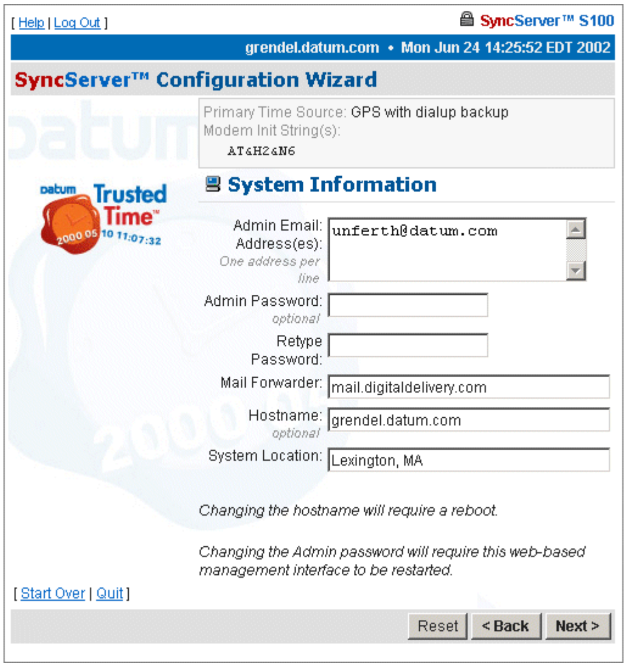
Dialup Settings

Dialup Phone Number

Figure 2-8: Dialup Settings

In the field, type in your **modem phone number**. Obtain these from your IS person if you do not know them yourself.

Then click **Next** for the *System Information* dialog.



grendel.datum.com • Mon Jun 24 14:25:52 EDT 2002

SyncServer™ Configuration Wizard

Primary Time Source: GPS with dialup backup
Modem Init String(s):
AT&H2&N6

System Information

Admin Email: Address(es): *One address per line* unferth@datum.com
Admin Password: *optional*
Retype Password:
Mail Forwarder: mail.digitaldelivery.com
Hostname: *optional* grendel.datum.com
System Location: Lexington, MA

Changing the hostname will require a reboot.

Changing the Admin password will require this web-based management interface to be restarted.

Figure 2-9: System Info fields

System Information dialog

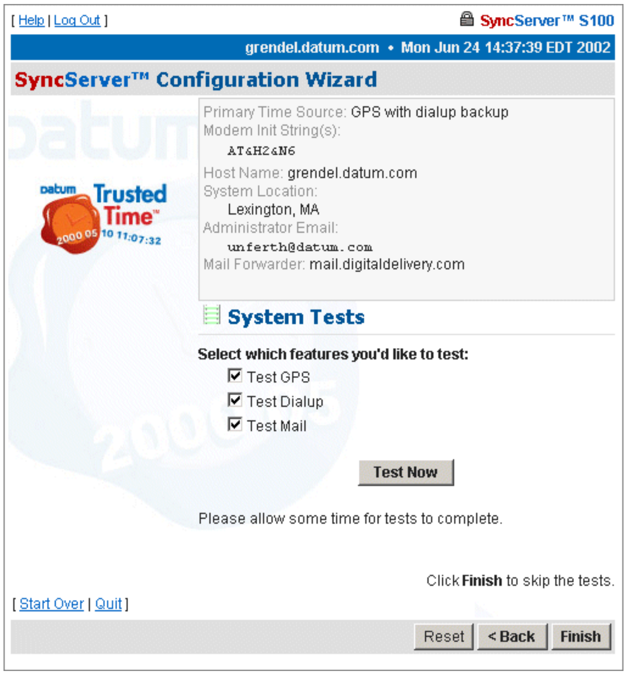
The *System Information* dialog shows you:

- Admin e-mail, for the administrator of the SyncServer
- Mail forwarder, or the SMTP server
- Host name
- System (SyncServer) location

Confirm the data that is in the fields. If it is not accurate, change it to the correct information.

Click **Next**.

The *System Tests* dialog displays.



[Help | Log Out]

SyncServer™ S100

grendel.datum.com • Mon Jun 24 14:37:39 EDT 2002

SyncServer™ Configuration Wizard

Primary Time Source: GPS with dialup backup
Modem Init String(s):
AT&H2&N6
Host Name: grendel.datum.com
System Location:
Lexington, MA
Administrator Email:
unferth@datum.com
Mail Forwarder: mail.digitaldelivery.com

System Tests

Select which features you'd like to test:

- ☑ Test GPS
- ☑ Test Dialup
- ☑ Test Mail

Test Now

Please allow some time for tests to complete.

Click **Finish** to skip the tests.

[Start Over | Quit]

Reset | < Back | Finish

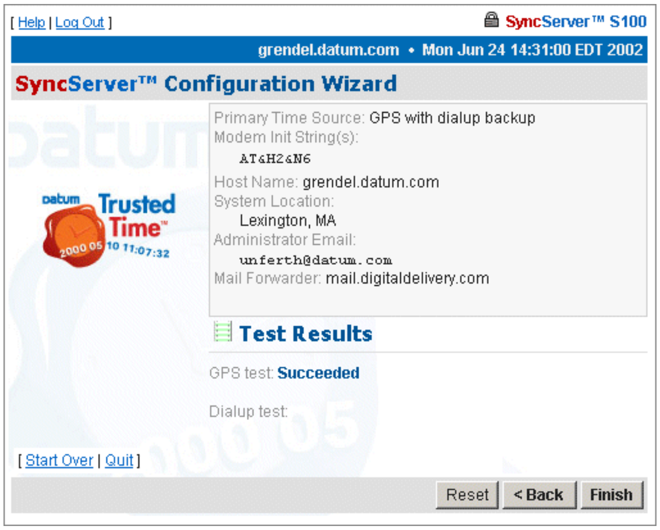
Figure 2-10: System Testing options

You can skip the test by clicking **Finish**, *or* initiate the test by clicking **Test Now**.

The default is to test all the services, so unless you un-check them, they all will be tested. If you do not use dialup as backup, it will not be listed here nor will it be tested.

Initiate the test by clicking **Test Now**.

The *Test Results* dialog displays, with the results of your test.



[Help | Log Out]
SyncServer™ S100
grendel.datum.com • Mon Jun 24 14:31:00 EDT 2002
SyncServer™ Configuration Wizard
datum Trusted Time™ 2000 05 10 11:07:32

Primary Time Source: GPS with dialup backup
Modem Init String(s):
AT&H2&N6
Host Name: grendel.datum.com
System Location:
Lexington, MA
Administrator Email:
unferth@datum.com
Mail Forwarder: mail.digitaldelivery.com

Test Results

GPS test: Succeeded

Dialup test:

[Start Over | Quit]
Reset
< Back
Finish

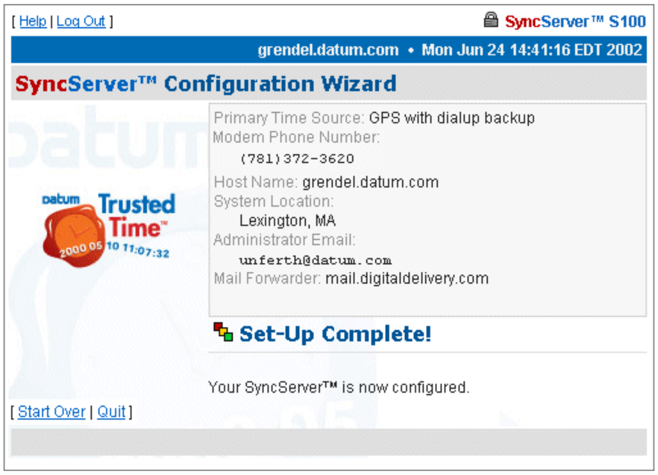
Figure 2-11: Test Results shown

What this tells you is the GPS for your SyncServer is functioning properly.

There is no output to the “Mail test” field. That is because mail is tested by sending an e-mail to the address that you indicated earlier.

Click **Finish**.

The *Setup Complete* screen displays.



grendel.datum.com • Mon Jun 24 14:41:16 EDT 2002

SyncServer™ Configuration Wizard

Primary Time Source: GPS with dialup backup
Modem Phone Number:
(781)372-3620
Host Name: grendel.datum.com
System Location:
Lexington, MA
Administrator Email:
unferth@datum.com
Mail Forwarder: mail.digitaldelivery.com

Set-Up Complete!

Your SyncServer™ is now configured.

Figure 2-12: Your GPS set-up is complete

This screen verifies your configuration of your SyncServer:

- Its time source
- Modem phone number (if you designated dialup as the backup source for time)
- Host name
- System location
- Administrator e-mail

Dialup

When using dial-up (or ACTS or 1PPS), the time reference is coming from an analog phone line through the built-in modem. The Automated Computer Time System is maintained by NIST.

In the US, use either of these phone numbers to access time:

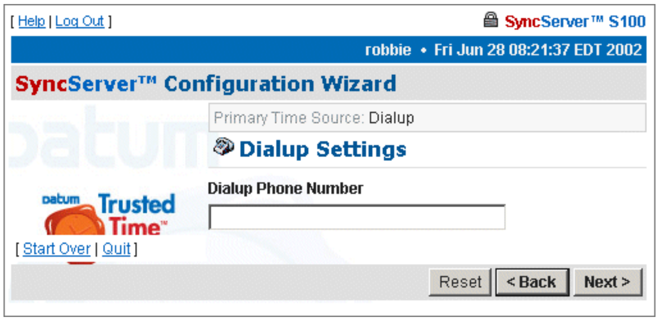
- Colorado: (303) 494-4774
- Hawaii: (808) 335-4721

Outside the US, connect with your local measurement institute.

Your modem or adapter should be configured according to these parameters:

Line speed:	9600 bps
Data format:	Eight word bits, no parity bit, one stop bit (8/N/1)
Flow control:	XON/XOFF (software)
Data:	V.120 data (ISDN only)

If you choose the **Dialup** radio button and click **Next**, the *Dialup Settings* dialog displays.



robbie • Fri Jun 28 08:21:37 EDT 2002

SyncServer™ Configuration Wizard

Primary Time Source: Dialup

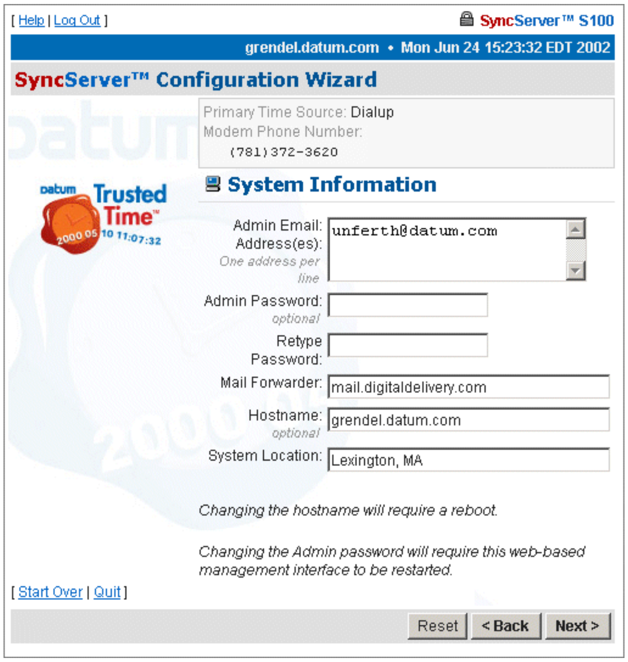
Dialup Settings

Dialup Phone Number

Figure 2-13: Dialup Settings

In the field, type in or paste your **modem phone number**.

Then click **Next** for the *System Information* dialog.



grendel.datum.com • Mon Jun 24 15:23:32 EDT 2002

Primary Time Source: Dialup
Modem Phone Number:
(781)372-3620

Admin Email: Address(es): One address per line: unferth@datum.com
Admin Password: optional:
Retype Password:
Mail Forwarder: mail.digitaldelivery.com
Hostname: optional: grendel.datum.com
System Location: Lexington, MA

Changing the hostname will require a reboot.

Changing the Admin password will require this web-based management interface to be restarted.

Figure 2-14: System Info fields

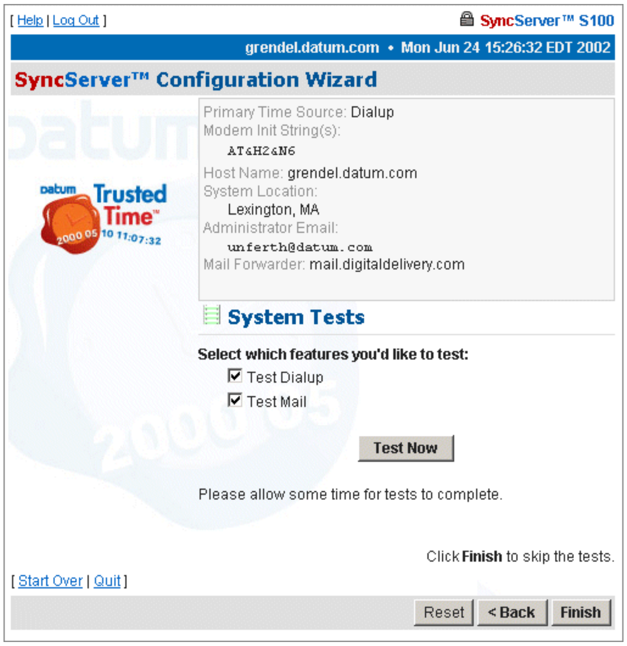
The *System Information* dialog shows you:

- Admin e-mail, for the administrator of the SyncServer
- Mail forwarder, or the SMTP server
- Host name
- System (SyncServer) location

Confirm the data that is in the fields. If it is not accurate, change it to the correct information.

Click **Next**.

The *System Tests* dialog displays.



[Help | Log Out]
SyncServer™ S100
grendel.datum.com • Mon Jun 24 15:26:32 EDT 2002
SyncServer™ Configuration Wizard
datum Trusted Time™
2000 05 10 11:07:32

Primary Time Source: Dialup
Modem Init String(s):
AT&H2&N6
Host Name: grendel.datum.com
System Location:
Lexington, MA
Administrator Email:
unferth@datum.com
Mail Forwarder: mail.digitaldelivery.com

System Tests

Select which features you'd like to test:

☑ Test Dialup
☑ Test Mail

Please allow some time for tests to complete.

Click **Finish** to skip the tests.

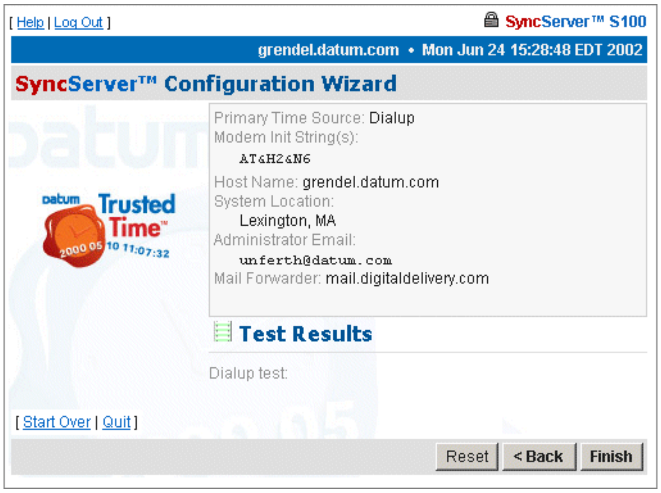
Figure 2-15: System Testing options

You can skip the test by clicking **Finish**, *or* initiate the test by clicking **Test Now**.

The default is to test all the designated services, so **Dialup** and **E-Mail**, unless you un-check them, will be tested.

To initiate the test, click **Test Now**.

The *Test Results* dialog displays, with the results of your test.



Primary Time Source: Dialup
Modem Init String(s):
AT&H2&N6
Host Name: grendel.datum.com
System Location:
Lexington, MA
Administrator Email:
unferth@datum.com
Mail Forwarder: mail.digitaldelivery.com

Test Results

Dialup test:

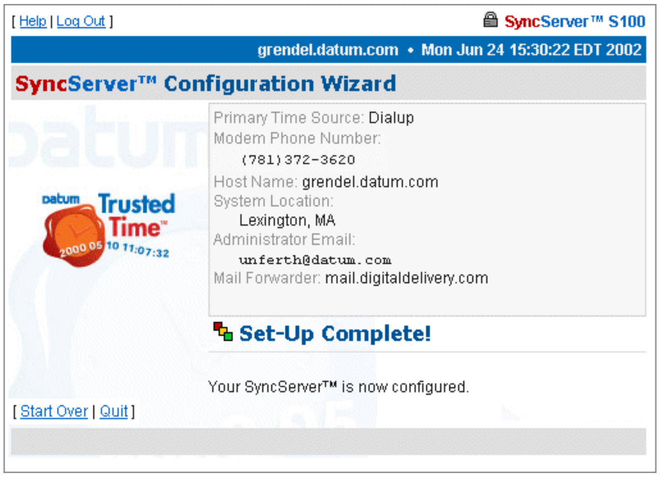
Figure 2-16: Test Results shown

What this tells you is the dialup timesource for your SyncServer is functioning properly.

There is no output to the “Mail test” field. That is because mail is tested by sending an e-mail to the address that you indicated earlier.

Click **Finish**.

The *Setup Complete* screen displays.


[Help | Log Out]
SyncServer™ S100
grendel.datum.com • Mon Jun 24 15:30:22 EDT 2002
SyncServer™ Configuration Wizard
datum Trusted Time
[Start Over | Quit]

Primary Time Source: Dialup
Modem Phone Number:
(781)372-3620
Host Name: grendel.datum.com
System Location:
Lexington, MA
Administrator Email:
unferth@datum.com
Mail Forwarder: mail.digitaldelivery.com

Set-Up Complete!

Your SyncServer™ is now configured.

Figure 2-17: Your Dialup set-up is complete

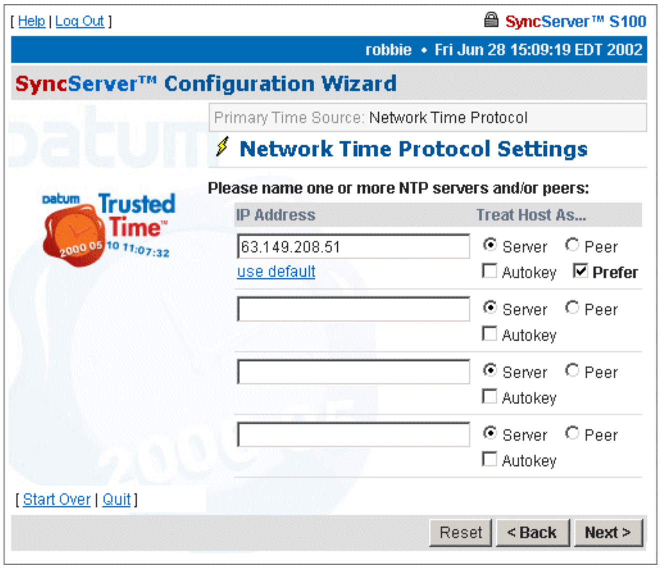
This screen verifies your configuration of your SyncServer:

- Its time source
- Modem phone number
- Host name
- System location
- Administrator e-mail

NTP

You can also acquire time through other NTPv4 servers and SyncServers.

If you choose the *NTP* radio button and click **Next**, the *Network Time Protocol Settings* dialog displays.



robbie • Fri Jun 28 15:09:19 EDT 2002

SyncServer™ Configuration Wizard

Primary Time Source: Network Time Protocol

Network Time Protocol Settings

Please name one or more NTP servers and/or peers:

IP Address	Treat Host As...
63.149.208.51 use default	● Server ○ Peer □ Autokey ☑ Prefer
	● Server ○ Peer □ Autokey
	● Server ○ Peer □ Autokey
	● Server ○ Peer □ Autokey

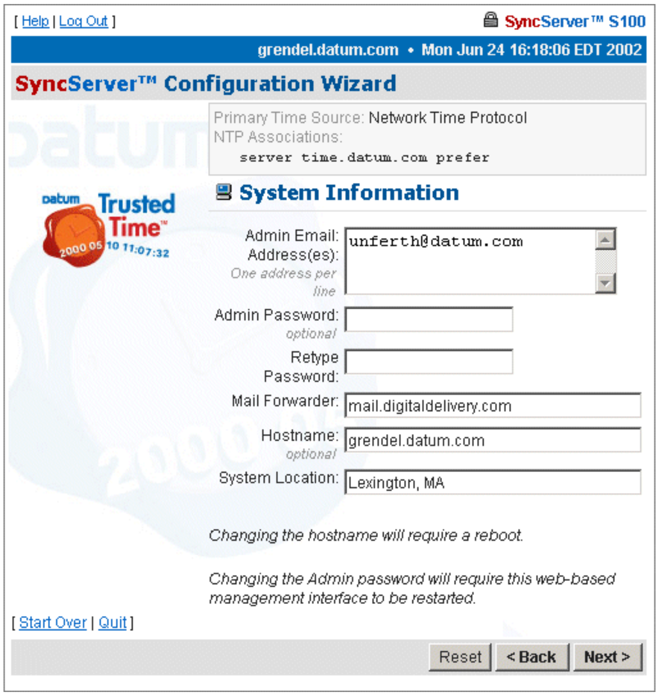
Figure 2-18: Defining Your NTP Settings

Here, you name one (or more) NTP servers or peers.

NTPv4’s Autokey requires digitally signed certificates. For more about the Autokey protocol, see SyncServer and NTPv4’s Security Features.

Then click **Next**.

The *System Information* dialog displays.



grendel.datum.com • Mon Jun 24 16:18:06 EDT 2002

Primary Time Source: Network Time Protocol
NTP Associations:

```
   server time.datum.com prefer
```

Admin Email: Address(es): unferth@datum.com
One address per line

Admin Password:
optional

Retype Password:

Mail Forwarder: mail.digitaldelivery.com

Hostname: grendel.datum.com
optional

System Location: Lexington, MA

Changing the hostname will require a reboot.

Changing the Admin password will require this web-based management interface to be restarted.

Figure 2-19: System Info fields

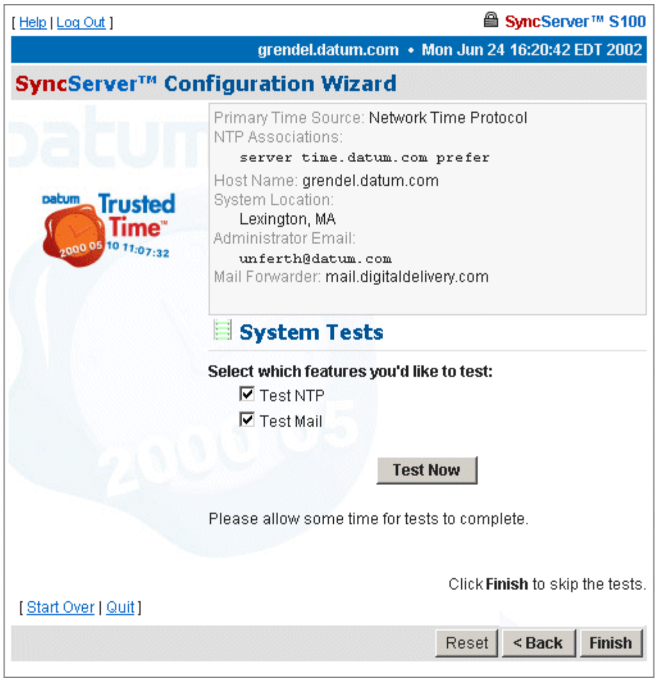
The *System Information* dialog shows you:

- Admin e-mail, for the administrator of the SyncServer
- Mail forwarder, or the SMTP server
- Host name
- System (SyncServer) location

Confirm the data that is in the fields. If it is not accurate, change it to the correct information.

Click **Next**.

The *System Tests* dialog displays.



[Help | Log Out] SyncServer™ S100

grendel.datum.com • Mon Jun 24 16:20:42 EDT 2002

SyncServer™ Configuration Wizard

Primary Time Source: Network Time Protocol
NTP Associations:
server time.datum.com prefer
Host Name: grendel.datum.com
System Location:
Lexington, MA
Administrator Email:
unferth@datum.com
Mail Forwarder: mail.digitaldelivery.com

System Tests

Select which features you'd like to test:

☑ Test NTP
☑ Test Mail

Test Now

Please allow some time for tests to complete.

Click **Finish** to skip the tests.

[Start Over | Quit]

Reset | < Back | Finish

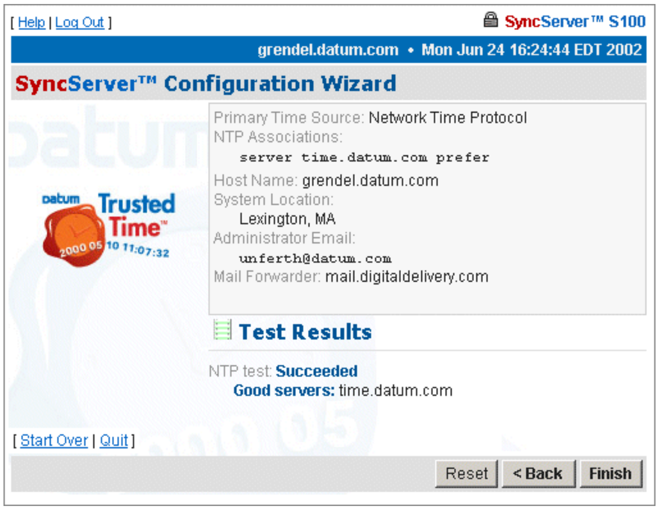
Figure 2-20: System Testing options

You can skip the test by clicking **Finish**, *or* initiate the test by clicking **Test Now**.

The default is to test all the services, so **NTP** and **E-Mail**, unless you un-check them, will be tested.

Click **Test Now**.

The *Test Results* dialog displays, with the results of your test.



[Help | Log Out]
SyncServer™ S100
grendel.datum.com • Mon Jun 24 16:24:44 EDT 2002
SyncServer™ Configuration Wizard
datum Trusted Time™
2000 05 10 11:07:32

Primary Time Source: Network Time Protocol
NTP Associations:

```
server time.datum.com prefer
```

Host Name: grendel.datum.com
System Location:
Lexington, MA
Administrator Email:
unferth@datum.com
Mail Forwarder: mail.digitaldelivery.com

Test Results

NTP test: Succeeded
Good servers: time.datum.com

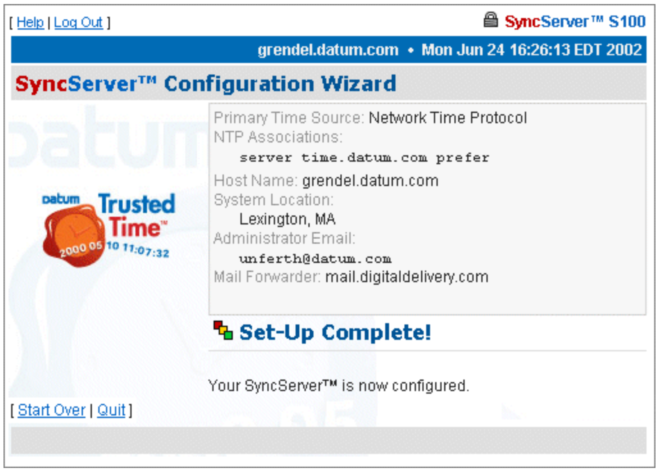
Figure 2-21: Test Results shown

What this tells you is the NTP time source for your SyncServer is functioning properly.

There is no output to the “Mail test” field. That is because mail is tested by sending an e-mail to the address that you indicated earlier.

Click **Finish**.

The *Setup Complete* screen displays.



[Help | Log Out]

SyncServer™ S100

grendel.datum.com • Mon Jun 24 16:26:13 EDT 2002

SyncServer™ Configuration Wizard

Primary Time Source: Network Time Protocol
NTP Associations:
server time.datum.com prefer
Host Name: grendel.datum.com
System Location:
Lexington, MA
Administrator Email:
unferth@datum.com
Mail Forwarder: mail.digitaldelivery.com

Set-Up Complete!

Your SyncServer™ is now configured.

[Start Over | Quit]

Figure 2-22: Your NTP set-up is complete

This screen verifies your configuration of your SyncServer:

- Its time source
- Host name
- System location
- Administrator e-mail

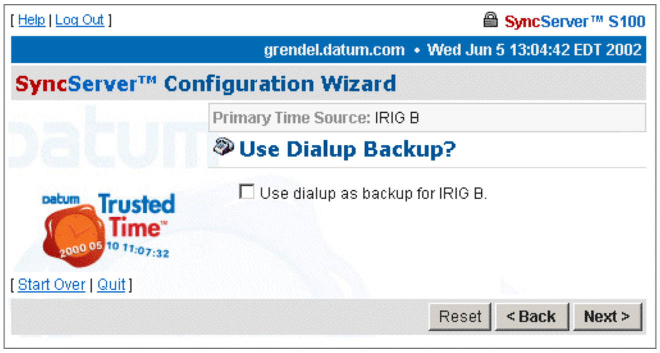
Configuring NTP

To configure NTP, use the NTP Relationships dialog of the interface, as described in Chapter 3. Use the dialog to view the NTP status and create the NTP associations.

IRIG B

With the optional Datum cable, you can reference time for your SyncServer via IRIG (timecode).

If you choose **IRIG B** and click **Next**, the *Dialup Backup* dialog displays.

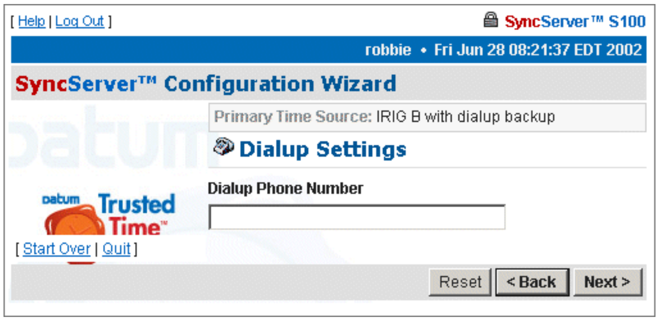


[Help | Log Out]
SyncServer™ S100
grendel.datum.com • Wed Jun 5 13:04:42 EDT 2002
SyncServer™ Configuration Wizard
Primary Time Source: IRIG B
Use Dialup Backup?
□ Use dialup as backup for IRIG B.
[Start Over | Quit]
Reset
< Back
Next >

Figure 2-23: Dialog Backup

If you wish to use dialup as a backup time source to GPS, click the checkbox next to **Use dialup for backup to IRIG B**, then the **Next** button.

If you do not want to back up your IRIG with dialup, leave the checkbox unselected, and click **Next**.



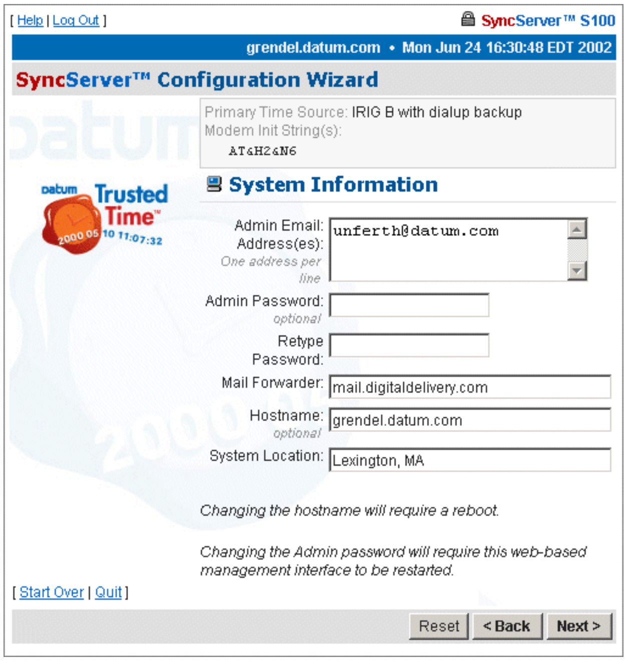
[Help | Log Out]
SyncServer™ S100
robbie • Fri Jun 28 08:21:37 EDT 2002
SyncServer™ Configuration Wizard
Primary Time Source: IRIG B with dialup backup
Dialup Settings
Dialup Phone Number
[Start Over | Quit]
Reset
< Back
Next >

Figure 2-24: Dialup Settings

If you do check **Use dialup as backup for IRIG**, this *Dialup Settings* dialog displays.

In the field, type in or paste in your **modem phone number**.

Then click **Next** for the *System Information* dialog



grendel.datum.com • Mon Jun 24 16:30:48 EDT 2002

SyncServer™ Configuration Wizard

Primary Time Source: IRIG B with dialup backup
Modem Init String(s):
AT&H2&N6

System Information

Admin Email: Address(es): unferth@datum.com
One address per line

Admin Password: optional

Retype Password:

Mail Forwarder: mail.digitaldelivery.com

Hostname: grendel.datum.com
optional

System Location: Lexington, MA

Changing the hostname will require a reboot.

Changing the Admin password will require this web-based management interface to be restarted.

Figure 2-25: System Info fields

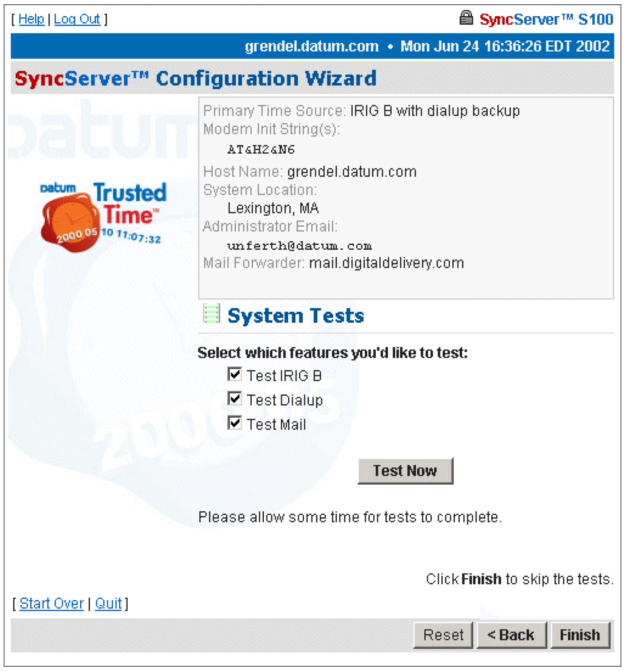
The *System Information* dialog shows you:

- Admin e-mail, for the administrator of the SyncServer
- Mail forwarder, or the SMTP server
- Host name
- System (SyncServer) location

Confirm the data that is in the fields. If it is not accurate, change it to the correct information.

Click **Next**.

The *System Tests* dialog displays.


[Help | Log Out]
SyncServer™ S100
grendel.datum.com • Mon Jun 24 16:36:26 EDT 2002
SyncServer™ Configuration Wizard
datum Trusted Time™

Primary Time Source: IRIG B with dialup backup
Modem Init String(s):
AT&H2&N6
Host Name: grendel.datum.com
System Location:
Lexington, MA
Administrator Email:
unferth@datum.com
Mail Forwarder: mail.digitaldelivery.com

System Tests

Select which features you'd like to test:

☑ Test IRIG B
☑ Test Dialup
☑ Test Mail

Please allow some time for tests to complete.

Click **Finish** to skip the tests.

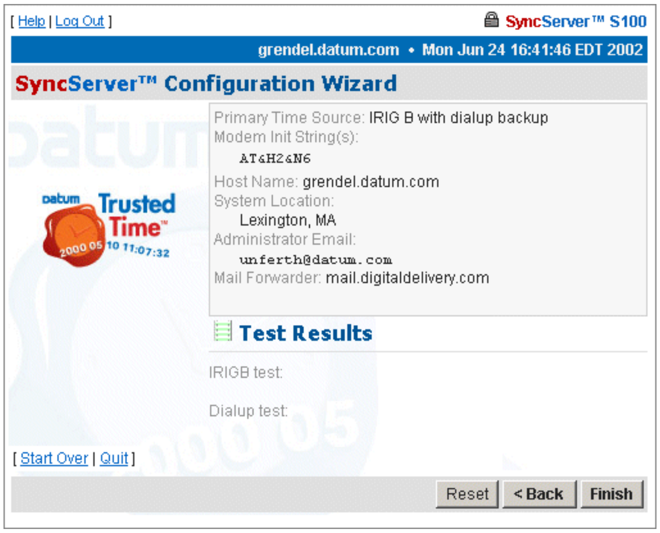
Figure 2-26: System Testing options

You can skip the test by clicking **Finish**, *or* initiate the test by clicking **Test Now**.

The default is to test all the services, so unless you un-check them, they all will be tested. If you do not use dialup as backup, it will not be listed here nor will it be tested.

Initiate the test by clicking **Test Now**.

The *Test Results* dialog displays, with the results of your test.


[Help | Log Out]
SyncServer™ S100
grendel.datum.com • Mon Jun 24 16:41:46 EDT 2002
SyncServer™ Configuration Wizard
datum Trusted Time™
2000 05 10 11:07:32

Primary Time Source: IRIG B with dialup backup
Modem Init String(s):
AT&H2&N6
Host Name: grendel.datum.com
System Location:
Lexington, MA
Administrator Email:
unferth@datum.com
Mail Forwarder: mail.digitaldelivery.com

Test Results

IRIGB test:

Dialup test:

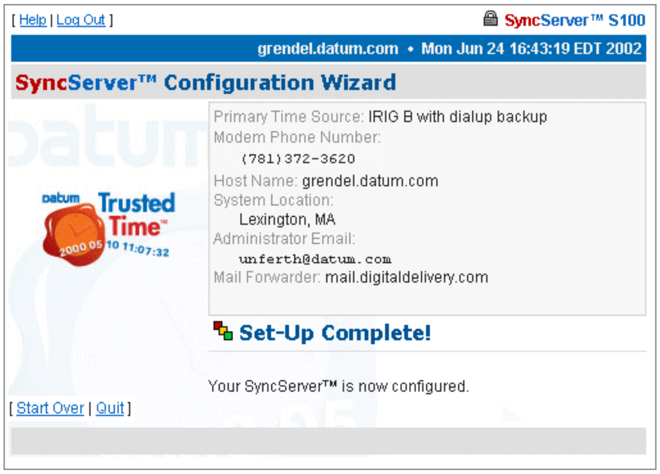
Figure 2-27: Test Results shown

What this tells you is the IRIG for your SyncServer is functioning properly.

There is no output to the “Mail test” field. That is because mail is tested by sending an e-mail to the address that you indicated earlier.

Click **Finish**.

The *Setup Complete* screen displays.



[Help | Log Out]
SyncServer™ S100
grendel.datum.com • Mon Jun 24 16:43:19 EDT 2002
SyncServer™ Configuration Wizard
datum Trusted Time™
2000 05 10 11:07:32

Primary Time Source: IRIG B with dialup backup
Modem Phone Number:
(781) 372-3620
Host Name: grendel.datum.com
System Location:
Lexington, MA
Administrator Email:
unferth@datum.com
Mail Forwarder: mail.digitaldelivery.com

Set-Up Complete!

Your SyncServer™ is now configured.

Figure 2-28: Your IRIG set-up is complete

This screen verifies your configuration of your SyncServer:

- Its time source
- Modem phone number (if you designated dialup as the backup source for time)
- Host name
- System location
- Administrator e-mail

Using DatumTime™

Next, you need to install client software to test NTP (Windows installation).

The DatumTime time utility is a handy way of doing this. It keeps accurate time on your client computer.

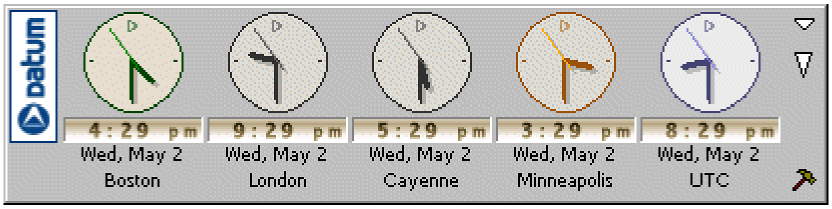


Figure 2-29 DatumTime™ Time Utility, sample configuration

Installing the DatumTime™ Client Software

1. On the client computer's hard drive, create a separate directory for DatumTime.
2. Copy the `Datumtime.exe` file from the utility disk into this directory.
3. Double-click `Datumtime.exe`. This will install the program onto your computer.
4. Configure the clocks the way you want by using the Build tool (click on the hammer in the lower right corner).
5. Right-click on the displayed clocks for the menu and select **Sync Servers**.
6. On the dialog that opens, click **Add Server**.
7. In the New Server dialog, enter the **IP address** and **location** of the SyncServer. Click **OK**.
8. Click **OK**.

To synchronize DatumTime:

1. Right-click anywhere on the clocks. Select **Sync Status** to tell your computer when to automatically get time from the SyncServer.
2. Click **Sync Now**. If you get a non-response, it is because you have not yet configured the SyncServer; configure it now. An affirmative response confirms you have configured the SyncServer.

Next: Use the Web-Based Interface

Now that you have established your SyncServer as a network appliance, and have configured your time source and installed your client software, you can use the web-based interface to manage SyncServer operations. See Chapter 3 for complete descriptions.

Chapter 3

The Web-Based Interface

Overview

The following is a description of the web-based software interface that you use to manage SyncServer.

This material is designed to be a reference for you as you use your SyncServer. It also describes some of the procedures that will help you begin using your S100.

Datum recommends you review this section before beginning the permanent installation of your S100, so that you will be familiar with it when you need to use it.

If you are not familiar with Network Time Protocol, we recommend that you use the NTPD Help link in the interface menu to review the NTP Distribution document (source: University of Delaware) embedded in the SyncServer interface. Reading through this document, and using the links within it, will give you an in-depth information about NTP.

Interface: Screen Reference

The SyncServer management interface has been designed with ease of use in mind. As a result, you access the management interface SyncServer through any web browser. This section describes the screens used in the interface, including their functions. It supplies some procedural instructions, as well.

Each dialog or screen, except in the Config Wizard, lets you *refresh* that screen or open a *new window*, and all will let you *log out*.

For security reasons, the interface will time out after 20 minutes if there is no activity.

Logging In

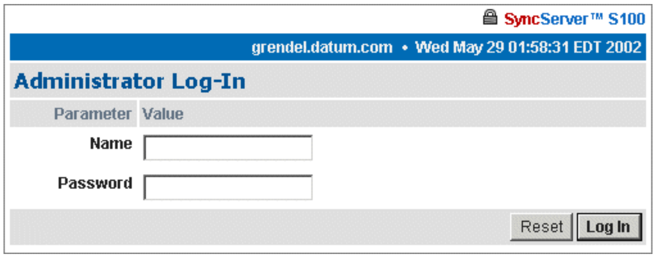


Figure 3-1: Logging In

This dialog displays once you enter the SyncServer's IP address or click on the link to or icon for your SyncServer S100.

Enter the default user name, **`admin`**, and default password, **`datum`**.

Assuming this is the first time you have logged in, you will see the System Status screen.

Log-ins after this first log-in will bring you to the last screen you accessed in your most recent session.

Administrative Interface

This is your main tool as you use your SyncServer.

If you click *Refresh* at the top of any screen, it will remove any confirmation or error messages on the screen.

If you click *New Window* at the top of any screen, it opens a second browser window without the admin menu.

Admin Interface: Base Menu

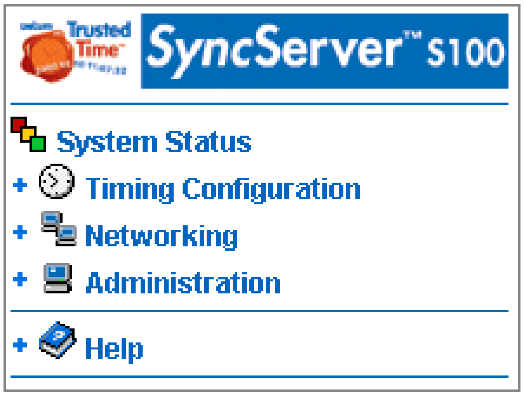


Figure 3-2: Administrative Interface: Base Menu

The first thing you see on the left of your screen is the base **Administrative** (Admin) **Menu**. This is your "home base" interface as you use SyncServer.

Click on each "+" symbol to see that portion of the menu expand.

Administrative Menu: Expanded

Expanding each item on the base menu shows you all the available options. Click on *Collapse* (at the bottom of the menu) to revert to the base version of the menu.

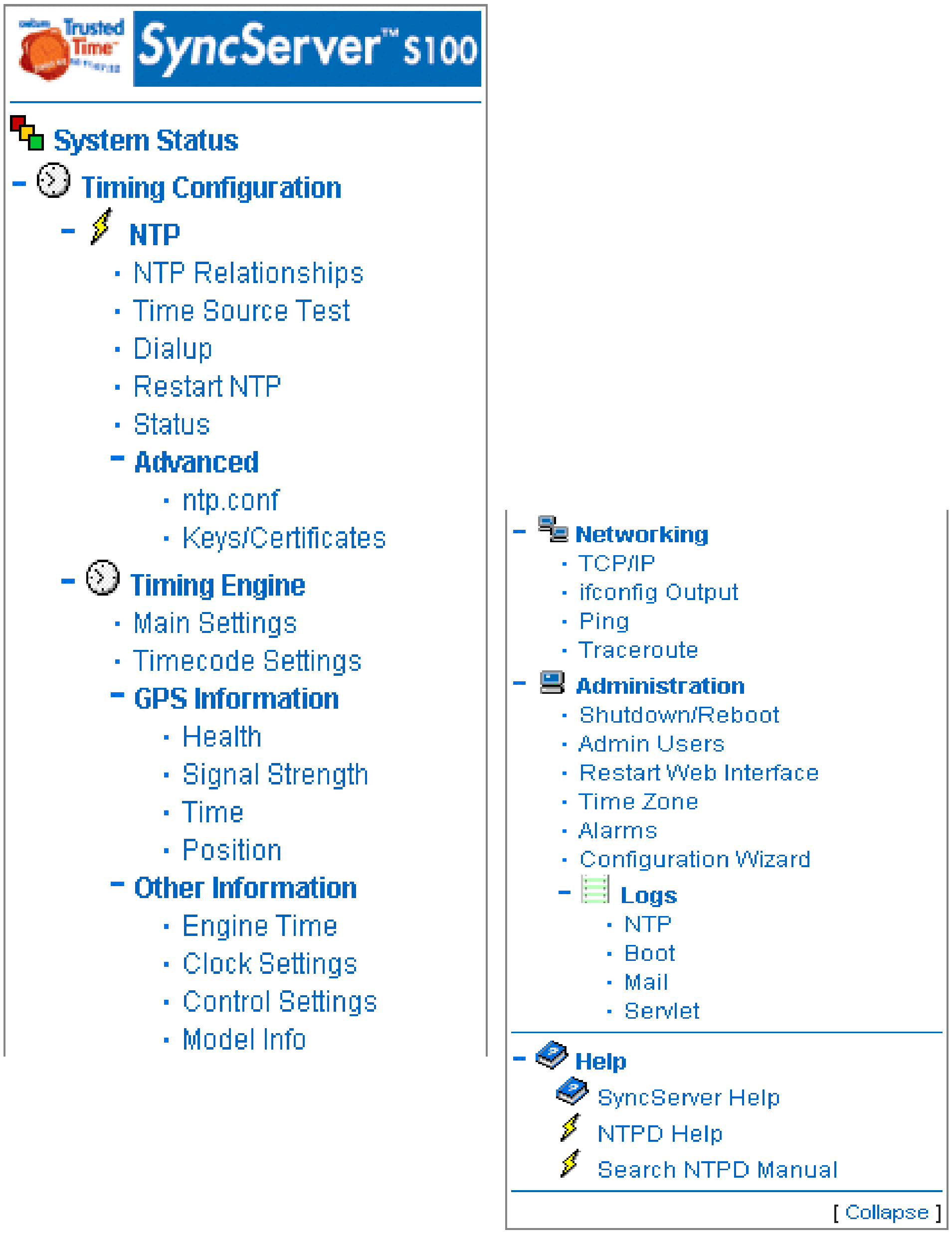
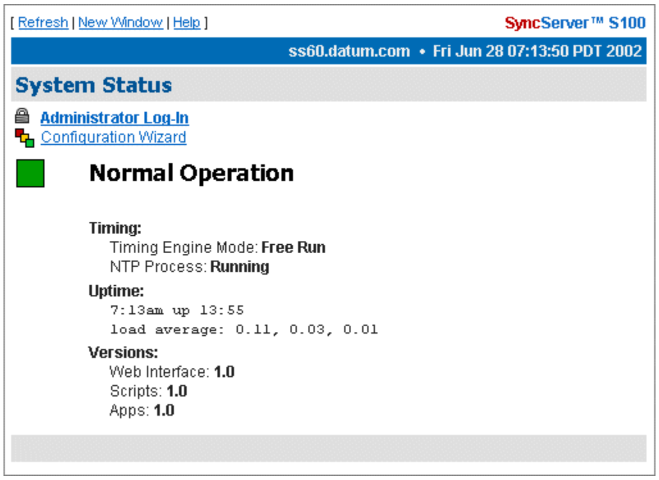


Figure 3-3: Interface Admin Menu, expanded

System Status



[Refresh | New Window | Help]
SyncServer™ S100
ss60.datum.com • Fri Jun 28 07:13:50 PDT 2002
System Status
Administrator Log-In
Configuration Wizard

🟩 Normal Operation

Timing:
Timing Engine Mode: **Free Run**
NTP Process: **Running**

Uptime:

```
7:13am up 13:55
load average: 0.11, 0.03, 0.01
```

Versions:
Web Interface: **1.0**
Scripts: **1.0**
Apps: **1.0**

Figure 3-4: Checking the Status

Clicking this item, you will quickly see the status of your SyncServer.

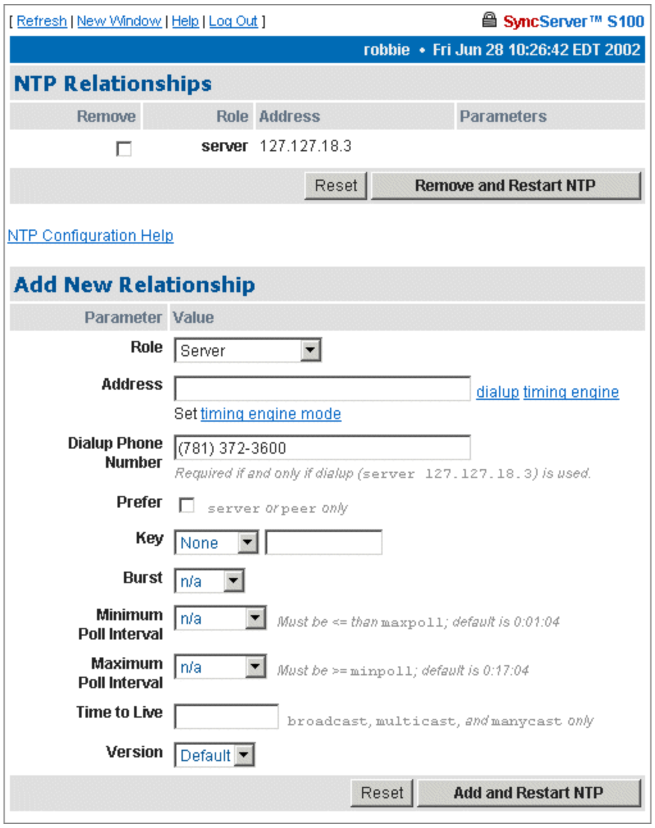
The color of the box on the left side of the page is your guide. It follows the traffic light convention:

- Green = Normal Operation: SyncServer up and running with the correct time
- Amber = Unsatisfactory: Some settings still need attention before secure time can be issued
- Red = Unsatisfactory: System not yet ready to issue time

Timing Configuration

These menu options let you manage NTP, the heart of the SyncServer system. For more details on each of the NTP terms used here, see NTPD Help.

NTP Relationships



NTP Relationships

Remove	Role	Address	Parameters
□	server	127.127.18.3	

Add New Relationship

Parameter	Value
Role	Server
Address	dialup timing engine Set timing engine mode
Dialup Phone Number	(781) 372-3600 *Required if and only if dialup (server 127.127.18.3) is used.*
Prefer	□ *server or peer only*
Key	None
Burst	n/a
Minimum Poll Interval	n/a *Must be <= than maxpoll; default is 0:01:04*
Maximum Poll Interval	n/a *Must be >= minpoll; default is 0:17:04*
Time to Live	*broadcast, multicast, and manycast only*
Version	Default

Figure 3-5: Configuring New Clients and Servers

Use this option to configure NTP. Essentially, here you define the relationships between and among this host and other hosts.

For more details, see the **NTPD Help**.

In the *NTP Associations* panel of this screen you see the configuration of the network that you are putting the SyncServer on. These are all the devices the SyncServer will supply time to, and/or get time from. They are named (as server, peer, or client) depending on their relationship to the SyncServer.

In this section, clicking **Reset** clears any data you've just added, and clicking **Remove and Restart NTP** deletes the checked host(s).

The *Add New Relationships* panel lets you add a host to your configuration. Next to each parameter, enter the values for the clients you are adding to the configuration:

Role - The host you add can serve in any one of these roles:

- A peer
- Client
- Server
- Broadcast
- Manycast client
- Broadcast client
- Manycast server
- Multicast client

Address - Here, enter the IP address or host name for the host you are adding.

Dialup, *timing engine*, and *Set timing engine mode* links - Use these links to populate the address field appropriately.

Dialup Phone Number - Here, enter the modem phone number you will be using.

Prefer - This marks the server as "preferred", meaning this server, of all the correctly operating hosts and if all things are equal, will be the host chosen for synchronization.

Key (NTPv4 only) - All packets sent to and received from the server or peer will include authentication fields encrypted using the specified key.

- **None**: The default, no encryption field.
- **Key=** : This is the index of the key in the keystore.
- **Autokey**: All packets sent to and received from the server or peer include authentication fields encrypted using the autokey scheme.

Burst - Data grouped for transmission, in these ways:

- **N/A**: If you choose this option, the Burst command will not be executed.
- **Burst**: Selecting this option tells the system that when the server is reachable, send eight packets instead of one.
- **iBurst**: Selecting this option tells the system that when the server is *not* reachable, send eight packets and keep trying every 16 seconds.

Minimum Poll Interval - Indicate in seconds the smallest measure of time in which you want the SyncServer to check the network hosts' time. If you enter nothing here, the SyncServer will use the default, 0:01:04 seconds.

Maximum Poll Interval - Indicate in seconds the largest measure of time in which you want the SyncServer to check the network hosts' time. If you enter nothing here, the SyncServer will use the default, 0:17:04 seconds.

Time to Live - Data in the Internet Protocol that specifies how many more hops a packet can travel before being discarded or returned, here entered in the form of whole numbers.

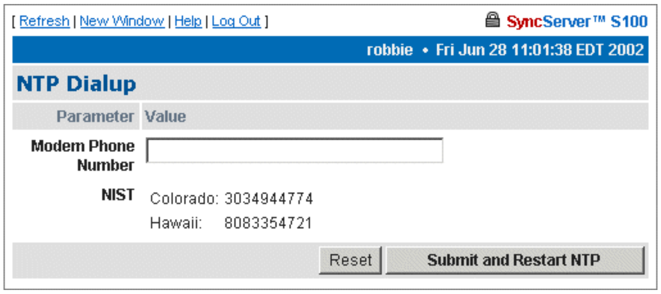
Version - These are Default, 1, 2, 3, or 4.

Clicking **Reset** clears the data you've just entered.

Clicking **Add and Restart NTP** adds the data you've just entered and restarts NTP.

When you are finished with the addition of any new clients, they will display in the NTP Relationships panel at the top of the screen.

NTP Dialup



robbie • Fri Jun 28 11:01:38 EDT 2002

NTP Dialup

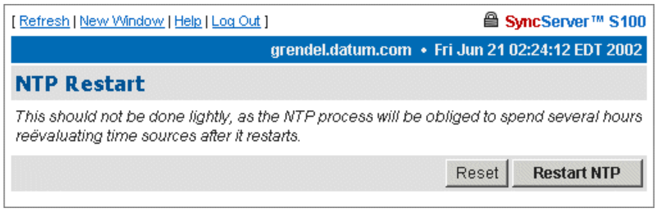
Parameter	Value
Modem Phone Number	
NIST	Colorado: 3034944774 Hawaii: 8083354721

Figure 3-6: NTP Dialup

In this dialog, type in or paste in your **modem phone number**.

Then click **Submit**.

NTP Restart



grendel.datum.com • Fri Jun 21 02:24:12 EDT 2002

NTP Restart

This should not be done lightly, as the NTP process will be obliged to spend several hours reëvaluating time sources after it restarts.

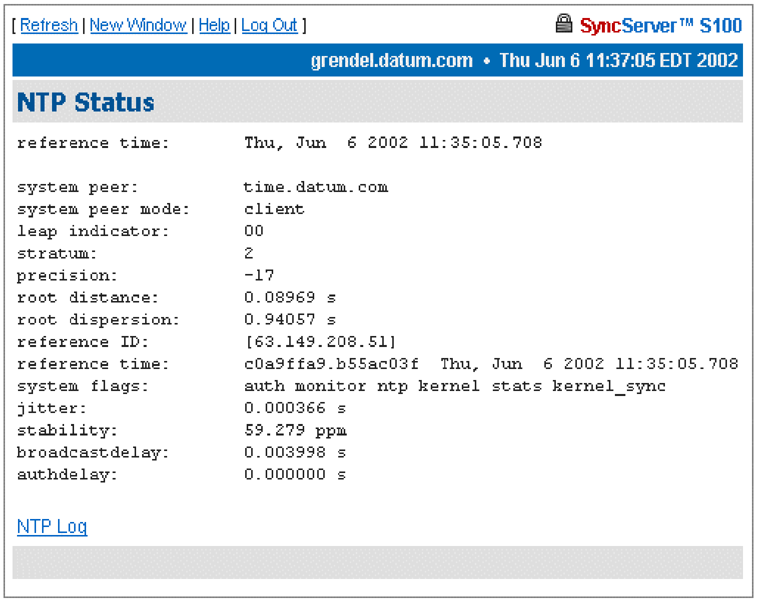
Figure 3-7: Restart NTP Here

Here, you can restart the NTP daemon, for troubleshooting purposes only.

Please note the following warning:

Warning!
It can take NTP a significant period of time to go through its processes. If you choose to restart, you will be required to reset your time source.

NTP Status


[Refresh | New Window | Help | Log Out]
SyncServer™ S100
grendel.datum.com • Thu Jun 6 11:37:05 EDT 2002

NTP Status

```
reference time:       Thu, Jun  6 2002 11:35:05.708

system peer:          time.datum.com
system peer mode:     client
leap indicator:       00
stratum:              2
precision:            -17
root distance:        0.08969 s
root dispersion:      0.94057 s
reference ID:         [63.149.208.51]
reference time:       c0a9ffa9.b55ac03f  Thu, Jun  6 2002 11:35:05.708
system flags:         auth monitor ntp kernel stats kernel_sync
jitter:               0.000366 s
stability:            59.279 ppm
broadcastdelay:       0.003998 s
authdelay:            0.000000 s
```

Figure 3-8: Snapshot of NTP Status

This screen gives you the following information:

Reference Time - This is the last time it synced.

System Peer - This tells you which NTP server your S100 is synced to.

System Peer Mode - This tells you what your SyncServer is—client or otherwise—to the NTP server it is synced to.

Leap Indicator - This is a two-bit code warning of an impending leap second. The numbers mean:

00 = no warning

01 = the last minute has 61 seconds

10 = the last minute has 59 seconds

11 = alarm condition (clock not synchronized)

Stratum - This is the stratum level of your S100.

Precision - This is an eight-bit signed integer indicating the precision of the local clock, in seconds to the nearest power of two. The range is -6 to -18.

Root Distance, or *root delay* - This is a signed fixed-point number indicating the total roundtrip delay to the primary reference source at the root of the synchronization subnet, in seconds. It can be expressed as either a positive or negative number.

Root Dispersion - A 32-bit unsigned fixed point number indicating the maximum error relative to the primary reference source, in seconds (milliseconds).

Reference ID - A 4-byte code indicating the reference source. If the reference source is stratum 0, this string will identify the type of source (GPS or dial-up, for example). If the source is stratum 1 or higher, this 4-byte code will contain the IP address of the reference source.

Reference Time - The local time at which the local clock was last set or corrected, in a 64-bit time-stamp format.

System Flags - These are various flags which can be enabled or disabled through the configuration commands.

Jitter - Distortion of a signal caused by some weakness in synchronization, here shown in seconds (milliseconds).

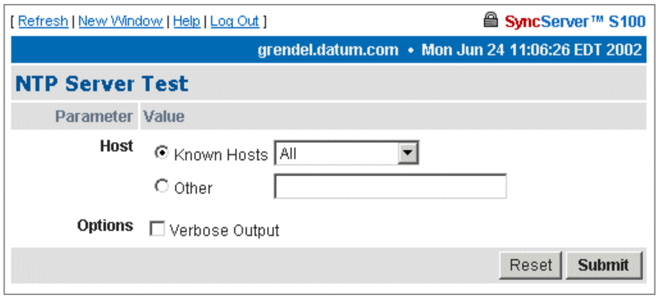
Stability - This is the residual frequency error remaining after the system frequency correction is applied. Used most often in maintenance, the value starts as high as 500 ppm but settles into the .01 to 0.1 ppm range.

Broadcastdelay - This shows the default broadcast delay.

authdelay - This is the default authentication delay.

NTP Time Source Test

The *NTP Server Test* dialog lets you test the servers you designated in the NTP Relationships dialog, above.



[Refresh | New Window | Help | Log Out]

SyncServer™ S100

grendel.datum.com • Mon Jun 24 11:06:26 EDT 2002

NTP Server Test

Parameter	Value
Host	● Known Hosts All ○ Other
Options	□ Verbose Output

Figure 3-9: Testing the NTP Time Source

Host -

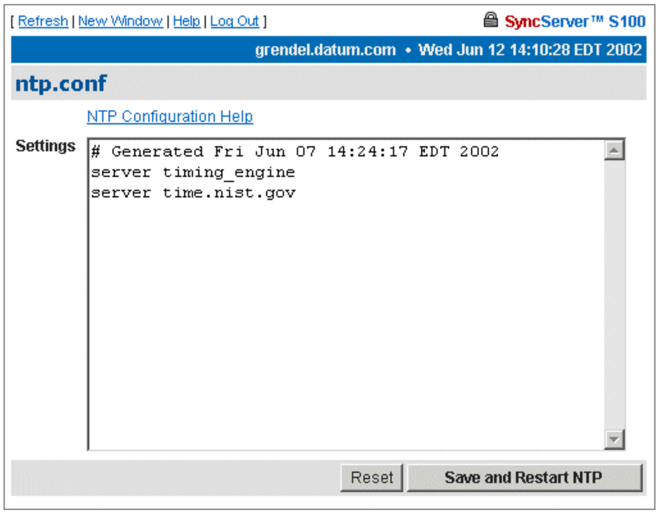
- All
- 127.127.40.0
- 127.127.18.3
- Dialup
- localhost

Options - Use the checkbox to enable **Verbose Output**, which will give you details.

NTP Advanced Configuration

Here you will find advanced configuration features of NTP. You probably won't need to access these, but they are here if you need to edit the configuration.

Advanced: ntp.conf


[Refresh | New Window | Help | Log Out]
SyncServer™ S100
grendel.datum.com • Wed Jun 12 14:10:28 EDT 2002
ntp.conf
NTP Configuration Help
Settings
Reset
Save and Restart NTP

```
# Generated Fri Jun 07 14:24:17 EDT 2002
server timing_engine
server time.nist.gov
```

Figure 3-10: Viewing the NTP Configuration File

This dialog is only for those with advanced knowledge of NTP.

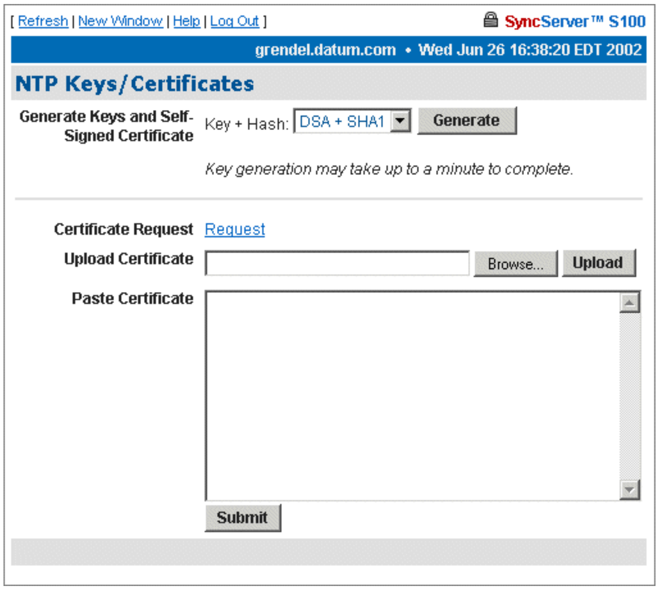
The dialog displays the NTP configuration file. It allows you to edit the config text file.

If you need help with the NTP config file, click on the **NTP Configuration Help** link near the top of the screen, and you will be directed to NTP Help. Or, use the resources at www.ntp.org.

⚠	**Warning!** If you improperly configure the ntp.conf, you will render the SyncServer unable to sync to any time source. Be certain you know NTP well enough to do this.

Advanced: Keys/Certificates

Use this *NTP Keys/Certificates* dialog to obtain a digital certificate that verifies the identity of the SyncServer S100.



[Refresh | New Window | Help | Log Out]

SyncServer™ S100

grendel.datum.com • Wed Jun 26 16:38:20 EDT 2002

NTP Keys/Certificates

Generate Keys and Self-Signed Certificate — Key + Hash: DSA + SHA1

Key generation may take up to a minute to complete.

Certificate Request — Request

Upload Certificate

Paste Certificate

Figure 3-11: Obtaining and Generating Keys and Certificates

Work from top to bottom:

Generate Keys - Select the key algorithm and hash algorithm you wish to use:

- RSA + MD5
- RSA + SHA1
- DSA + SHA1

DSA + SHA1 is the default.

Then click **Generate**.

The screen refreshes and a “keys generated” message displays in the upper left corner.

Next to the *Certificate Request* field, click **Request** to issue a certificate request. A confirmation dialog will prompt you to tell the system where you want the certificate; respond to the prompt.

If you choose *Upload Certificate*, browse to the certificate request, as sent to you by the certificate authority, or type in its name. Then click **Upload**.

You can choose, instead, *Paste Certificate*, which does the same thing as *Upload Certificate*. First use Notepad or other editor to open the `certreq.jsp` file, then copy the contents. These should be base 64 encoded. Paste the contents in the field here, then click **Submit**.

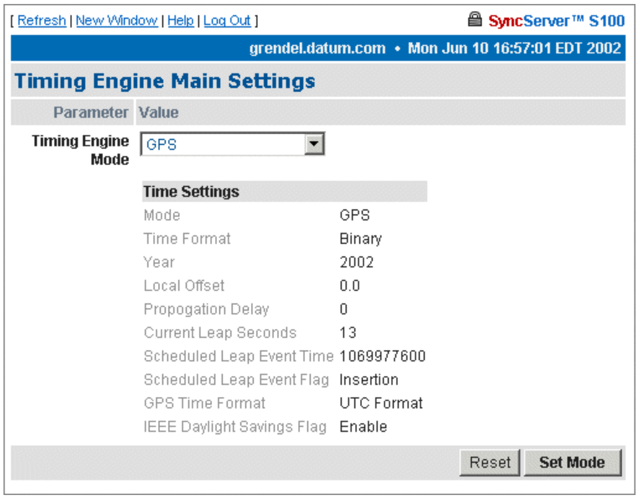
The SyncServer is self-signed, thus it can verify your certificate.

For more about how SyncServer uses NTP keys and certificates, see Chapter 1, SyncServer and NTPv4's Security Features.

Timing Engine

This section of the interface lets you view various aspects of the Datum bc635/637 PCI board, which is the timing engine of your SyncServer S100.

Main Settings



[Refresh | New Window | Help | Log Out]   SyncServer™ S100

grendel.datum.com • Mon Jun 10 16:57:01 EDT 2002

Timing Engine Main Settings

Parameter	Value
Timing Engine Mode	GPS

Time Settings	
Mode	GPS
Time Format	Binary
Year	2002
Local Offset	0.0
Propogation Delay	0
Current Leap Seconds	13
Scheduled Leap Event Time	1069977600
Scheduled Leap Event Flag	Insertion
GPS Time Format	UTC Format
IEEE Daylight Savings Flag	Enable

Figure 3-12: Timing Engine Main Settings

The timing engine mode choices you see in the drop-down list box are:

- **GPS** is the default, which obtains time via the Global Positioning System antenna
- **IRIG**
- **Free Running** means there is no external timing source used, that the time is set manually
- One Pulse Per Second, or **1PPS**, syncs the oscillator to a user-supplied 1PPS
- Real-Time Clock, or **RTC**, synchronizes the oscillator to the 1PPS signal from the timing engine itself

Mode - How time is being acquired.

Time Format - The timing engine uses Binary code time.

Year - Set the year here.

Local Offset - Allowed values are -16 through +16, and can include half-hour offsets.

Propagation Delay - If there is any propagation delay from the reference source, the timing engine will adjust for it. Values range from -9999999 to +9999999.

Current Leap Seconds - This figure accounts for the local offset.

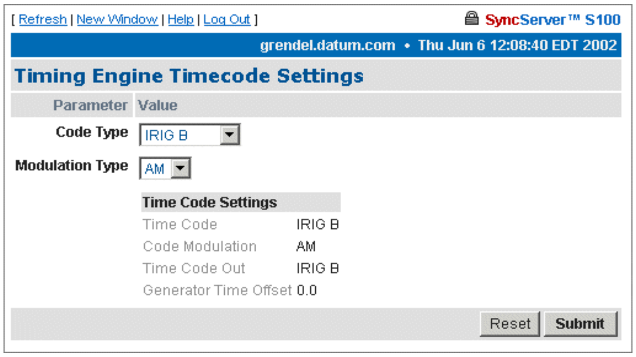
Scheduled Leap Event Time - This is a 32-bit binary value corresponding to the number of seconds elapsed since 0 hour January 1, 1970 UTC.

Scheduled Leap Event Flag - This will alert you to an upcoming leap event.

GPS Time Format - UTC is the default.

IEEE Daylight Savings Flag - This alerts you to an upcoming Daylight Savings Time event.

Timecode Settings



grendel.datum.com • Thu Jun 6 12:08:40 EDT 2002

Timing Engine Timecode Settings

Parameter	Value
Code Type	IRIG B
Modulation Type	AM

Time Code Settings	
Time Code	IRIG B
Code Modulation	AM
Time Code Out	IRIG B
Generator Time Offset	0.0

Figure 3-13: Timecode Settings

Code type choices in the drop-down list box are:

- IRIG A
- IRIG B
- IEEE 1344
- NASA 36

Code Type - This identifies the time code in setting.

Modulation Type - The type associated with the time code signal:

- **AM**, for amplitude modulated
- **DC**, for direct current level shift, or digital IRIG

The default modulation envelope is AM.

Time Code Settings - This confirms the settings:

- Time Code = The time code *in* setting
- Code Modulation = The modulation type associated with the time code signal
- Time Code Out = The time code *out* setting

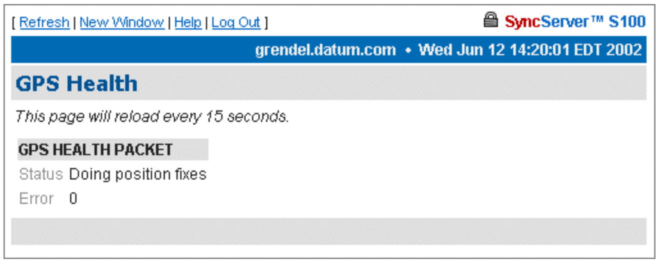
- Generator Time Offset = This shows any offset to the time code signal being produced by the timing engine.

Clicking **Reset** lets you clear any data you've entered, and **Submit** implements changes you have made.

GPS Information

These next few items give details on GPS activity:

GPS Health



grendel.datum.com • Wed Jun 12 14:20:01 EDT 2002

GPS Health

This page will reload every 15 seconds.

GPS HEALTH PACKET

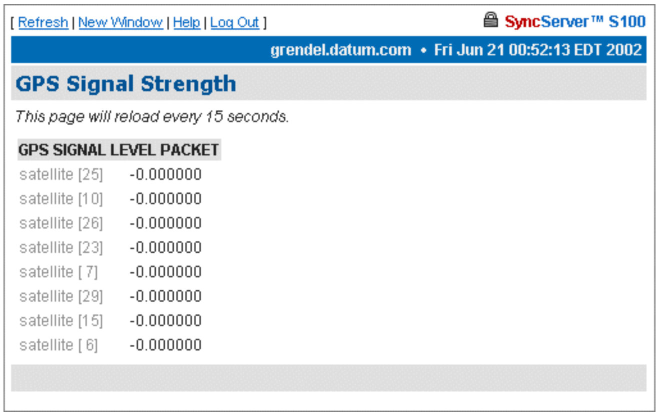
Status Doing position fixes

Error 0

Figure 3-14: GPS Health Status

This screen updates the signal status. This example shows a normal screen.

GPS Signal Strength



grendel.datum.com • Fri Jun 21 00:52:13 EDT 2002

GPS Signal Strength

This page will reload every 15 seconds.

GPS SIGNAL LEVEL PACKET

satellite [25]	-0.000000
satellite [10]	-0.000000
satellite [26]	-0.000000
satellite [23]	-0.000000
satellite [7]	-0.000000
satellite [29]	-0.000000
satellite [15]	-0.000000
satellite [6]	-0.000000

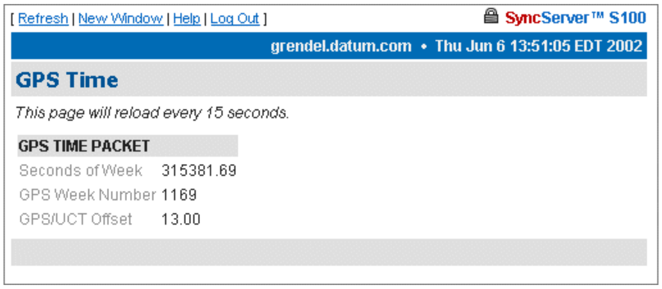
Figure 3-15: GPS Signal Strength

Here, the signal strength and position are displayed.

The data is for the satellites that are currently being tracked:

- The satellite number
- The db level for each satellite

GPS Time



grendel.datum.com • Thu Jun 6 13:51:05 EDT 2002

GPS Time

This page will reload every 15 seconds.

GPS TIME PACKET	
Seconds of Week	315381.69
GPS Week Number	1169
GPS/UCT Offset	13.00

Figure 3-16: GPS Time

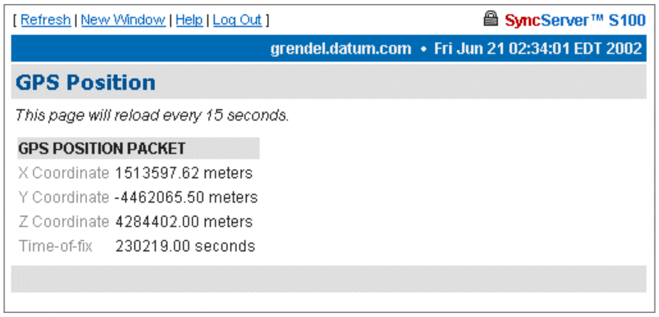
GPS time is noted here.

Seconds of Week - This is expressed in the number of seconds since January 6, 1980 (GPS Week).

GPS Week Number -This is expressed in the number of weeks since January 6, 1980.

GPS/UTC Offset - Currently this is 13 seconds.

GPS Position



grendel.datum.com • Fri Jun 21 02:34:01 EDT 2002

GPS Position

This page will reload every 15 seconds.

GPS POSITION PACKET	
X Coordinate	1513597.62 meters
Y Coordinate	-4462065.50 meters
Z Coordinate	4284402.00 meters
Time-of-fix	230219.00 seconds

Figure 3-17: GPS Position

This screen shows you where the satellites are.

X Coordinate = Latitude

Y Coordinate = Longitude

Z Coordinate = Altitude

Time-of-fix = Time

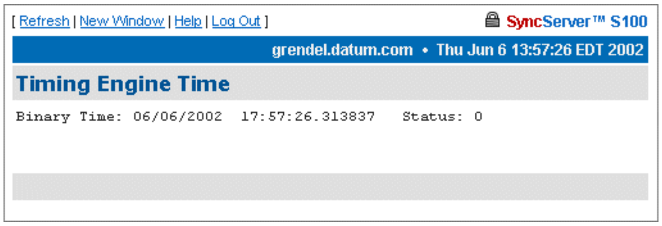
For more about GPS position, see Chapter 1, SyncServer and the Global Positioning System.

Other Information

The following screens give additional information about your SyncServer.

Engine Time

The engine time is expressed in binary time.



[Refresh | New Window | Help | Log Out]

SyncServer™ S100

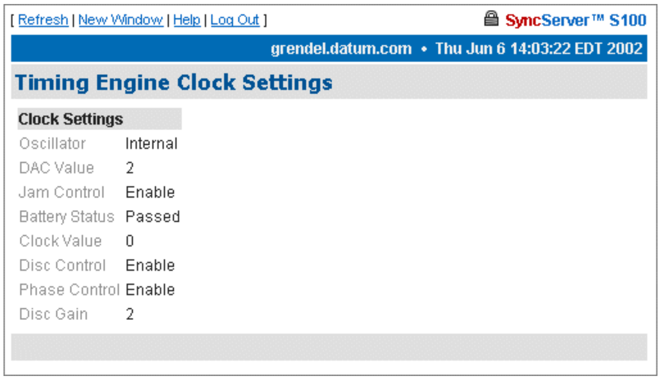
grendel.datum.com • Thu Jun 6 13:57:26 EDT 2002

Timing Engine Time

```
Binary Time: 06/06/2002  17:57:26.313837   Status: 0
```

Figure 3-18: Timing Engine Time

Clock Settings



[Refresh | New Window | Help | Log Out]

SyncServer™ S100

grendel.datum.com • Thu Jun 6 14:03:22 EDT 2002

Timing Engine Clock Settings

Clock Settings	
Oscillator	Internal
DAC Value	2
Jam Control	Enable
Battery Status	Passed
Clock Value	0
Disc Control	Enable
Phase Control	Enable
Disc Gain	2

Figure 3-19: Clock Settings

The clock settings here are:

Oscillator - This is *internal* to the timing engine.

DAC Value - A 16-bit Digital Analog Converter is used to set the frequency on the oscillator. The value here shows a rate match between the hardware clock frequency and the selected time reference source.

Jam Control - “Jam” refers to *jam synchronization*. This controls whether or not the software may “jam” the clock circuitry if a phase discontinuity of greater than 1 millisecond is found.

Battery Status - The timing engine’s battery status is noted here.

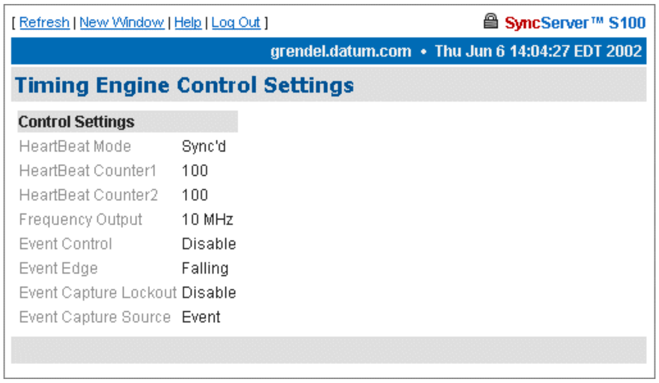
Clock Value - This register shows the number of 100ns steps needed to advance or slow dowm the phase of the local clock circuit.

Disc Control - Short for *disciplining control*, this disciplining function is the part of the software which matches the local clock phase and frequency with the selected time reference function.

Phase Control - Short for *local clock phase shifting*, this function shows if the software is shifting the one-second rollover point of the local hardware clock by a specified amount.

Disc Gain - Short for *oscillator disciplining function gain value*, this is a scalar value which sets the gain for the Kalman filter so it can discipline the local oscillator to the selected time reference.

Control Settings


[Refresh | New Window | Help | Log Out]
SyncServer™ S100
grendel.datum.com • Thu Jun 6 14:04:27 EDT 2002

Timing Engine Control Settings

Control Settings	
HeartBeat Mode	Sync'd
HeartBeat Counter1	100
HeartBeat Counter2	100
Frequency Output	10 MHz
Event Control	Disable
Event Edge	Falling
Event Capture Lockout	Disable
Event Capture Source	Event

Figure 3-20: Control Settings

HeartBeat Mode - The *heartbeat* is the specified frequency.

HeartBeat Counter1 and *2* - These are internal counters to the timing engine.

Frequency Output - The available frequencies are 1, 5, and 10 MHz.

Event Control - This setting enables or disables the ability of the internal clock to capture the time at which an external event occurs.

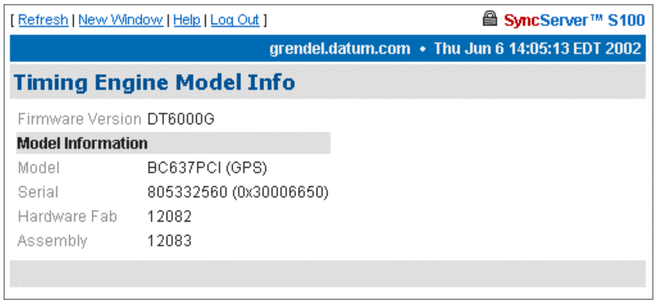
Event Edge - This is either the *rising* or *falling* edge of the heartbeat signal.

Event Capture Lockout - If enabled, the capture lockout can be used to control whether or not subsequent signals will overwrite the data in the timing engine's event time registers.

Event Capture Source - This setting controls the source of the external event—an external event input or strobe, for example.

Model Info

Here you see some basic data about the bc635/637 PCI board, the timing engine of your S100.


[Refresh | New Window | Help | Log Out]
SyncServer™ S100
grendel.datum.com • Thu Jun 6 14:05:13 EDT 2002

Timing Engine Model Info

Firmware Version DT6000G

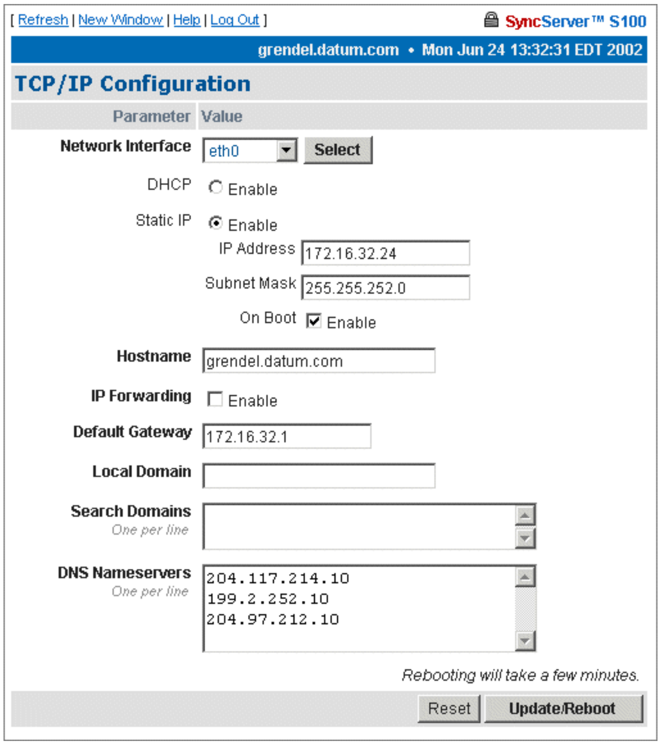
Model Information	
Model	BC637PCI (GPS)
Serial	805332560 (0x30006650)
Hardware Fab	12082
Assembly	12083

Figure 3-21: Model Info

Networking

Use these dialogs to configure several parameters of your SyncServer on your network.

Networking: TCP/IP



[Refresh | New Window | Help | Log Out] SyncServer™ S100

grendel.datum.com • Mon Jun 24 13:32:31 EDT 2002

TCP/IP Configuration

Parameter	Value
Network Interface	eth0
DHCP	○ Enable
Static IP	● Enable
IP Address	172.16.32.24
Subnet Mask	255.255.252.0
On Boot	☑ Enable
Hostname	grendel.datum.com
IP Forwarding	□ Enable
Default Gateway	172.16.32.1
Local Domain	
Search Domains One per line	
DNS Nameservers One per line	204.117.214.10 199.2.252.10 204.97.212.10

Rebooting will take a few minutes.

Figure 3-22: Configuring TCP/IP

This dialog enables you to define these parameters:

Network Interface - Here, choose which Ethernet port you are using. If there is only one interface, use **eth0**, the default. A **local loopback** refers to a loopback plug inserted in one of the ports; a signal is transmitted and returned to the sending device and the returned signal is compared with the transmitted signal in order to evaluate the integrity of the equipment or transmission path.

DHCP - This is the Dynamic Host Configuration Protocol, which assigns an IP address to each node in a network. Here, the default is *Enable*.

Static IP - Click the radio button to *Enable*, then enter the SyncServer’s IP address, subnet mask, and default gateway.

The setting for *On Boot* is defaulted to *Enable*. Uncheck this box if you do not want the IP address when you reboot.

Local Domain - This is your local domain name.

Search Domains - The system will search these domains—which usually include your local domain as well as others—so it can resolve any unresolved host names that may be missing the host, local, or top level portion of the name.

Hostname - Enter the SyncServer's name here.

IP Forwarding - You can redirect data from one IP address to another by checking *Enable* here.

DNS Nameservers - These are the DNS servers on the network.

Reset - Click this button to return to the previous settings.

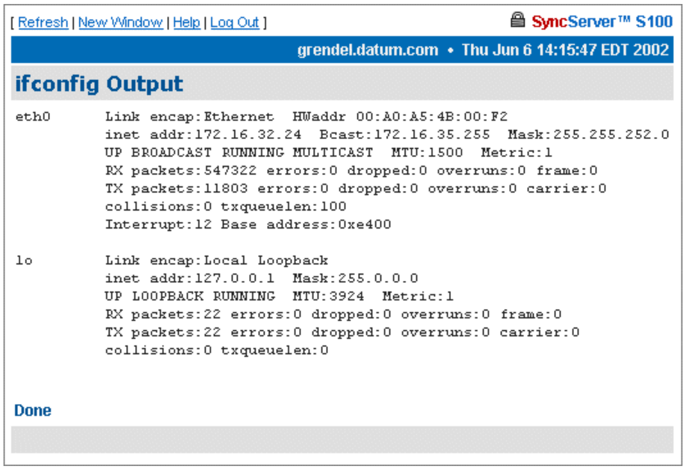
Update/Reboot - Click this button to reboot the server, but first, please note the warning:

⚠	**Warning** If you click **Update/Reboot**, you will reboot the server, and will need to reacquire time. Be certain you want to do this.

If you choose to do this, a confirmation message will display at the top if this screen.

Networking: ifconfig Output

This screen gives you information about the network configuration of your SyncServer. It lets you troubleshoot network problems.

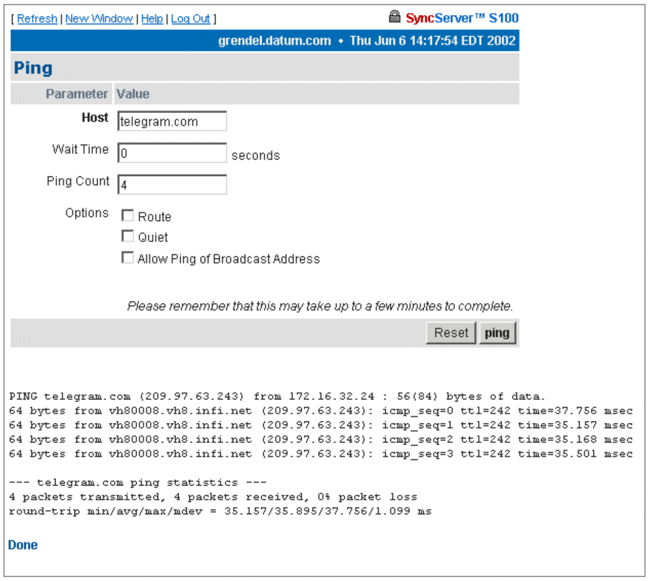

[Refresh | New Window | Help | Log Out]
SyncServer™ S100
grendel.datum.com • Thu Jun 6 14:15:47 EDT 2002
ifconfig Output
Done

```
eth0      Link encap:Ethernet  HWaddr 00:A0:A5:4B:00:F2
          inet addr:172.16.32.24  Bcast:172.16.35.255  Mask:255.255.252.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:547322 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11803 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          Interrupt:12 Base address:0xe400

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:3924  Metric:1
          RX packets:22 errors:0 dropped:0 overruns:0 frame:0
          TX packets:22 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
```

Figure 3-23: Configuration Information

Networking: Ping



[Refresh | New Window | Help | Log Out]
SyncServer™ S100
grendel.datum.com • Thu Jun 6 14:17:54 EDT 2002

Ping

Parameter	Value
Host	telegram.com
Wait Time	0 seconds
Ping Count	4
Options	□ Route □ Quiet □ Allow Ping of Broadcast Address

Please remember that this may take up to a few minutes to complete.

```
PING telegram.com (209.97.63.243) from 172.16.32.24 : 56(84) bytes of data.
64 bytes from vh80008.vh8.infi.net (209.97.63.243): icmp_seq=0 ttl=242 time=37.756 msec
64 bytes from vh80008.vh8.infi.net (209.97.63.243): icmp_seq=1 ttl=242 time=35.157 msec
64 bytes from vh80008.vh8.infi.net (209.97.63.243): icmp_seq=2 ttl=242 time=35.168 msec
64 bytes from vh80008.vh8.infi.net (209.97.63.243): icmp_seq=3 ttl=242 time=35.501 msec

--- telegram.com ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/mdev = 35.157/35.895/37.756/1.099 ms
```

Figure 3-24: Pinging the Remote Host

Use the ping command to test the network route between the SyncServer and a remote host.

This is a diagnostic tool that confirms that all is well between the two devices.

This dialog lets you define these parameters:

Host - URL of the remote host

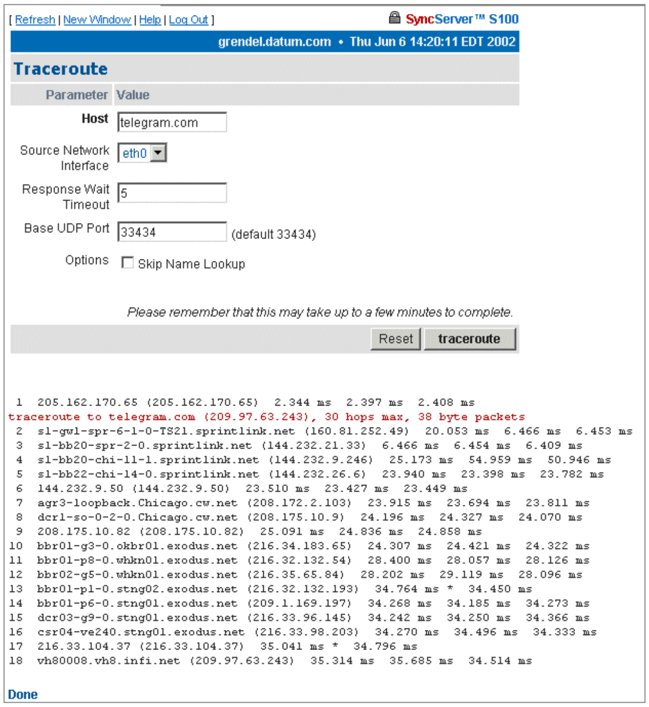
Wait time - Response time between pings

Ping count - Try to ping this number of times before quitting

Options -

- **Route**: Gives detailed information about the route followed between two hosts
- **Quiet**: No output until done
- **Allow Ping of Broadcast Address**: Lets you ping broadcast addresses so all machines in a broadcast group can respond

Networking: Traceroute


[Refresh | New Window | Help | Log Out]
SyncServer™ S100
grendel.datum.com • Thu Jun 6 14:20:11 EDT 2002

Traceroute

Parameter	Value
Host	telegram.com
Source Network Interface	eth0
Response Wait Timeout	5
Base UDP Port	33434 (default 33434)
Options	□ Skip Name Lookup

Please remember that this may take up to a few minutes to complete.

```
 1  205.162.170.65 (205.162.170.65)  2.344 ms  2.397 ms  2.408 ms
traceroute to telegram.com (209.97.63.243), 30 hops max, 38 byte packets
 2  sl-gwl-spr-6-1-0-TS21.sprintlink.net (160.81.252.49)  20.053 ms  6.466 ms  6.453 ms
 3  sl-bb20-spr-2-0.sprintlink.net (144.232.21.33)  6.466 ms  6.454 ms  6.409 ms
 4  sl-bb20-chi-11-1.sprintlink.net (144.232.9.246)  25.173 ms  54.959 ms  50.946 ms
 5  sl-bb22-chi-14-0.sprintlink.net (144.232.26.6)  23.940 ms  23.398 ms  23.782 ms
 6  144.232.9.50 (144.232.9.50)  23.510 ms  23.427 ms  23.449 ms
 7  agr3-loopback.Chicago.cw.net (208.172.2.103)  23.915 ms  23.694 ms  23.811 ms
 8  dcr1-so-0-2-0.Chicago.cw.net (208.175.10.9)  24.196 ms  24.327 ms  24.070 ms
 9  208.175.10.82 (208.175.10.82)  25.091 ms  24.836 ms  24.858 ms
10  bbr01-g3-0.okbr01.exodus.net (216.34.183.65)  24.307 ms  24.421 ms  24.322 ms
11  bbr01-p8-0.whkn01.exodus.net (216.32.132.54)  28.400 ms  28.057 ms  28.126 ms
12  bbr02-g5-0.whkn01.exodus.net (216.35.65.84)  28.202 ms  29.119 ms  28.096 ms
13  bbr01-p1-0.stng02.exodus.net (216.32.132.193)  34.764 ms *  34.450 ms
14  bbr01-p6-0.stng01.exodus.net (209.1.169.197)  34.268 ms  34.185 ms  34.273 ms
15  dcr03-g9-0.stng01.exodus.net (216.33.96.145)  34.242 ms  34.250 ms  34.366 ms
16  csr04-ve240.stng01.exodus.net (216.33.98.203)  34.270 ms  34.496 ms  34.333 ms
17  216.33.104.37 (216.33.104.37)  35.041 ms *  34.796 ms
18  vh80008.vh8.infi.net (209.97.63.243)  35.314 ms  35.685 ms  34.514 ms
```

Figure 3-25: Seeing the Traceroute

Traceroute shows you the network route between the SyncServer and a remote host. Use it as a diagnostic tool.

This dialog lets you determine these parameters:

Host - Remote server's IP address

Source Network Interface - SyncServer has two Ethernet cards, 0 (zero, left) and 1 (right). The default is **eth0**, as you see here.

Response Wait Timeout - This is how long the SyncServer should wait for a host respond.

Base UDP Port - This refers to the User Datagram Protocol port number. The default is port 33434.

Options -

- **Skip Name Lookup**: If you check this, SyncServer will not take the time to look up the host names of the intermediate hosts along the path.

Administration

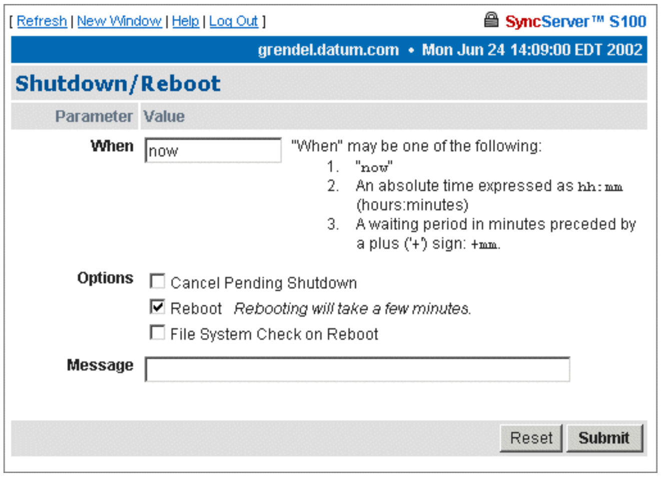
Here, configure non-NTP features of SyncServer.

You can also shut down or restart the SyncServer.

Administration: Shutdown/Reboot

This option shuts down the network connection.

WARNING!
If you click **Shutdown,** you will shut down the SyncServer's network connection.


[Refresh | New Window | Help | Log Out]
SyncServer™ S100
grendel.datum.com • Mon Jun 24 14:09:00 EDT 2002
Reset
Submit

Shutdown/Reboot

Parameter	Value
When	now "When" may be one of the following: 1. "now" 2. An absolute time expressed as hh:mm (hours:minutes) 3. A waiting period in minutes preceded by a plus ('+') sign: +mm.
Options	□ Cancel Pending Shutdown ☑ Reboot *Rebooting will take a few minutes.* □ File System Check on Reboot
Message	

Figure 3-26: Shutdown/Reboot

When - Using a 24-hour clock, enter the time here.

Options - These are:

- **Cancel Pending Shutdown**: Lets you cancel a shutdown
- **Reboot**: The default setting. Useful if you need to shut down and restart the hardware and software. This is very handy if the SyncServer is remote.
- **File System Check on Reboot**: Here the system checks for errors, lost clusters, and other problems.

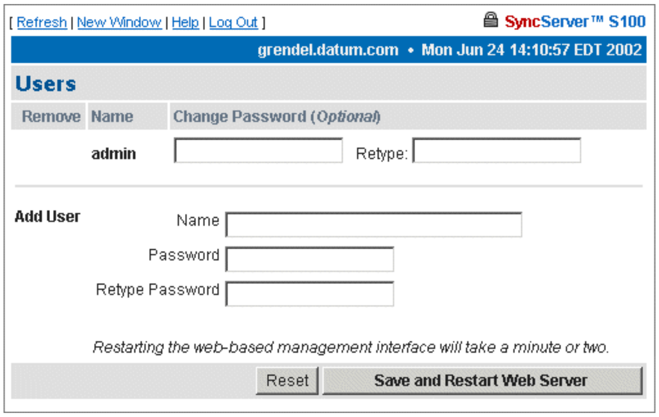
Message - Here, enter a message that would be sent only to someone who might be logged in via Secure Shell.

Reset - Click here to clear the data you have entered.

Submit - Clicking here disconnects the server from the network.

Administration: Admin Users

Use this dialog to change, delete, or add a user.


[Refresh | New Window | Help | Log Out]
SyncServer™ S100
Users
Remove
Name
Change Password (Optional)
admin
Retype:
Add User
Name
Password
Retype Password
Reset
Save and Restart Web Server

grendel.datum.com • Mon Jun 24 14:10:57 EDT 2002

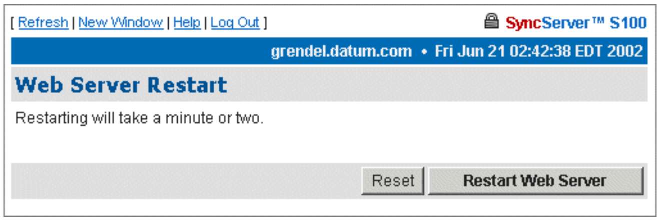
Restarting the web-based management interface will take a minute or two.

Figure 3-27: Changing or Adding Users

Administration: Restart Web Interface

This page lets you do a clean restart of the web server.

WARNING
If you click **Restart**, you will shut down the webserver, then it will restart. This will take a minute or two to complete.



grendel.datum.com • Fri Jun 21 02:42:38 EDT 2002

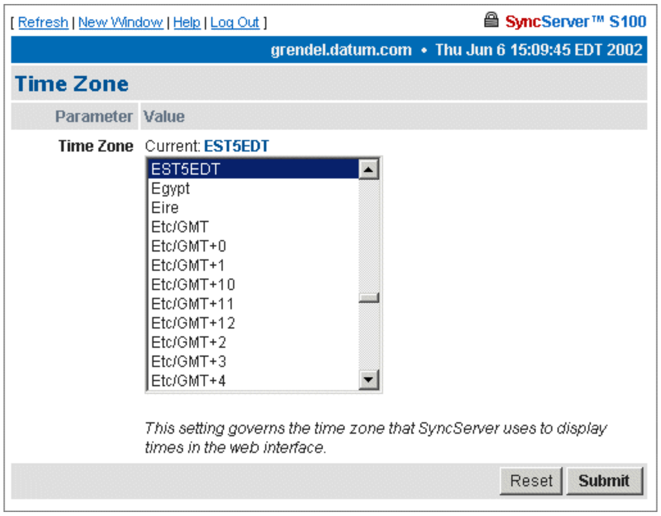
Web Server Restart

Restarting will take a minute or two.

Figure 3-28: Server Restart option

The restart affects only the management of the system, not the time or service.

Administration: Time Zone



grendel.datum.com • Thu Jun 6 15:09:45 EDT 2002

Time Zone

Parameter	Value
Time Zone	Current: EST5EDT

This setting governs the time zone that SyncServer uses to display times in the web interface.

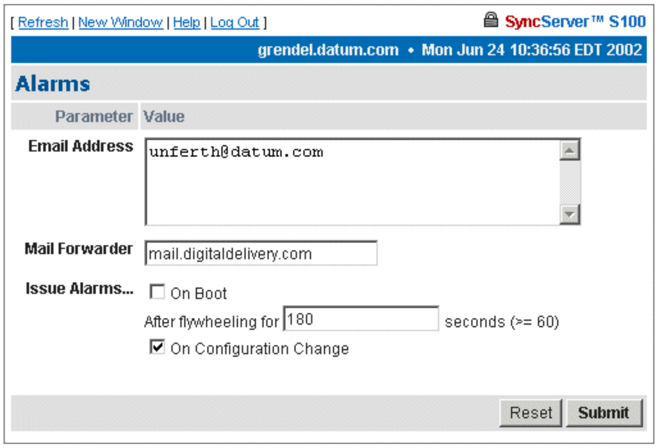
Figure 3-29: Setting the Time Zone

Use this option to set the time zone displayed in the web-based admin interface.

NOTE: The time zone is for display purposes only. It will not affect NTP, the output, or clients.

Highlight the time zone you want, then click **Submit** to set the time zone.

Administration: Alarms



[Refresh | New Window | Help | Log Out] SyncServer™ S100

grendel.datum.com • Mon Jun 24 10:36:56 EDT 2002

Alarms

Parameter	Value
Email Address	unferth@datum.com
Mail Forwarder	mail.digitaldelivery.com
Issue Alarms...	□ On Boot After flywheeling for 180 seconds (>= 60) ☑ On Configuration Change

Figure 3-30: Setting Alarm Parameters

E-mail Address - This e-mail address is where any alarm messages will be sent.

Mail forwarder - The server that will handle the e-mail.

Issue Alarms - Here, check when you want alarms sent:

- Upon boot, and if **Flywheeling** continues for more than 60 seconds. If you check here for this alarm, it will tell you that the system has lost contact with its source of time but will keep going for some period.
- If there has been a **Configuration Change**, you can check here for an alarm to be sent.

Reset lets you clear the entered data, and **Submit** tells the system you are finished.

Config Wizard

The next item on the Admin menu is the Config Wizard. This helps you select and configure your time reference.

Step-by-step Config Wizard instructions are in Chapter 2, The Config Wizard.

Logs

You can access the **NTP**, **Boot**, **Mail**, and **Servlet** logs through either the admin menu or in the drop-down list box in the Logs parameter.

All the logs have these parameters and values:

Logs - This drop-down list box lets you access other logs from this screen.

The size of the log you choose will be displayed beneath the drop-down box.

Filter -

- **No filter:** Will show you all logs
- **Display only the last __ lines:** Useful for avoiding screen clutter
- **Search:** Search feature allows you to see what has happened on any given day.

Checking the **case-blind** option lets you ignore case in your search.

Checking the **line numbers** option lets you base the search on log line numbers.

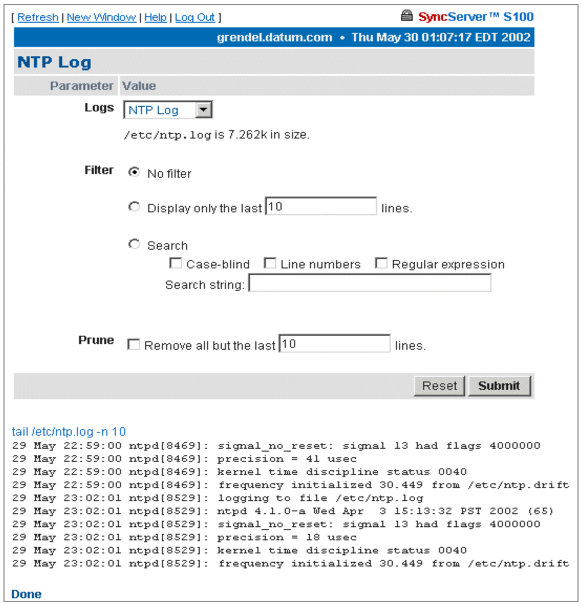
Choosing **regular expression** allows for pattern matching in your search.

Prune -

Remove all but the last __ lines: Lets you pare down the log after you have viewed it.

NTP Log

Use this log to see NTP activity.


[Refresh | New Window | Help | Log Out]
SyncServer™ S100
grendel.datum.com • Thu May 30 01:07:17 EDT 2002
Parameter
Value
Reset
Submit
Done

NTP Log

Logs: NTP Log

/etc/ntp.log is 7.262k in size.

Filter:
● No filter
○ Display only the last 10 lines.
○ Search
□ Case-blind □ Line numbers □ Regular expression
Search string:

Prune: □ Remove all but the last 10 lines.

tail /etc/ntp.log -n 10

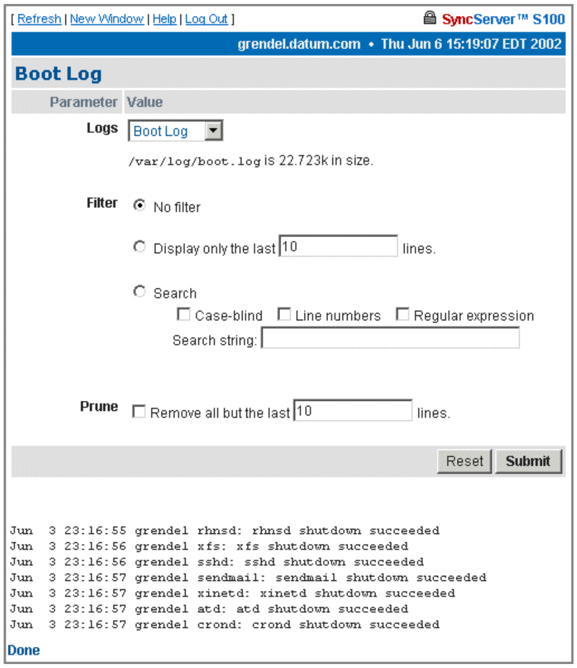
```
29 May 22:59:00 ntpd[8469]: signal_no_reset: signal 13 had flags 4000000
29 May 22:59:00 ntpd[8469]: precision = 41 usec
29 May 22:59:00 ntpd[8469]: kernel time discipline status 0040
29 May 22:59:00 ntpd[8469]: frequency initialized 30.449 from /etc/ntp.drift
29 May 23:02:01 ntpd[8529]: logging to file /etc/ntp.log
29 May 23:02:01 ntpd[8529]: ntpd 4.1.0-a Wed Apr  3 15:13:32 PST 2002 (65)
29 May 23:02:01 ntpd[8529]: signal_no_reset: signal 13 had flags 4000000
29 May 23:02:01 ntpd[8529]: precision = 18 usec
29 May 23:02:01 ntpd[8529]: kernel time discipline status 0040
29 May 23:02:01 ntpd[8529]: frequency initialized 30.449 from /etc/ntp.drift
```

Figure 3-31: NTP Log

Boot Log

Use this log to see what has happened, if anything, since your last boot.

Here you can see the whole process, helpful when you want to find the cause of a problem.


[Refresh | New Window | Help | Log Out]
SyncServer™ S100
grendel.datum.com • Thu Jun 6 15:19:07 EDT 2002
Boot Log
Parameter
Value
Reset
Submit
Done

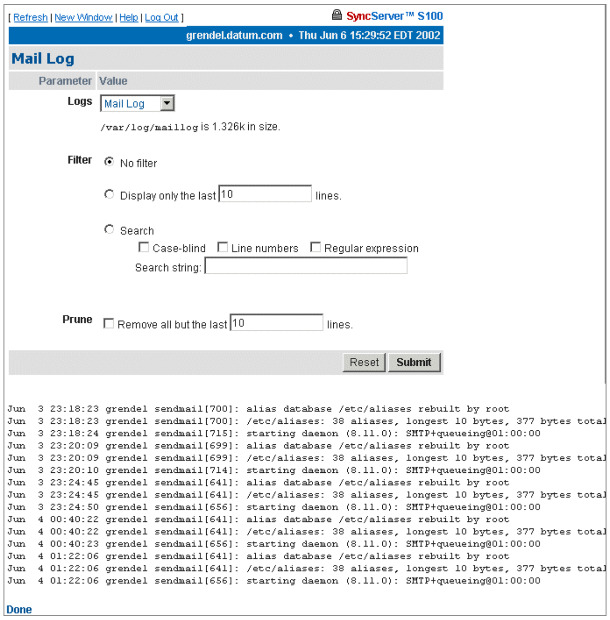
Logs	Boot Log ▾ /var/log/boot.log is 22.723k in size.
Filter	● No filter ○ Display only the last 10 lines. ○ Search □ Case-blind □ Line numbers □ Regular expression Search string:
Prune	□ Remove all but the last 10 lines.

```
Jun  3 23:16:55 grendel rhnsd: rhnsd shutdown succeeded
Jun  3 23:16:56 grendel xfs: xfs shutdown succeeded
Jun  3 23:16:56 grendel sshd: sshd shutdown succeeded
Jun  3 23:16:57 grendel sendmail: sendmail shutdown succeeded
Jun  3 23:16:57 grendel xinetd: xinetd shutdown succeeded
Jun  3 23:16:57 grendel atd: atd shutdown succeeded
Jun  3 23:16:57 grendel crond: crond shutdown succeeded
```

Figure 3-32: Boot Log

Mail Log

Use this log to monitor mail activity on the system.



[Refresh | New Window | Help | Log Out]
SyncServer™ S100
grendel.datum.com • Thu Jun 6 15:29:52 EDT 2002
Mail Log

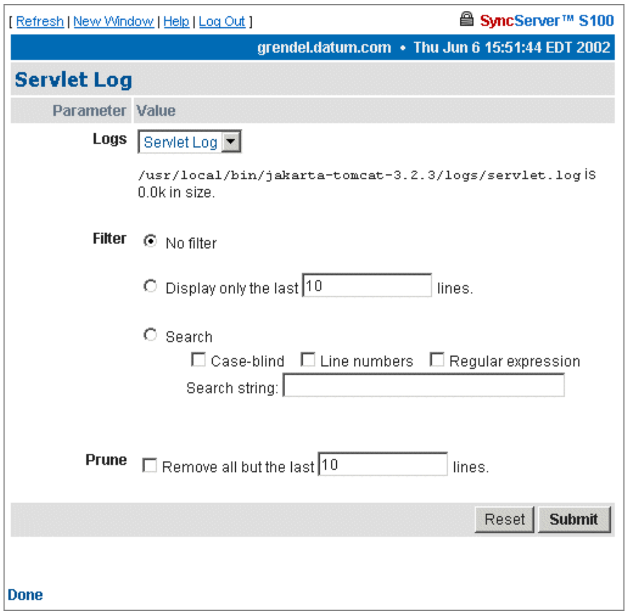
Parameter	Value
Logs	Mail Log ▾ /var/log/maillog is 1.326k in size.
Filter	● No filter ○ Display only the last 10 lines. ○ Search □ Case-blind □ Line numbers □ Regular expression Search string:
Prune	□ Remove all but the last 10 lines.

```
Jun  3 23:18:23 grendel sendmail[700]: alias database /etc/aliases rebuilt by root
Jun  3 23:18:23 grendel sendmail[700]: /etc/aliases: 38 aliases, longest 10 bytes, 377 bytes total
Jun  3 23:18:24 grendel sendmail[715]: starting daemon (8.11.0): SMTP+queueing@01:00:00
Jun  3 23:20:09 grendel sendmail[699]: alias database /etc/aliases rebuilt by root
Jun  3 23:20:09 grendel sendmail[699]: /etc/aliases: 38 aliases, longest 10 bytes, 377 bytes total
Jun  3 23:20:10 grendel sendmail[714]: starting daemon (8.11.0): SMTP+queueing@01:00:00
Jun  3 23:24:45 grendel sendmail[641]: alias database /etc/aliases rebuilt by root
Jun  3 23:24:45 grendel sendmail[641]: /etc/aliases: 38 aliases, longest 10 bytes, 377 bytes total
Jun  3 23:24:50 grendel sendmail[656]: starting daemon (8.11.0): SMTP+queueing@01:00:00
Jun  4 00:40:22 grendel sendmail[641]: alias database /etc/aliases rebuilt by root
Jun  4 00:40:22 grendel sendmail[641]: /etc/aliases: 38 aliases, longest 10 bytes, 377 bytes total
Jun  4 00:40:23 grendel sendmail[656]: starting daemon (8.11.0): SMTP+queueing@01:00:00
Jun  4 01:22:06 grendel sendmail[641]: alias database /etc/aliases rebuilt by root
Jun  4 01:22:06 grendel sendmail[641]: /etc/aliases: 38 aliases, longest 10 bytes, 377 bytes total
Jun  4 01:22:06 grendel sendmail[656]: starting daemon (8.11.0): SMTP+queueing@01:00:00
```

Figure 3-33: Mail Log

Servlet Log

This log shows you activity of the Tomcat Java webserver.



[Refresh | New Window | Help | Log Out]
SyncServer™ S100
grendel.datum.com • Thu Jun 6 15:51:44 EDT 2002
Servlet Log
Parameter
Value
Reset
Submit
Done

Logs: Servlet Log

/usr/local/bin/jakarta-tomcat-3.2.3/logs/servlet.log is 0.0k in size.

Filter: ● No filter

○ Display only the last 10 lines.

○ Search

□ Case-blind □ Line numbers □ Regular expression

Search string:

Prune: □ Remove all but the last 10 lines.

Figure 3-34: Servlet Log

Help

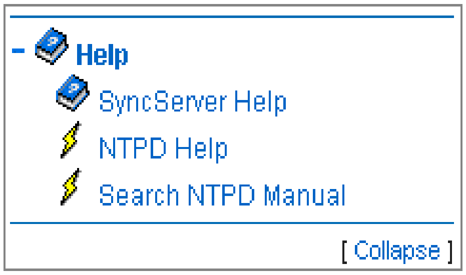


Figure 3-35: Help Options

This is the last section of the SyncServer admin menu. Available **Help** functions are:

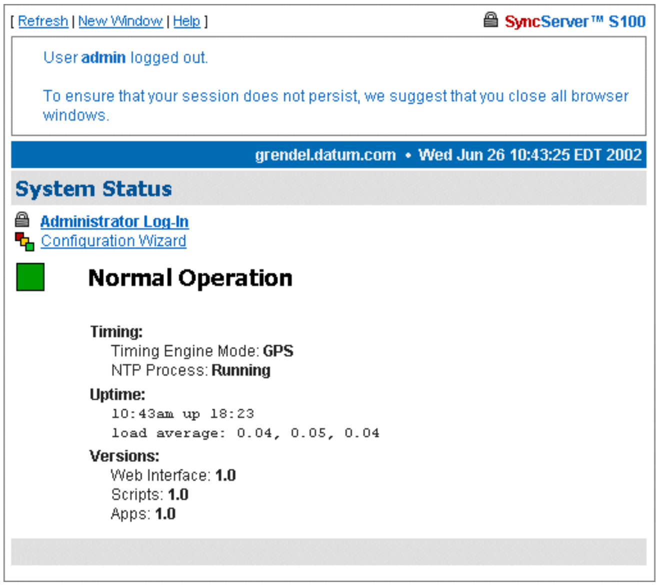
SyncServer Help
This is the application Help. Use the Table of Contents, Index, or Search to find information.

NTPD Help
For detailed information about NTP, click here. This links you to NTP documentation, embedded here for your convenience.

Search NTPD Manual
This option gives you the ability to do basic searches within the NTPD Help.

Collapse Button
Click the *Collapse* button at the bottom right of the admin menu to reduce the menu down to its main elements.

Logging Off



User **admin** logged out.

To ensure that your session does not persist, we suggest that you close all browser windows.

grendel.datum.com • Wed Jun 26 10:43:25 EDT 2002

System Status

Administrator Log-In

Configuration Wizard

🟩 **Normal Operation**

Timing:
Timing Engine Mode: **GPS**
NTP Process: **Running**

Uptime:
```
10:43am up 18:23
load average: 0.04, 0.05, 0.04
```

Versions:
Web Interface: **1.0**
Scripts: **1.0**
Apps: **1.0**

Figure 3-36 Log Out screen

Log off by clicking **Log Out**, at the top of each screen within the interface.

You will see the *System Status* screen with some prompts. At this point, you can choose among these options:

- Log back in
- Go to the Config Wizard, which will require you to log back in but will then take you directly to the wizard
- Continue the logoff by closing your browser

Chapter 4

SyncServer Operations and Time-Related Protocols

Overview

This section reviews the basic SyncServer operations, and time protocols used.

SyncServer: Operations and Time Protocols

Following are details about the time protocols SyncServer uses.

Time Protocol (RFC 868)

This protocol provides a site-independent, machine-readable date and time. The time service on the SyncServer responds to the originating source with the time in seconds since midnight of January 1, 1900. The time is the *number of seconds* since 00:00

(midnight) January 1, 1900 GMT. So the time "1" is 12:00:01 A.M. on January 1, 1900 GMT. This base will serve until the year 2036.

If the server is unable to determine the time, it either refuses the connection or it closes the connection without sending any response.

When used over the Transmission Control Protocol (TCP), the SyncServer listens for a connection on port 37; once the connection is established, the server returns a 32-bit time value and closes the connection. When used over the User Datagram Protocol (UDP), the SyncServer listens for a datagram on port 37. When a datagram arrives, the SyncServer returns a datagram containing the 32-bit time value.

Daytime Protocol (RFC 867)

The Daytime protocol sends the current date and time as a character string without regard to the input.

When used over TCP, the SyncServer listens for a connection on port 13; once a connection is established the current date and time is sent out as an ASCII character string. The service closes the connection after sending the quote.

When used over UDP, the SyncServer listens for a datagram on port 13. SyncServer responds to the UDP request with the current date and time as an ASCII character string.

Simple Network Time Protocol (RFC 2030)

Simple Network Time Protocol (SNTP) is a simplified access protocol for servers and clients using NTP as it is now used on the Internet. The access paradigm is identical to the UDP/Time client implementation. SNTP is also designed to operate on a dedicated server configuration, including an integrated radio clock. SNTP uses the standard NTP time stamp format described in RFC 1305 and previous versions of that document. NTP stamps are represented as a 64-bit unsigned, fixed-point number, in seconds relative to 0^h on January 1, 1900.

Network Time Protocol (RFC 1305)

The Network Time Protocol (NTP) is used to synchronize computer clocks in a TCP/IP computer network. It provides a comprehensive mechanism for accessing national time and frequency distribution services, for organizing the time-synchronization subnet, and for adjusting the local clocks. NTP provides accuracy of 1-10 milliseconds (ms), depending on the jitter characteristics of the synchronization source and network paths. NTP is a client of the User Datagram Protocol (UDP), which itself is a client of the Internet Protocol (IP).

Some definitions follow. For more, see Time Glossary.

NTP Data Format

The format of the NTP message data area, which immediately follows the UDP header, is shown in Figure 3-2. NTP time stamps are represented as a 64 bit unsigned fixed-point number, in seconds relative to 0^h on 1 January 1900. The integer portion is in the first 32 bits and the fractional portion is in the last 32 bits.

Table 4-1: NTP Message Data

0 8 16 24 31

LI	VN	MODE	Stratum	Poll	Precision
Synchronizing Distance (Root Distance) (32 bits)					
Synchronizing Dispersion (Root Dispersion) (32 bits)					
Reference Identifier (32 bits)					
Reference Time Stamp (64 bits)					
Originate Time Stamp (64 bits)					
Receive Time Stamp (64 bits)					
Transmit Time Stamp (64 bits)					
Authenticator (Optional) (96 bits)					
Autokey (Optional)(Variable)					

Leap Indicator (LI)

This is a two-bit code warning of an impending leap second that will be inserted or deleted in the last minute of the current day, with bit 0 and bit 1, respectively, coded as follows:

00:	No warning
01:	Last minute has 61 seconds
10:	Last minute has 59 seconds
11:	Alarm condition (clock not synchronized)

You are alerted to an alarm condition when the SyncServer is first powered on—in other words, before time is initially acquired from the timing signal. An alarm condition will also signal when the timing parameters are changed. This alarm condition will persist until the SyncServer acquires time. It should not signal again until the unit is powered off and on.

Version Number (VN)

This is a three-bit integer indicating the NTP version number. The SyncServer will return the version number from the incoming NTP message.

Mode

This is a three-bit integer indicating the mode. The SyncServer can be operated in any mode.

Stratum

This is an eight-bit integer indicating the stratum level of the local clock. For the SyncServer this field is set to **one** indicating a primary reference, if the SyncServer is relying on its GPS receiver or dial-up modem connection for timing information. Otherwise, it will accurately reflect its location in a timing hierarchy.

Poll Interval

This is an eight-bit signed integer indicating the maximum interval between successive messages, in seconds to the nearest power of two. The SyncServer will return the poll interval from the incoming NTP message.

Precision

This is an eight-bit signed integer indicating the precision of the local clock, in seconds to the nearest power of two. For the SyncServer this field is set to –19 (minus nineteen) which is the value closest to the 1u sec precision of the SyncServer when operating in GPS mode.

Synchronizing Distance (Root Distance Version 3)

This is a 32-bit fixed-point number indicating the estimated round-trip delay to the primary synchronizing source, in seconds with fraction point between bits 15 and 16. Set to zero in the SyncServer for GPS mode and a corresponding value when operating with another time source.

Synchronizing Dispersion (Root Dispersion Version 3)

Synchronizing Dispersion is a 32 bit fixed-point number indicating the estimated dispersion to the primary synchronizing source, in seconds. Root Dispersion indicates the maximum error relative to the primary reference source.

Reference Clock Identifier

This is a 32-bit code identifying the particular reference clock. In the case of Stratum 1 (primary reference), this is a four-octet, left justified, zero-padded ASCII string. For the SyncServer the four-octet string is dependent on the time source selected, ‘GPS’ for GPS and ‘FREE’ for Free Running Clock. If the unit is synchronizing to another SyncServer, the reference clock identifier will contain the four-byte address of the selected SyncServer.

Reference Timestamp
This is the local time at which the local clock was last set or corrected, in 64-bit timestamp format. With the SyncServer, the Reference Timestamp is the last time that a valid timing signal was detected. Therefore, the Reference Timestamp will indicate the time at which the timing signal was lost. When the timing signal returns, the Reference Timestamp will be updated.

Originate Timestamp
This is the local time at which the request departed the client host for the service host, in 64-bit time stamp format.

Receive Time stamp
This is the local time at which the request arrived at the service host, in 64-bit time stamp format.

Transmit Time stamp
This is the local time at which the reply departed the service host for the client host, in 64-bit time stamp format.

Authenticator
This field is used to hold a cryptochecksum if authentication has been enabled. Refer to the next section for more information about this mechanism.

Autokey
This field contains various autokey parameter requests and responses if autokey is enabled for the association. These parameters can include signatures, certificates, or other data.

NTP Authentication

NTP authentication enables an NTP client to ensure two things: that the time stamp received has come from a trusted source, and that it has not been modified in transit. Because Datum has extended the authentication method, you can use it to deny service to unauthorized clients who submit NTP time stamp requests.

The NTP protocol includes space for two variables related to authentication: an authentication key identifier field and a cryptochecksum field.

Authentication: NTP v3

The NTP client can operate with both non-authenticated and authenticated servers. This approach uses symmetric-key cryptography. Thus, keys and key identifiers are determined in advance and distributed in traditional ways.

The message digest is computed using preferred Message Digest 5 (MD5). An alternative is the Digital Encryption Standard, Cipher Block Chaining (DES-CBC).

The Message Authentication Code (MAC) is made up of a key identifier, then the message digest. Keys are held in a key cache; the cache is initialized from a private file.

Authentication: NTP v4 Autokey

NTPv4 uses public-key cryptography, meaning all keys are random, and private keys are never revealed. A certificate scheme binds the public key to the server identification. Symmetric-key cryptography uses fixed private keys which must be distributed in advance. The Diffie-Hellman model defines the key agreement, and is required for private random keys.

Public Domain xNTP Package

For clients not using the public domain xNTP package, the NTP packet is enlarged by 8 bytes to handle the entire cryptochecksum, which is 16 bytes (128 bits) in size as generated by the MD5. Since this field is the last in the packet, it should not present any difficulty.

How NTP Defines the Authentication Process

If authentication is enabled, and a valid authentication key identifier and cryptochecksum is received, then the NTP packet is filled in and a new cryptochecksum is computed and added to the packet. The packet is then sent back to the client.

More information

For more about NTP authentication, see `http://www.eecis.udel.edu/~ntp/ntp_spool/html/authopt.htm`.

ACTS Interface: Dial-up

The Automated Computer Time Service (ACTS) is maintained by the U. S. National Institute of Standards and Technology (NIST). More information is in the next section. In most of this guide, the term *dial-up* is used instead.

ACTS Operation

Use the SyncServer's web-based interface to configure this method of access to time (for info, see Timing Engine, Main Settings). ACTS provides a backup time service through an ASCII time broadcast, and supports a measured delay mode for enhanced accuracy. This service is based on the use of asynchronous modems attached to the SyncServer S100 at the serial port. It also supports Digital ISDN terminal adapters. And it is designed to coexist with a standard IRIG B time code input.

ACTS is designed to operate in either manual or automatic mode. It operates with analog modems running over POTS, and digital terminal adapters running over ISDN. A nonvolatile initialization string is available to configure almost any type of asynchronous communications device for use with ACTS. Also, ACTS uses software flow control (Xon/Xoff) instead of RTS/CTS hardware flow control.

The SyncServer's ACTS operation includes simultaneous support of both client and server modes. This means the SyncServer can obtain time information from a remote site through an ACTS client connection while providing server capabilities such as distributing time information to local clients or other SyncServer units.

When services are available, an ACTS client call will not modify the SyncServer clock if the unit is currently decoding a valid time code signal.

The SyncServer will periodically call a remote server to check its time base. Two servers may be specified, in which case the SyncServer will switch to the alternate service in the event the primary service is unavailable. The period for calling is programmable in one-hour intervals with values from 1–99 supported.

More Information

For more about NIST and ACTS:

`http://www.boulder.nist.gov/timefreq/service/acts.htm`

Chapter 5

FAQ and Solutions

Overview

This section gives information in response to the most-asked user questions about SyncServer, answers common “how to...?” questions, and provides solutions.

Frequently Asked Questions

How can we obtain NTP client software to use with SyncServer?
NTP client software information and configuration details are available from:

- `http://www.datum.com/tt/downloads/datum_time.html`
- `http://www.ntp.org`

- `http://cs3.ecok.edu:457/NetAdminG/netadminN.about.html`

Client software and configuration information for Unix, Windows, and Novell platforms can be downloaded from these sites.

SNTP client software is included with the SyncServer hardware.

What are the main differences between SNTP and NTP clients?

SNTP is a Simple Network Time Protocol. It is based on RFC 1361/2030: it gets its time from the specified time servers of the machine on which it is installed. This protocol cannot be configured to obtain time from an alternate time server if the primary server is down. This could be called as a short version of NTP client software.

NTP, Network Time Protocol, is based on RFCs 1305 and 1119 which can be configured to obtain and distribute the time on the network. It has a built-in algorithm that calculates the time accurately up to 1-10 milliseconds. The algorithm can be configured to obtain time from an alternate source in case the original time server fails or gets out of synchronization.

Is there a way to get GPS time instead of UTC time from the SyncServer?

The SyncServer normally provides UTC time. However, it can be configured to output GPS time—currently UTC + 13 seconds—by making several hardware changes to the unit. Contact your Datum representative about this.

What outputs are available on the SyncServer S100?

These are:

- Dual Ethernet 10/100BaseT (RJ 45)
- RS-232 Serial Console (DCE)

How does the SyncServer handle Leap Second?

Today’s clocks keep pace with one another to within two or three millionths of a second over a year’s time. However, the earth on its rotation might randomly accumulate almost a full second in a year. This time is deleted (or added, if needed) as a *leap second* from (or to) the UTC time on the last day of June or December in the affected year. This way, the clocks stay in step with the earth’s rotation.

The GPS satellites send notice of an upcoming leap second about two months in advance. The SyncServer receives this notice and, following NTP specifications, starts advising clients 24 hours in advance. At the leap second event, the SyncServer will add or delete the leap second from the transmitted time.

NOTE: The SyncServer will do the same to an IEEE 1344 IRIG B signal. However, in the event of a leap second, if the time source is regular IRIG B, dial-up, 1PPS, or Freerun (including ACTS), you must pre-program the leap second event with the command `leap` so that SyncServer can be notified and maintain time correctly.

What signal strengths are required by the SyncServer receiver to start tracking?

SyncServer requires four satellite signals with strengths greater than 6 dB to turn the tracking LED on. After the tracking LED is on, SyncServer requires only one satellite signal to maintain its time. If it loses the fourth signal, the SyncServer will automatically transfer to Freerun mode and will keep on providing time.

How do I check versions of the software in SyncServer?

To check for the version of SyncServer software, use the web-based administrative interface main admin menu, **Versions** option.

What is the maximum number of computers that can be networked to the SyncServer?

SyncServer acts as a standalone time server. Average time to process the NTP request is less than 1 millisecond. Testing has shown SyncServer can handle approximately 10,000 requests per second. However, clients running as Stratum 2 computers access SyncServer in an interval of 64 to 65,536 seconds as the time progresses. The optimum number of computers is based on the capability of the network and on the acceptable level on load on the network.

How many satellites are necessary for me to operate SyncServer?

Four. The unit will usually track six to eight satellites.

How do I know if the satellite signal strength is good?

Any signal over 6 is good and usable by SyncServer. The unit will continue to track a satellite down to 3 once it has acquired it at a level 6 or over.

What is the maximum antenna cable length for use with SyncServer?

A maximum length of 300 feet can be used with the standard (Bullet II) antenna. From 300–500 feet, the High Gain Antenna option is required. If you need longer lengths, please contact Datum Technical Support.

What are the available antenna cable lengths and antenna requirements?

These are:

Cable length/cable type	Antenna
50’’–100’ Belden RG58	Standard bullet-type
100’–300’ Belden 9913	Standard bullet-type
300’–500’ Belden 9913	High Gain
Over 500’	Contact Datum

What are some guidelines for correctly cutting the cable, using splitters, and using cable connectors?

Some critical “do’s and don’ts” are:

- *Do* use pre-made kits from Datum.
- *Do* install the antenna where there are no obstructions—either on the roof, or with a view of the horizon that is at least 30 degrees.
- *Do not* split the antenna cable signal to try to use the signal to drive other GPS devices.
- *Do not* cut the cable to a shorter length. Instead, bundle any excess cable. Correct antenna cable length—even if you do not “use it all”—is critical to proper SyncServer operation, which should have a gain within the range of 15dB–25dB.

How-tos and Tips

Here are some guideposts to often-asked “how to” questions. The answer will direct you to another part of this material, in Chapter 3, where there is more detail.

How to install your SyncServer

All information about this is covered in Installing Your SyncServer, on page 20.

How to get time via dial-up

See Dialup on page 34 for details about this.

How to get time via GPS

See GPS, on page 29.

How to install your GPS antenna

See Installing the GPS Antenna, on page 21.

How to acquire and install DatumTime™

To acquire DatumTime, download this free software from `http://www.datum.com/tt/downloads/datum_time.html`.

Directions on its installation are found in Installing the DatumTime™ Client Software, on page 48.

How to get info about NTP
To learn more about NTP, use these links:

- `http://www.ntp.org`
- `http://www.ietf.org/rfc/rfc1305.txt`

Solutions

This section offers solutions to some situations you may run into as you use your SyncServer.

If you still cannot solve the problem, please contact SyncServer technical support at `ttsupport@datum.com`, or (781) 372-3600.

SyncServer does not respond to ping command
Use the SyncServer web interface to ping your client (see Networking: Ping, on page 74). If your client cannot be reached with the ping command, the SyncServer provides a traceroute utility to show the path data is taking.

Also check the Ethernet 10/100baseT cable connections between the RJ45 connector and the hub or network.

SyncServer does not respond to NTP queries
If SyncServer can be pinged, but it doesn't respond to NTP queries, then verify that the NTP software on your computers is set up properly, and also verify that the client has the correct IP address of the SyncServer.

I cannot establish a serial connection with the SyncServer
Make sure that the connection is made with the front panel serial console in the SyncServer.

Make sure you are using the correct com port on your management PC (com1).

Also check that the configuration settings are set to a VT100 ASCII terminal using 38.4kbps, 8, N, 1.

Try pinging the SyncServer from your management PC, and the PC from the SyncServer. Then use Networking: Traceroute to check the path between the two; this should give you some useful data that will solve the problem.

My SyncServer won’t track satellites

Check the following:

Possible cause of tracking problems:	How to fix:
Antenna not positioned correctly	Be sure antenna is on the roof or location with at least a 30-degree view of the horizon, and at least two meters from other active receiving antennas and shielded from transmitting antennas
Cable is cut to the wrong length, causing dB gain problems	Replace with cable of correct length
Incorrect connector(s) at the end(s) of the cable(s) or along the cable run, causing dB gain problems	Replace with correct connector
Incorrect use of splitters, including signal splitting to another GPS device or cable cut to wrong length	Replace with splitter that does not “share” signal, on a cable of correct length

Appendix A
SyncServer Specifications

SyncServer Product Specifications

Table A-1: SyncServer S100 Data Sheet Specifications

Component	Specifics	Description
Network Interface	Ethernet over 10/100Base-T	IEEE 802.3 specifications
	Connection	10/100BaseT, Twisted Pair RJ45
	Time Protocols	NTPv2 (RFC 1119), NTPv3 (RFC 1305), NTPv4 (IETF Draft Standard), SNTP (RFC 2030), Time Protocol (RFC 868), Daytime Protocol (RFC 867)
	Supported Protocols	TCP/IP, MD5 Authentication (NTP), SNMP v1 (RFC 1157), DHCP (RFC 2131), SSH (Secure Shell), HTTP/ HTML/HTTPS (RFC 2616)
Serial Connection	Serial Port	RS-232/DB9 DTE
Software	NTP Client	www.ntp.org, or www.datum.com/tt
	Time Utility (MS Windows)	DatumTime™ (www.datum.com/tt)
Timing Accuracy	Network	1–10 milliseconds, typical
	GPS	<1 microsecond (relative to UTC, GPS tracking)
	Dial-up service	<1-10 milliseconds, on sync
	Oscillator	Rate stability: 5 x 10^{-7}
GPS Input	Channels and Frequency	Eight, C/A code
	Cable Type	50 feet (15.25m) /RG58
	Antenna	Size: 3.04"d x 2.94"h (7.72cm x 7.47cm) Operating temperature: -40°C to +85°C Acquisition <5 minutes
Chassis	A/C Power In	100–240VAC, Auto-switching 50-60 Hz
	Size and Weight	1.75"H x 17.0"W x 18"D (4.45cm x 43.2cm x 45.7cm) 1U Height Rack Mount, 18 lbs. (8.2Kg)
Operating and Storage Environments	Temperature and Humidity	0°C to +45°C/5-95% @ 40°C
Options	Long Antenna Cable (Belden 9913), Lightning Arrester, High-Gain GPS Antenna, GPS In-Line Amplifier, Rack Mount Slides	

Pin Descriptions

P1: Ethernet RJ45

***Description:* 8-pin Phone Jack, Mfr: AMP, Part # 555153-1**

Pin Number	Description
1	TX (+)
2	TX (-)
3	RX (+)
4	N/C
5	N/C
6	RX (-)
7	N/C
8	N/C

P3: Serial A (Data Terminal Port/DTE)

***Description:* 9-pin "D" Plug, Mfr: AMP, Part # 869436**

Pin Number	Description
1	RS-232 Data Carrier Detect (in)
2	RS-232 Receive Data (in)
3	RS-232 Transmit Data (out)
4	RS-232 Data Terminal Ready (out)
5	Ground
6	RS-232 Data Set Ready (in)
7	RS-232 Request to Send (out)
8	RS-232 Clear to Send (in)
9	RS-232 Ring Indicator (in)

Appendix B
Time Glossary

Overview

There are many time-related terms that have been defined and re-defined just in the last few years. This glossary is provided so that you have the latest information on developments in secure time distribution.

Glossary Terms

Access Control
Network managers define access control by requiring authentication of the user's identity before permitting or limiting entry to a network or server resource/printer.

ACTS
Automated Computer Time System, a NIST service that provides announced time via telephone.

Advanced Encryption Standard (AES)
Developed by NIST and private companies, this standard is 256-bit based and is a stronger defense for sensitive material when compared to 40-bit or 128-bit.

Algorithm
Any mechanical of recursive computational procedure.

ANSI
American National Standards Institute. The agency that sets US standards in such areas as computer communications.

Antiwarrant
Attribute certificate that has the same expire date as its valid date; in other words, it was never valid. This is still sent, at times, because it contains other information that the system needs. See also *Warrant*

API
Application Program Interface. This interface allows software developers to write their software so that it can communicate with the computer's operating system or other programs.

ASCII
American Standards Code Information Interchange, a code in which each alphanumeric character is represented as a number from 0 to 127, in binary code so the computer can understand it. Its simplicity allows diverse computers to understand one another.

ATM
Asynchronous Transfer Mode, or ATM switching. This is a type of packet switching that makes it possible to transmit data at high speeds over a network. It also allows dynamic allocation of bandwidth, meaning users get only the bandwidth they need and are charged accordingly.

Audit Trail
A series of events, usually kept in and managed by a computer-based log, that give proof of a defined activity.

Authentication
Method by which a person is verified to be who they say they are, by password or other means.

Authorization
Method by which an authenticated person is allowed certain access to the system, via password or other means.

BCD
Binary Coded Decimal. Also called packed decimal, this is the representation of a number by using 0s and 1s, or four-bit binary numbers. So the number 29 would be encoded as 0010 1001.

CA
Certificate Authority

Calibration
To fix the graduations of time measurement against the established national standard, including any periodic corrections that should be made.

CDMA
Code Division Multiple Access. A technique of multiplexing, also called spread spectrum, in which analog signals are converted into digital form for transmission.

CDSA
Common Data Security Architecture. This describes the security structure for the entire network. It is unique to each network because security is managed differently for each.

Certificate
Often called “digital certificates”, this is a credential that includes security information and keys.

Certificate Authority (CA)
Independent organization or vendor that acts as a notary, verifying the identification of involved parties, and issues certificates that contain authenticating and identifying data. The certificate also contains keys and other security information.

Certificate Extension
An extension of the X.509 standard that lets the certificate hold additional identifying information.

Certification Path
A specified sequence of issued certificates necessary for the user to get their key.

Certificate Request Message
A certificate request message is composed of the certificate request along with other identifying data.

Certification Revocation List
A CA maintains a list of certificates that have been cancelled but remain unused; revocation lists are vital when certificates have been stolen, for example.

Confidentiality
Keeping secret data from unauthorized eyes.

Coordinated Universal Time (UTC)
The international time standard is called Universal Coordinated Time or, more commonly, UTC, for “Universal Time, Coordinated”. This standard has been in effect since 1972 by worldwide representatives within the International Telecommunication Union. The UTC designation was chosen as a compromise among all the countries’ abbreviations for Universal Coordinated Time. UTC is maintained by the Bureau International de l’Heure (BIPM) which forms the basis of a coordinated dissemination of standard frequencies and time signals. The acronyms UTC and BIPM are each a compromise among all the participating nations.

Content Filtering
A filter that screens out data by checking, for example, URLs or key words.

Credential(s)
Much like a photo ID or birth certificate, electronic credentials are recognized as proof of a party's identity and security level. Examples: certificate, logon ID, secure ID, and so forth.

CRM
See *Certificate Request Message*

Cross-Certificate
Two or more CAs which issue certificates (cross-certificates) recognized in each others’ domains.

Cryptography
See *Encryption*

Data Encryption Standard (DES)
Encryption method in which both the sender and receiver of a message share a single key that decrypts the message.

Datum Secure Network Time Protocol (DS/NTP)
The protocol created by Datum, based on NTP, that includes additional security features.

DCLS
Direct Current Level Shift, or digital IRIG.

See also: *IRIG*

Decryption
The transformation of unintelligible data (“ciphertext”) into original data (“clear text”).

Denial of Service
When a network is flooded with traffic, the systems cannot respond normally, so service is curtailed or denied. This is a favorite technique of network saboteurs, along with Distributed DOS.

DES
See *Data Encryption Standard*

DHCP
Dynamic Host Configuration Protocol, or Windows server software that assigns an IP address to each node in a network.

Diffie-Hellman
A key-agreement algorithm used to create a random number that can be used as a key over an insecure channel.

Digital Certificate
Digital Certificates are issued by a Certificate Authority, which verifies the identification of the sender. The certificate is attached to an electronic message, so the recipient knows the sender is really who they claim to be.

Digital Fingerprint
Similar to digital signature, a digital fingerprint is the encryption of a message digest with a private key.

Digital Signature
Like a digital certificate, a digital signature is a data string that is verified by a Certificate Authority, and is attached to an electronic message so that it can verify that the sender is really who they claim to be. The difference between a digital certificate and a digital signature is found in how the message is encrypted and decrypted.

Digital Signature Algorithm (DSA)
The asymmetric algorithm that is at the core of the digital signature standard.

Digital Signature Standard (DSS)
A National Institute of Standards and Technology (NIST) standard for digital signatures, used to authenticate both a message and the signer. DSS has a security level comparable to RSA (Rivest-Shamir-Adleman) cryptography, having 1,024-bit keys.

Digital time-stamp
See *time-stamp*

Directory
The directory is the storage area for network security information such as keys or server names.

DSA
Digital Signature Algorithm. DSA is a public-key method based on the discrete logarithm problem.

DS/NTP
Datum Secure Network Time Protocol

DSS
See *Digital Signature Standard*

DTT
Datum Temporal Token

Element Manager (ENMTMS)
Software that manages the components of an application.

Encryption
The transformation of clear data (clear text) into unintelligible data (ciphertext). Asymmetric encryption, also known as public key encryption, allows for the trading of information without having to share the key used to encrypt the information. Information is encrypted using the recipient's public key and then the recipient decrypts the information with their private key. Symmetric encryption, also known as private key encryption, allows information to be encrypted and decrypted with the same key. Thus the key must be shared with the decrypting party--but anyone who intercepts the key can also use it.

ENMTMS
See *Element Manager*

Ephemeris Time
Time obtained from observing the motion of the moon around the earth.

FIPS
Federal Information Processing Standards. These are a set of standards for document processing and for working within documents. Some commonly-used FIPS standards are 140-1, 140-2, and 180.

Firewall

Firewalls are software and hardware systems that define access between two networks, offering protection from outside data that could be harmful, such as a virus sent via the Internet.

GMT

Greenwich Mean Time, the mean solar time of the meridian of Greenwich, England, used until 1972 as a basis for calculating standard time throughout the world.

GPS

Global Positioning System. The GPS is a constellation of 24 US Department of Defense satellites orbiting the earth twice a day.

Hack/crack

“Hackers” are unauthorized programmers who write code that enables them to break into a computer network or program. “Crackers” are unauthorized programmers whose goal it is to break into computer networks or programs protected by security software or hardware.

Hash

Also called “hash function” or hashing, used extensively in many encryption algorithms. Hashing transforms a string of characters usually into a shorter, fixed-length value or key. Information in a database is faster to search when you use a hashed key, than if you were to try to match the original data.

HTML

HyperText Markup Language, the computer language used to create pages for the World Wide Web.

HTTP

HyperText Transfer (or Transport) Protocol, the protocol most often used to transfer information from World Wide Web servers to users of the Web.

Identity Certificate

The hash creates a message digest based on the contents of the message. The message is then encrypted using the publisher's private key, then it is appended to the original message.

IEEE

Institute of Electrical and Electronic Engineers, an international organization that sets standards for electrical and computer engineering.

IETF

Internet Engineering Task Force, an international organization which sets standards for Internet protocols in their Request for Comment (RFC) papers.

These papers are numbered (RFC 1305, RFC 868, and so on) and are referred to by engineers worldwide as they work on technologies that support IETF standards.

IKE

Internet Key Exchange, a security system that uses a private key and an exchange key that encrypts private keys. Passwords are delivered via the Internet.

In-band Authentication

When you use PKI for authentication, it is called in-band authentication.

See also: *out-of-band authentication*

Integrity

Data that has retained its integrity has not been modified or tampered with.

IPSec

Internet Protocol Security describes the IETF protocols that protect the secure exchange of packets on the IP layer.

IRIG

InteRange Instrumentation Group is an analog standard for serial time formats.

Irrefutability

In the time security world, irrefutability means the source of the message cannot be disproved.

ITU

International Telecommunications Union, the international organization that sets standards for data communication.

Key

An alphanumeric string that encrypts and decrypts data.

Key Escrow

A secure storage maintained by a trusted third party, which holds keys.

Key Generation

Creation of a key.

Key Management

The process by which keys are created, authenticated, issued, distributed, stored, recovered, and revoked.

Key Pair

An integrated pair of keys, one public, one private.

Key Recovery

A method that allows messages to be decrypted even if the original key is lost.

L1 Band, L2 Band

Each Navstar GPS satellite currently transmits in two dedicated frequency bands: L1 and L2, which is centered on 1227.6 MHz. L1 carries one encrypted signal, as does L2, both being reserved for the military. L1 also carries one unencrypted signal, for civilian use.

LDAP

The Lightweight Directory Access Protocol allows access to a directory service.

Leap Second

Today’s scientists and engineers have perfected clocks based on a resonance in cesium atoms to an accuracy of better than one part in 10 trillion. These clocks keep pace with each other to within one two- or three-millionth of a second over a year’s time. The earth, on the other hand, might randomly accumulate nearly a full second’s error during a given year. To keep coordinated with the rotation of the earth, this error is added to (or deleted from) UTC time as a leap second, on the last day of the June or December in that year.

Message Authentication Code(MAC)

A MAC is a function that takes a variable length input and a key to produce a fixed-length output.

Message Digest

The hash of a message.

See also: *Hash*

MIB

Management Information Base, a database on the network that tracks, records, and corrects performance for each device on the network.

MTBF

Mean Time Between Failure, a measure of reliability. The longer the time span between failures, the more reliable the device.

Multiplexing

Process during which two or more signals are combined into one; at the other end, signals are “unbundled” by a demultiplexer. *TDM* is Time Division Multiplexing, *FDM* is Frequency Division Multiplexing, and *CDMA* is Code Division Multiple Access.

National Measurement Institute

The national authority in each country that is recognized as the source of official time.

Network Time Management System (NTMS)

Datum's architecture for the use of its Trusted Time product.

NIST

National Institute of Standards and Technology, the National Measurement Institute in the United States. In the form of FIPS documents, NIST produces standards for security and cryptography.

NMI
National Measurement Institute(s) or National Metrology Institute(s), the national authority in each country that is usually recognized as the source of official time.

NMIServer
National Measurement Institute Server

NOC
A Network Operations Center monitors and manages networking.

Non-repudiatable
The Trusted Time time-stamp has an audit trail back to its time source, during which the sender of the transaction is authenticated. Therefore, the sender cannot deny the time of the transaction.

Notarization
Certification of the identity of the party in a transaction based on identifying credentials.

NTMS
Network Time Management System, the architecture for Datum's Trusted Time product.

NTP
Network Time Protocol is a protocol that provides a reliable way of transmitting and receiving the time over the TCP/IP networks. The NTP, defined in IETF RFC 1305, is useful for synchronizing the internal clock of the computers to a common time source.

Online validation
A way of validating a key each time before it is used to verify that it has not expired o revoked.

OCSP
Online Certificate Status Protocol, a method for validating digital certificates and signatures.

OID
Object Identifier.

OSI
Operations System Interface,

Out-of-band Authentication
When authentication is performed using relatively insecure methods, such as over the telephone, it is called out-of-band authentication. In-band authentication, which uses PKI, is preferred.

See also: *In-band Authentication*

PCI
Peripheral Component Interconnect, a local bus that supports high-speed connection with peripherals. It plugs into a PCI slot on the motherboard.

PKCS
Public Key Cryptography Standards. These standards allow compatibility among different cryptographic products.

PKI
Public Key Infrastructure. The PKI includes the Certificate Authority (CA), key directory, and management. Other components such as key recovery, and registration, may be included. The result is a form of cryptography in which each user has a public key and a private key. Messages are sent encrypted with the receiver's public key; the receiver decrypts them using the private key.

PKI Certificate
Verifies a person’s identification.

PKIX
Extended Public Key Infrastructure, of PKI with additional features approved by the IETF.

PLB
Private Label Branch

Policy
A company's security policy.

PSTN
Public Switched Telephone Network, a voice and data communications service for the general public which uses switched lines.

Private Key
This is a secret key, known to only of the parties involved in a transaction.

Public Key
Messages are sent encrypted with the recipient's public key, which is known to others; the recipient decrypts them using their private key.

Public Key Certificate
Certificate in the form of data that holds a public key, authentication information, and private key information.

RA
A Registration Authority does not issue certificates, but does the required identification for certain certificate data.

Resolution
Resolution of a time code refers to the smallest increment of time, whether it is days, hours, seconds, or other.

Revocation
The withdrawing of a certificate by a Certificate Authority before its expiration date or time.

Also see *Certificate Revocation List (CRL)*

Risk Management
The tasks and plans that help avoid security risk, and if security is breached, helps minimize damage.

RSA
The RSA (Rivest-Shamir-Andleman) algorithm is used to create digital signatures.

SHA-1
Secure Hash Algorithm, which has a larger message digest, making it more secure against certain hacker attacks.

Smart card
A card the size of a credit card, which holds a microprocessor that stores information.

S/MIME
Secure Multipurpose Internet Mail Extensions. The standard for secure messaging.

SNMP
Simple Network Management Protocol is the Internet standard protocol for network management software. It monitors devices on the network, and gathers device performance data for management information (data)bases ("MIB").

Solar Time
Time based on the revolution of the earth around the sun.

SSL
Secure Sockets Layer, a protocol that allows secure communications on the World Wide Web/Internet.

SSL Client Authentication
Part of the SSL "handshake" process, when the client responds to server requests for a key.

SSL Server Authentication
Part of the SSL "handshake" process, when the server informs the client of its certificate (and other) preferences.

SSL-LDAP
Secure Sockets Layer-Lightweight Directory Access Protocol.

Stratum Level
These are standards set by Network Time Protocol RFC 1305. The highest level are Stratum 0 devices such as GPS, which get their time from a primary time source such as a national atomic clock. Stratum 1 servers, such as TymServe, source their time from a Stratum 0 device. Stratum 2 and beyond obtain their time from Stratum 1 servers. The further away a

network is from a primary source, the greater the chance of signal degradations due to variations in communications lines, and so forth.

Sysplex Timer

The Sysplex Timer provides a synchronized Time-of-Day clock for multiple attached computers.

TCCert

Time Calibration Certificate

TCP/IP

A mainstay of the Internet, the Transmission Control Protocol (TCP) provides dependable communication and multiplexing It is connection-oriented, meaning it requires a connection be established data transfer. It sits on top of the Internet Protocol (IP), which provides packet routing. This is connectionless, meaning each data packet has its source and destination data embedded, so it can bounce around a network and still get to its destination.

Telnet

Telnet is a terminal emulation application protocol that enables a user to log in remotely across a TCP/IP network to any host supporting this protocol. The keystrokes that the user enters at the computer or terminal are delivered to the remote machine, and the remote computer response is delivered back to the user’s computer or terminal.

Time-stamp

A record mathematically linking a piece of data to a time and date.

Time-stamp Request

The client computer or application sends a time-stamp request to a stamp server.

Time-stamp Token

The essential part of the time-stamp. It contains the time, the message digest/the message imprint (hash), and it is signed to verify the accuracy of that time. In detail, it is a signed data object where the encapsulated content is a TSTInfoObject, thus it verifies the stamp as coming from the device you submitted it to, and it is bound to the file you are working with.

Time-stamping Authority

An authorized device that issues time-stamps, and its owner.

TLS

Transport Layer Security, security that protects the OSI layer that is responsible for reliable end-to-end data transfer between end systems.

Tool box

A group of software applications that have similar functions.

Token

See *time-stamp token*

TMC
See *Trusted Time Master Clock*

TPC
Third Party Certificate.

See also: *Certificate*

TPCA
Third Party Certification/Certificate Authority.

See also: *Certificate Authority*

Traceability
Traceability infers that the time standard used on the time-stamp server was set using time directly or indirectly from a National Measurement Institute.

Transaction
An activity, such as a request or an exchange.

Triple-DES
Also called Triple Data Encryption Algorithm (TDEA) Data Encryption Standard is an algorithm that encrypts blocks of data.

Trust
In the network security context, trust refers to privacy (the data is not viewable by unauthorized people), integrity (the data stays in its true form), non-repudiation (the publisher cannot say they did not send it), and authentication (the publisher--and recipient--are who they say they are).

Trusted Time
Datum’s family of products that produce extremely accurate and auditable time-stamps.

Trusted Time Infrastructure
The internal architecture of Datum's Trusted Time products.

Trusted Time MasterClock (TMC)
Datum’s Trusted MasterClock is a rubidium-based master clock synchronized to UTC time and certified by a National Measurement Institute.

Trusted Time NMIServer
Datum’s NMI Trusted Time Server, or NMIServer, is a standalone secure server based on the Trusted MasterClock, which is dedicated to the creation of trusted UTC time at the NMI.

Trusted Time Products (TTP)
The family of Datum’s Trusted Time products, including the Network Time Management System, Trusted MasterClock, Trusted time-stampServer, and Trusted Time application software.

Trusted Time-StampServer (TSS)
Datum’s Trusted time-stampServer (TSS) services time-stamp requests from applications, transactions, or computer logs.

TSA
See *Time-Stamp Authority*

TSP
time-stamp Protocol

TSR
See *time-stamp Request*

TSS
See *Time-StampServer*

TT
See *Trusted Time*

TTI
See *Trusted Time Infrastructure*

TTDS
See *Trusted Time Distribution Service*

TTP
See *Trusted Time Product*

UDP/IP
User Datagram Protocol/Internet Protocol is a communications protocol that provides service when messages are exchanged between computers in a network that uses the Internet Protocol. It is an alternative to the Transmission Control Protocol.

USNO
U.S. Naval Observatory, in Washington, D.C., where the atomic clock that serves as the official source of time for the United States is maintained.

UTC
See *Coordinated Universal Time*

Vault
Secure data storage facility.

Verification
The process of making sure the identity of the parties involved in a transaction is what they claim it to be.

Virus
An unwanted program that hides “behind” legitimate code, and which is activated when the legitimate program is activated.

VPN
Virtual Private Network, a way that authorized individuals can gain secure access to an organization's intranet, usually via the Internet.

W3C
The World Wide Web Consortium, based at the Massachusetts Institute of Technology(MIT), is an international organization which creates standards for the World Wide Web.

Warrant
An attribute certificate that attests to the time of the device. It is used to adjust the clock. See also: *PKI certificate*

Wireless Application Protocol (WAP)
Wireless Application Protocol, a worldwide standard for applications used on wireless communication networks.

WPKI
Wireless Public Key Infrastructure.

WTLS
Wireless Transport Layer Security

X.509
The ITU's X.509 standard defines a standard format for digital certificates, the most-widely used PKI standard.

X.509 v3 Certificate Extension
The X.509 standard with extended features approved by the IETF.

Index

Datum - Trusted Time Division
10 Maguire Road, Suite 120
Lexington, MA 02421-3110 USA
(1)(781) 372-3600   Toll-free (U.S.): (888) 551-4022
www.datum.com   e-mail: trustedtime@datum.com
SS v1.2, Doc v1.2