Domain Time II

Audit Server

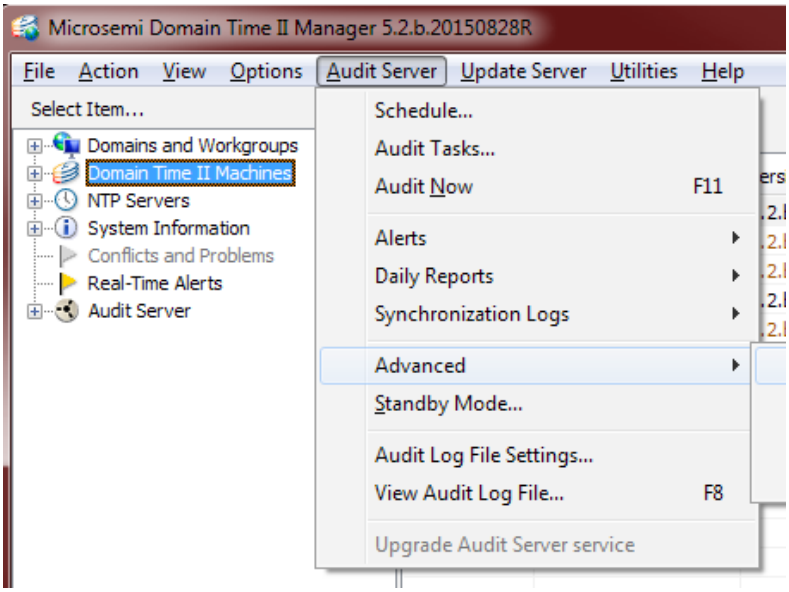
(Optional Domain Time II Add-In)

Key Features

- Automatically audit the time on your network
- Clear, indisputable records
- Generate alerts if time or audit period exceeds specified tolerances
- Integrates perfectly with Domain Time II time synchronization software suite
- Integrates with existing network Management programs

Key Benefits

- Complete records of time synchronization accuracy of the computers on your network
- Know when a machine was last synchronized, with what time source, as well as its variance from the reference time source
- Peace of mind from an automatic software system routinely auditing time on your network
- Know that you will be notified if time or audit period is out of tolerance
- Cross check network time with independent time sources for historical validation



Audit Server is a Domain Time II add-in designed to provide a secure, verifiable audit trail of the time synchronization of your network. It automatically provides the clear, indisputable records you need to easily resolve any contested timestamp or synchronization issue that may arise.

Federal regulatory agencies as well as major securities organizations already require this type of audit collection to prevent fraud and to establish the validity of transactions. Audit Server meets or exceeds such requirements and makes it painless to comply with the regulations.

The records collected by Audit Server include complete information to allow auditors to determine precisely when a machine was last synchronized, with what time source, as well as its variance from the reference time source. Audited Time is being able to prove conclusively (on demand) whether the time on any monitored system was correctly synchronized at a particular time and date with a specified time source.

Audit Server uses the built-in time synchronization and data collection capabilities of the Domain Time II time synchronization components (Domain Time II Server and Clients) to construct and maintain a verifiable and secure audit trail indicating when the clock on a machine was last synchronized. Domain Time II components all work together to easily and automatically provide Audited Time on your network with minimal intervention on your part.

Auditing Best Practice #1
Identifying Monitored Machines

All Domain Time II Server and Client services are individually identified using a unique serial number that is assigned when the Domain Time software is installed. Even if the IP address or name of the machine changes, the audit records will clearly identify the machine running that particular instance of Domain Time II.

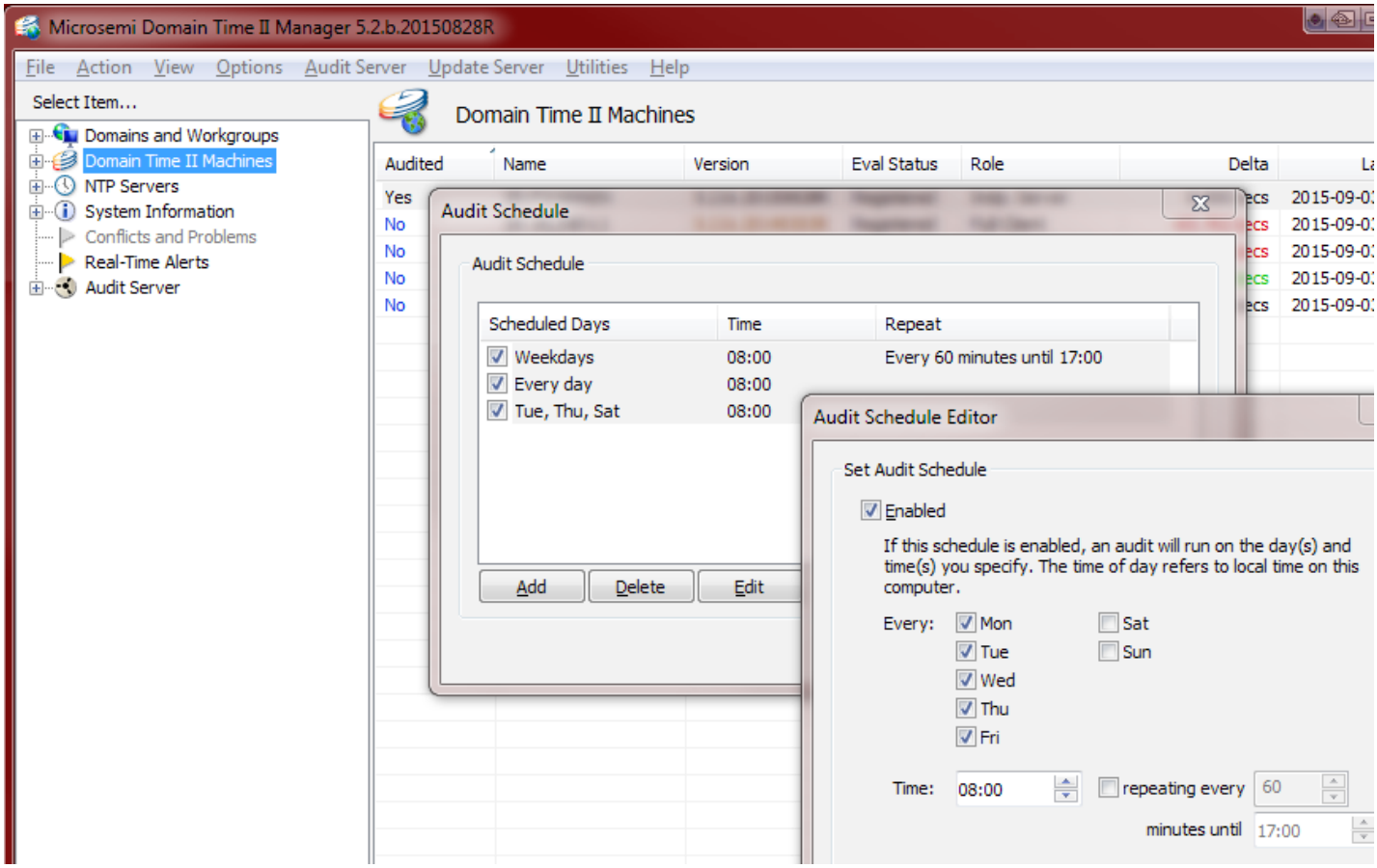
Auditing Best Practice #2
Accurate and Reliable Network Synchronization

A Domain Time II Server connects securely to a trusted network time source such as a Microsemi dedicated GPS referenced network time server, and then distributes that time accurately and verifiably to every time-aware machine on the network using the Domain Time II time distribution system.

In addition, Domain Time II components have a function called Clock Change Monitor that prevents users from manually changing the time on machines to falsify records. Domain Time II also has sophisticated security features to ensure that the entire system time is correct, including protection from rogue time servers, Denial-of-Service attacks, and more.

Domain Time II

Audit Server



Auditing Best Practice #3
Retrieval of Vital Time Sync Information

Domain Time Servers and Client services keep detailed internal statistics on their operation, which is regularly queried by Audit Server. The statistics include such information as the name/IP address and time of the last time source used for synchronization, the amount of correction to the local clock that was made, the protocol used to set the time, and so on. Statistics are regularly retrieved from clients and servers using the Domain Time II protocol, which allows for efficient transfer of the information to the Audit Server, with a very small amount of traffic. This means that the audit process is very low-overhead and has a minimal impact on the network.

Audit Server can also obtain the current time from an NTP time source at the time an audit occurs. This allows the audit record to include at least basic information from any NTP machines (such as a GPS based network time server or router) that may also be involved in providing time to the network. This also can serve as a time cross check and historical validation if you also monitor an official public time source.

Auditing Best Practice #4
Regular Collection of Audit Records

The Audit Server automatically contacts Domain Time II Servers and Clients (and any specified NTP servers) to collect their audit data on a schedule you specify. This information is compiled into compact record files that include all relevant information about each monitored system. Each record is optimized to minimize the amount of disk space used to retain the records. The Audit Record Viewer allows to view the data in an easy-to read format, and to extract the data to text files in a summary or full-detail form.

Auditing Best Practice #5
Automatic Error Notification

Audit Server verifies that machines selected to be audited are actually having their time set and that they are responding to the audits. If any machine fails to be synchronized within your desired tolerance, or if a machine misses more audits than your specified maximum error limit, an email alert is automatically generated so that the problem can be addressed immediately.

Domain Time II

Domain Time II Specifications

System Requirements						
Operating System	32-bit	64-bit	Client	Server	Manager	Audit Server
Windows XP, 2003 (and R2), Vista, 2008 (and R2), Win7, Win8.x, 2012 (&Rw), Win10.	√	√	√	√	√	√
Warranty One year of updates/downloads included in price.						
Documentation All documentation is online at http://dtdocs.ntp-systems.com/						

Microsemi Corporate Headquarters
One Enterprise, Aliso Viejo, CA 92656 USA
Within the USA: +1 (800) 713-4113
Outside the USA: +1 (949) 380-6100
Sales: +1 (949) 380-6136
Fax: +1 (949) 215-4996
email: sales.support@microsemi.com
www.microsemi.com

Microsemi Corporation (Nasdaq: MSCC) offers a comprehensive portfolio of semiconductor and system solutions for communications, defense & security, aerospace and industrial markets. Products include high-performance and radiation-hardened analog mixed-signal integrated circuits, FPGAs, SoCs and ASICs; power management products; timing and synchronization devices and precise time solutions, setting the world's standard for time; voice processing devices; RF solutions; discrete components; security technologies and scalable anti-tamper products; Ethernet Solutions; Power-over-Ethernet ICs and midspans; as well as custom design capabilities and services. Microsemi is headquartered in Aliso Viejo, Calif., and has approximately 3,600 employees globally. Learn more at www.microsemi.com.