Grid MP Platform

Version 4.2

ENTERPRISE

System Administrator's Guide

Copyright, Trademark, and Version Notices

Copyright Notice

Trademark Notice

Document and Software Versions

- Document Version 3.0
- Software Version 4.2

About This Guide

The United Devices Grid MP platform uses a software layer to transform existing systems, storage, and networks into a virtual IT infrastructure so that applications are not bound to any specific system. The Grid MP platform selects the most appropriate resources from an enterprise-wide or inter-enterprise resource pool and allows applications to utilize different resources at different times. These resources can be dispersed across geographical and departmental boundaries while allowing control of resource usage at the device level.

Managing this virtual infrastructure involves setting resource usage parameters for groups of devices, creating and maintaining user accounts and access levels, analyzing job performance to best configure the system to handle your system load, and more.

The *Grid MP platform Version 4.2 System Administrator's Guide* describes how to perform the following administration tasks:

- Plan and configure an installation
- Manage and Monitor MP Services, Agents, Devices, and Access Control
- Maintain a supporting database
- Diagnose and correct atypical behaviors

In addition, this guide provides an overview of the concepts on which the Grid MP platform is based and a description of its primary components.

Audience

The audience for this guide is information technology professionals who manage the Grid MP platform. Ideally, Grid MP platform administrators possess a practical understanding of enterprise systems and their infrastructure.

The information technology skills that are required to support the Grid MP platform include

- Red Hat® Linux™ operating system administration skills
- Microsoft® Windows® operating system experience
- IBM® DB2® or Oracle 9*i*™ database experience, depending on the deployment
- Familiarity with Web concepts

Administrators might also benefit from familiarity with batch job management systems, scientific or engineering simulation applications, XML, and SOAP.

Related documentation

The following United Devices documentation is also useful to Grid MP platform administrators:

- *Grid MP platform Version 4.2 Application Developer's Guide*, which describes how to develop or port applications using the MP Software Developer's Kit.
- *Grid MP platform Version 4.2 Installation Guide*, which provides step-by-step instructions for planning and installing the Grid MP platform.
- *Grid MP platform Application User's Guide*, which contains easy, step-by-step instructions for how to submit Jobs and retrieve Results.
- MP Console online help, which provides context-sensitive online help for MP administration tasks. To access the context-sensitive online help from any Grid MP Console window, click the **Help** link in the top right corner of the Grid MP Console screen.
- United Devices Web site at http://www.ud.com/, which provides general information about the Grid MP platform.

In addition, Grid MP platform administrators need documentation for the intranet infrastructure components they maintain.

Using this guide

This section describes how this guide is organized, its typographical conventions, and provides information about printing the guide.

Guide organization

This *System Administrator's Guide* contains the following chapters:

- Chapter 1, "Understanding the Grid MP Platform," on page 1 introduces the Grid MP platform architecture, components, installation and operation, and features.
- Chapter 2, "Configuring the Grid MP Platform," on page 13, explains the configuration parameters you can adjust after the installation.
- Chapter 3, "Managing Services and Logs," on page 29, describes how to manage the MP Services, Management Server, and system log components of the Grid MP platform.
- Chapter 4, "Managing MP Agents," on page 37, describes the MP Agent and discusses MP Agent to MP Service communication, MP Agent packaging and installation, and monitoring and managing MP Agents on Devices.
- Chapter 5, "Managing Devices," on page 51, explains Devices, Device Groups, Device Profiles, and how to manage and utilize these features for optimal scheduling and network performance.
- Chapter 6, "Managing Access Control," on page 81, details the access control features offered by the Grid MP platform and provides step-by-step instruction for creating and managing Users.
- Chapter 7, "MP Console Reports," on page 107, describes MP Console reports.
- Appendix A, "Troubleshooting," on page 113, describes how to identify, diagnose, and correct atypical behavior.
- Appendix B, "Managing the Database," on page 121, describes how to perform basic DB2 and Oracle administration procedures.
- "System Administrator's Guide Feedback Form" on page 143, is a form you can use to provide feedback about this Guide. Print this form, write your comments, and fax it to us at +1-512-331-6235.

Typographical conventions

The following table shows the typographical conventions used in this book.

Table 1: Typographical conventions

Convention	Description
`Courier`	Code examples and screen output

Table 1: Typographical conventions (continued)

Convention	Description
`Bold Courier`	Functions, commands, and user input
Italic	Function and command place holders—replace with the appropriate name or value, such as a file name or path name.
Bold	Menu names, menu commands, menu options, and buttons

Viewing this guide online

This document is best viewed with Adobe® Acrobat® Reader® version 5.0. If you don't have this version of the Acrobat Reader, you can download it here at no charge: http://www.adobe.com/products/acrobat/readstep2.html.

This document contains a number of features that will enable you to navigate quickly and easily through the document:

- Bookmarks are on the left side of the screen. To use the bookmarks, click the bookmark for that section of the document that you want to view. To return to the previous view, right-click and select **Go To Previous View** from the pop-up menu.
- The index is at the end of this document. To go to the page for the topic you want to view, click the page number beside the topic. To return to the previous view, right-click and select **Go To Previous View** from the pop-up menu.
- Links to figures and sections can be seen throughout the document. These links allow you to go to a figure, table, or section that is referenced in the text. You can click any of these links to view the referenced figure, table, or section. To return to the previous view, right-click and select **Go To Previous View** from the pop-up menu.

Printing this guide

This guide is formatted for 8.5" x 11" size paper and designed for duplex printing. A printer that supports duplex printing will print one page of this book on each side of a sheet of paper.

Software maintenance and upgrades

United Devices is committed to improving continuously its products and services. When new maintenance or product releases are available, United Devices Professional

Services will contact you to help plan your upgrade. Upgrades involve assessing application impact, preparing database migration scripts, and testing upgrade procedures. Some licensing issues may also apply. For more information about upgrades, contact United Devices Professional Services.

Contacting United Devices

For technical support or to inquire about the information contained in this document, contact United Devices in one of the following ways:

- For technical support, send e-mail to customer@ud.com.
- For technical support, telephone (800) 370-5320 between 9 A.M. and 5 P.M. (CST) Monday through Friday.
- For Grid MP platform consulting or training, send e-mail to customer@ud.com, or see http://service.ud.com/.

Chapter 1: Understanding the Grid MP Platform

In distributed computing, separate computers that process a common task are linked through a communications network. In the United Devices distributed computing solution, the under-utilized resources of workstations, desktop PCs, laptop computers, and clusters are combined to solve large computational problems. The United Devices Grid MP platform is a software technology that aggregates these resources and utilizes them as a large virtual computer system.

This chapter contains an overview of the Grid MP platform architecture, data flow, interfaces, components, and features.

Grid MP Platform Architecture

The following figure shows the architecture and components of the Grid MP platform and the data flow between components.

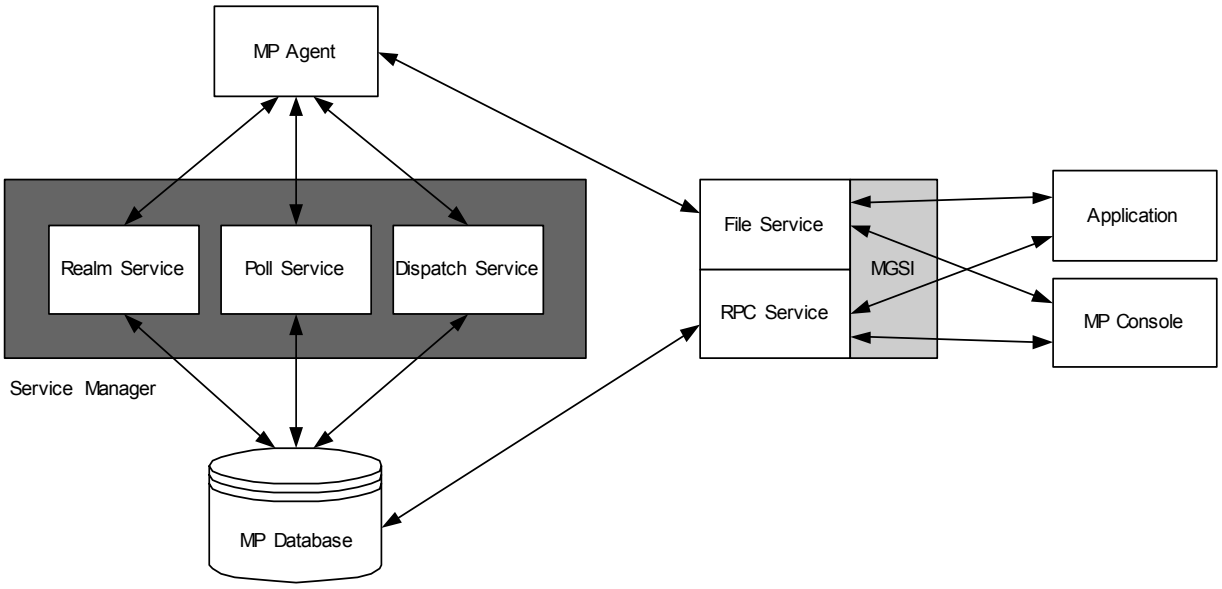


Figure 1. The Grid MP platform architecture, components, and data flow.

Overview of Communication between Components

When the MP Agent starts, it first connects the Device on which it runs to the Realm Service to authenticate and get credentials. Next, the MP Agent contacts the Dispatch Service to request work. The MP Agent then downloads any required files from the File Service and begins processing. While processing the work, MP Agents report usage statistics to the Poll Service. When the work is finished, the MP Agent uploads Results to the File Service, and returns to the Dispatch Service for more work. Application Users and Application Administrators use the MP Console or MGSI to interface with Applications and Jobs.

Grid MP Platform Interfaces

The Grid MP platform provides the following interfaces: the MP Grid Services Interface, the Program Loader, the Program Application Program Interface (TAPI[1]), and the MP Console. You can find MP Console instructions regarding system administration in this document.

For more information about the MGSI, Program Loader, and TAPI, see the *Application Developer's Guide*.

MGSI - RPC Service

The MP Grid Services Interface (MGSI) is comprised of the RPC Service and a File Service. The MGSI-RPC Service is a programmatic interface that provides third-party applications and the MP Console access to the MP Services and the database. The MGSI also incorporates access control for users of these services.

The RPC Service is the programmatic access to the Grid MP platform. The web interface— the MP Console— is written entirely by using MGSI calls. The MGSI defines a large number of functions for controlling the system, available in XML-RPC and SOAP. MGSI also provides an HTTP-based protocol for the upload of data to the system. See "File Service" on page 7 for information about the MGSI-File Service.

1. The acronym TAPI is a legacy term from earlier versions of the Grid MP platform. TAPI was the Task Application Program Interface. The notion of tasks was replaced with Programs and Jobs in the 4.0 release.

Program Loader

The Program Loader is a mandatory executable that loads executable code into memory for execution, and provides automatic encryption and compression for your executables.

NOTE	The Program Loader's encryption features are available on Windows NT®, Windows 2000, Windows XP, Windows Server 2003, Linux, AIX, Solaris™, and Macintosh.

For more information about the Program Loader, see the *Application Developer's Guide*.

MP Console

The MP Console presents a Web-based thin client for managing MP Services, MP Agents, Applications, Jobs, and Data. The MP Console includes these features:

- Security
  - Username and password required to log on
  - Roles and Privileges control User commands and access to data
- Platform Management
  - Easy organization and control of Device usage
  - MP Agent commands
  - Dashboard of service status
- Workload Management
  - Quick Job creation
  - Data and Application management
  - Job and performance monitors
- Context-sensitive help for each screen and step-by-step instructions for commonly performed tasks

United Devices supports the following browsers for the MP Console:

- Microsoft Internet Explorer 5.5 (Service Pack 1) or 6.0
- Netscape® Navigator 6.2.3 or 7.0
- Mozilla 1.01.+

Grid MP Platform Components

The Grid MP platform comprises these components:

Database

The Grid MP platform database is the main storage repository of common information for the Grid MP platform. The database stores the entire state of the system—with the exception of File-Service-controlled Application data—including:

- Administrative information for managing servers; MP Agent modules; administrators; Users, User Groups, and security settings
- Application information such as Data, executables, Job runtime parameters, and other attributes
- Device information such as Device configuration, preferences, MP Agent version, Device Groups, and more

Version 4.2 of the Grid MP platform supports the following database software:

- Oracle 9*i* Patch set 4 version 9.2.0.5 Server on Solaris 8 and Red Hat Linux AS2.1. Oracle client on Red Hat Enterprise Linux ES.
- IBM DB2 Universal Database® Workgroup Edition V8.2 special on Red Hat Enterprise Linux ES.

Most of the interfaces and services communicate directly with the database. The system administrator should not, therefore, have to interact directly with the database under normal circumstances.

MP Agent

The MP Agent is a lightweight program that runs on a Device and manages Job processing. The MP Agent is responsible for the following management functions:

- Communicates with MP Services. For example:
  - Receives tokens from the Realm Service to communicate with the other services
  - Requests work from the Dispatch Service
  - Downloads Program Modules and Data from the File Service or other Web locations
  - Uploads Results through the File Service

  - Provides the Poll Service with performance and status statistics
  - Receives MP Agent command notifications through the Poll Service

- Prevents application and data tampering by utilizing digital signatures when receiving executables

- Collects information about Device characteristics and capabilities

The MP Agent software operates as a native Microsoft Windows service once installed on supported Microsoft operating systems. On Linux machines, the software runs in the background as a daemon.On AIX, Solaris, and Macintosh platforms the software should be run through the command line. Table 3, "Supported Software," on page 16, contains information about the OS versions supported by the MP Agent.

When a new version of the MP Agent is registered through the MGSI as the current version, the installed MP Agent on a Device automatically downloads the new MP Agent module and updates the Device.

Service Manager

The primary function of the Service Manager is to ensure that all required services needed for the proper functioning of the Grid MP platform are always up and running. It provides the following services:

- Starts and stops the Dispatch, File, Poll, and Realm Services

- Periodically checks to ensure that services are up. If any are found to have failed or unexpectedly stopped, the Service Manager restarts the service.

- When services are running on several different machines, a local copy of the Service Manager is started on each separate system

As the Service Manager is responsible for monitoring all other services, it is run in an auto-restart manner so that it will automatically be restarted should it fail.

Realm Service

The Realm Service manages all MP Agent authentication and MP Agent resource access. MP Agents communicate with the Realm Service to register and authenticate themselves. An MP Agent cannot perform any operation until it has authenticated itself with the Realm Service.

The Realm Service handles the following major Roles when interacting with Agents:

- Validation of existing MP Agent User account or creation of new account, and Device registration
- Provision of tokens for distributed authentication of Devices
- Time synchronization
- Transmission of network addresses of other services
- Transmission of Device Profiles associated with the relevant Device Group

Poll Service

The Poll Service collects periodic status reports from MP Agents and communicates commands to the MP Agent from other services. Specifically, the Poll Service is responsible for:

- Gathering computer load data from MP Agents
- Assisting in sending commands to the MP Agent, such as:
  - Re-login—Revoke authentication token and force re-authentication with the Realm Service
  - Reset—Unlink all cached MP Agent Data files and expire authentication token immediately
  - Abort current running Workunit
  - Snooze
  - Shutdown MP Agent
- Heartbeat monitoring: The Poll Service will receive status “heartbeats” from the MP Agent when a Device belonging to a Device Group that has a designated poll period is processing a Workunit. Devices with no specific poll period give status updates when Workunits complete.

Dispatch Service

The Dispatch Service schedules Workunits to Devices based on Device capabilities and availability, and receives Result status from those Devices. Idle Devices in the Grid MP platform connect to the Dispatch Service to receive new Workunits. The Dispatch Service selects and sends a Workunit to each connecting Device.

The Dispatch Service includes a workload scheduler that schedules Workunits to Devices based on Job priority, User priority, resource requirements for the Program, Device preferences and Device capability. Selection of a Workunit at dispatch time also depends on the connecting Device's capability and Workunit time-out settings. The Grid MP platform also supports redundant scheduling and execution of Workunits to ensure Result accuracy. For more information about scheduling, see "Scheduling" on page 59.

When a Workunit is dispatched, all metadata about it is also sent. The files containing actual data are uploaded or downloaded through the File Service.

The Dispatch Service is also responsible for controlling Grid MP licenses. See "Uploading a New License File" on page 119 for more information about licenses.

File Service

The File Service is a secure (SSL encrypted) file transmission service for downloading and uploading data to and from MP Agents during the execution of a Job. It also provides background maintenance of deleted files for all files managed by the Grid MP platform. The primary functions provided are:

- File downloading—All file downloads to an MP Agent will occur via the File Service. Since Program Module executables and some Data files are cached on the Device, they are only transferred when necessary.

- Result uploading—Once an MP Agent has completed processing the Workunit associated with a Job the Result is uploaded to the File Service.

- File Maintenance—Once a file is no longer needed by the system it is marked as deleted in the database, but not immediately deleted from the underlying file system to optimize system performance. The File Maintenance utility cycles through all files marked as 'to be deleted' on a periodic basis and actually deletes files marked for deletion from the file system.

- MGSI Usage—In addition to use by the MP Agent, the File Service also supports programmatic application service interactions such as uploading and downloading Program Modules, Data modules, and Result modules. For more information, see the *Application Developer's Guide*.

Run_batch Service

The Run_batch Service is a low-level service that controls the execution of backend processes on the database, which affect the following operations:

- Result handling
- Error handling
- Sent Workunit handling
- Workunit generation
- Object deletion
- Device polling
- Statistics handling
- Periodic database maintenance

Due to the importance of its function, the Run_batch Service must run continuously; a crontab entry provided by the installer restarts it in the event that it is interrupted. Unlike the Dispatch, File, Poll, and Realm Services, the Service Manager does not control the Run_batch Service.

Grid MP Platform Features

The following sections provide an overview of Grid MP platform system administration features.

Configuration Management

After installing the Grid MP platform, system administrators can change configuration parameters to better suit their needs. Examples of editable configuration parameters include:

- Logging Parameters—How verbose logs should be; specific files to log to, etc. See "Logging Parameters," on page 20 for more information.
- Service Execution Parameters—The username and groupname the system should use to run each specific service; the number of threads to create for processing incoming client connections, etc. See "Service Execution Parameters," on page 20 for more information.

- Networking Parameters—The specific port on which a service should listen; the precise IP address to utilize on a machine with multiple network interfaces, etc. See "Networking Parameters," on page 21 for more information

- Database Parameters—Database username and password; database host and port number, etc. See"Required Database Variables in ud.conf," on page 26.

MP Services and Logs

System administrators can monitor and control MP Services from the command line as well as the MP Console. The following Service and Log related administration tools are available:

- Starting and stopping services. See "Managing Services from the MP Console," on page 29 and "Managing Services from the Command Line," on page 30 for step-by-step instructions.

- Managing the system logs. See "Managing the System Logs," on page 32 for information about the ud.log, messages log, and Apache access log.

- Changing service manager names and IP Addresses. See "Changing Service Manager Name," on page 35 and "Changing the IP Address or Port for a Service," on page 35 for step-by-step instructions.

- Moving services to new hardware. See "Moving Services to a New Machine," on page 36 for more information.

MP Agents

The MP Agent is a lightweight software program that is installed on all Grid MP platform Devices. For more information about how MP Agents communicate with MP Services, see "MP Agent Communication with MP Services" on page 39.

The following MP Agent management tools are available:

- MP Agent GUI—The MP Agent GUI resides on the Device and allows the Device user to send commands, such as snooze and stop, to the MP Agent, as well as to monitor the status of Jobs running on the machine. See "Controlling the MP Agent" on page 42 for instructions on how to install and use the MP Agent GUI for Windows and Linux machines.

- Monitoring Agents—MP Administrators can view the MP Agent logs to see all transactions, such as successful communication with services, downloads and uploads. For help decrypting the logs, see "Monitoring Agents" on page 46.

- Managing Agents from the MP Console—MP Administrators can view and delete MP Agent Versions and MP Agent Modules from the MP Console. See "Managing Agents in the MP Console," on page 46, for step-by-step instructions.

- Assign MP Agent Version to Device Groups—Once you upload a new MP Agent version, you can assign it to Device Groups. For instructions, see "Edit a Device," on page 63.

Manage Devices, Device Groups, and Device Profiles

When the MP Agent on a computer connects with the Grid MP platform for the first time, the Device registers on the platform and displays in the list of all Devices. Device management features include the ability to:

- View a list of all Devices on the Grid MP platform to ensure MP Agents are connecting properly. See"View Devices" on page 61 for step-by-step instructions.

- Create Devices groups based on capability, territorial control, geography, etc. See "Create Device Group" on page 70 for help.

- Move Devices to and from groups. See "Move Device to New Device Group" on page 65 for more information.

- Use Device Profiles to specify Device thresholds, such as maximum disk space a Program can use, whether or not to monitor Device thresholds, and the times of day Device Groups are available to run Jobs. See "Device Profile Properties" on page 57 for more information, and "Create Device Profile" on page 77 for help creating a Device Profile.

- Set Job Priority Level for Device Group—Device Administrators can specify Job priority limits for each User or User Group that has permission to run Jobs on a Device Group. See "Job Scheduling Priority" on page 56 for more information about how this works and "Assign Priority to Jobs from Users or User Groups" on page 72 for instructions.

- Send commands directly to a Device or group of Devices from the MP Console to stop Workunit processing, obtain a new Device GUID, and more. See "Send Device Commands" on page 66 for step-by-step instructions.

Access Control and User Management

Access control and User management features include the ability to:

- Manage User accounts to allow or remove access to the Grid MP platform. For instructions, see "Create a New User" on page 92, "Change User Password" on page 93, and "Disable User Account" on page 94.

- Manage Users with User Groups. The Grid MP platform contains five default User Groups based on the type of work a User in the group is likely to do. You can create User Groups based on project teams, departments, etc. For more information about default User Groups, see "Predefined User Groups" on page 82. For help creating a User Group, see "Create a New User Group" on page 98.

- Add Users to User Groups. See"Add User to User Group" on page 100.

Security

United Devices considers security one of the most important attributes of grid computing. See Chapter 5 of the *Installation Guide* for security recommendations to help you ensure a secure platform environment. General recommendations as well as instructions for utilizing the following security measures are discussed in detail:

- Securing the MP Agent—Creating the Grid MP Agent User account, encrypting initialization information at install time, etc.

- Digital Signatures—Utilizing digital signatures to validate Program Modules before execution

- MP Services security—Utilizing token keys for the Realm and MGSI services, as well as username and groupname control for the Poll, Realm, and Dispatch services.

- Network and operating system considerations

Database Management

- Execute DB2 and Oracle database commands. See "Introduction to DB2 commands," on page 121 and "Introduction to Oracle commands," on page 123 for instructions.

- Backup and restore a DB2 database. See "Regular maintenance - DB2," on page 122 for more information.

- Backup and restore an Oracle9*i* database. See "Regular maintenance - Oracle," on page 124 for more information.

OS compatibility of major features in Grid MP Platform, Version 4.2

The following table lists some of the features of the Grid MP platform and the respective platform compatibility. The left-most column lists the features and the top-most row lists the supported platforms. An X indicates the platform compatibility of the particular feature in the left-most column.

Table 2: OS compatibility of major features in Grid MP Platform, Version 4.2

	Win98/Me	WinNT/2k/ XP/2003	Linux	AIX	Solaris	Macintosh
I/O hooking (transparent encryption/ compression)		X				
C++ libudmgsi SOAP library	X	X	X			
OS-native agent installer and customizer	X (MSI)	X (MSI)	X (RPM)			X (PKG\DMG)
PAR binaries of SDK utilities	X	X	X			
Source for SDK utilities (Perl or C++)	X	X	X	X	X	X
Dynamic user switching of program modules in MP Agent			X	X	X	X
Graphical agent control utility (mpatray)		X				X
Console agent control utility	X	X	X	X	X	X
Targeting of gang-scheduled MPICH jobs via ud_mpirun	X	X	X	X	X	X
Targeting of third party MPI jobs via mpsub	X	X	X	X	X	X
Batch scheduled jobs via mpsub	X	X	X	X	X	X

Chapter 2: Configuring the Grid MP Platform

This chapter discusses the recommended hardware and software configurations and concerns you can control prior to installation and the configuration parameters you can adjust after you have installed the Grid MP platform.

Planning the Grid MP Platform

Successful deployment of the Grid MP platform requires planning. Consider the following impacts on performance when estimating the size of your configuration:

- The minimum Grid MP installation, including Linux, IBM DB2 and the UD database schema, requires approximately 2GB of storage. Expect storage requirements to expand to accommodate database growth and data growth for applications.
- Grid MP platform performance is strongly coupled to the performance of the underlying database; if the hardware running the database is fast, the Grid MP platform will be fast. For best performance the database should be on a separate machine from the rest of the MP services.
- The Dispatch Service will make use of as much memory as is available to cache database information.
- File Service hard disk usage is dependent upon the applications you run on the system. If Data or Result files are large, the File Service machine will require more hard disk space.
- Realm and Poll Service traffic will increase with the number of MP Agents in the system
- The increase of system throughput in your system (the RPC rate or number of results produced per second) will cause the system load to increase overall.

When planning your configuration, also consider the following aspects of your target implementation:

> **NOTE** The following considerations are interdependent. For example, a site with few Devices may require a medium or large configuration, especially if the Devices at the site transfer large amounts of data in short intervals. For more information, contact United Devices Professional Services.

- Number of Devices included in Grid MP platform

  The load on MP Services machines is directly proportional to the number of active Devices that are part of the platform divided by the average Workunit duration. The shorter the average Workunit duration, the more connections a service must simultaneously maintain.

- Network bandwidth

  The network bandwidth among the various components of the platform also determines how you configure this product. Specifically, the bandwidth between the Devices and the MP Services (both upstream and downstream) determines the number and characteristics of servers required. Lower network capacity will lead to longer connection times requiring the MP Services be able to manage more concurrent connections from Devices.

- Platform usage and Job characteristics

  Both the number of Jobs and how frequently they are submitted define platform usage. Heavy platform usage (for example, high number of Workunits at high frequency) indicates that you need a large system configuration. Job characteristics that affect configuration include the computation-communication ratio of the Jobs. The computation-communication ratio refers to the amount of time typically spent during computation on the MP Agent versus the amount of time spent communicating with the MP Services. The size of the configuration is inversely proportional to the computation-communication ratio.

Hardware Requirements

The following general requirements apply to the Grid MP platform Version 4.2:

- Ethernet or Gigabit Ethernet is required on all configurations
- All RAID should be RAID 10. Hardware RAID is preferred.

> **NOTE** RAID 5 increases disk I/O too much for database efficiency.

Small Single-Machine Configuration (Up to 150 MP Agents)

- Single processor Pentium 4 2.4 GHz or better with 1GB RAM.
- Minimum of 40GB storage.

NOTE This configuration is recommended for pilot and demo-deployments or small workgroups only.

Large Single-Machine Configuration (150 - 500 MP Agents)

- Dual processor Pentium 4 2.4 GHz or better with 2GB RAM.
- Minimum of 80 GB storage. For better performance and reliability, RAID is recommended at this level in place of multiple spindles.

NOTE: This is the minimum workgroup configuration

Two-Machine Installation (500-2000 MP Agents):

- Database: Dual processor Pentium 4 2.4 GHz or better with 2GB RAM or more.
  - Minimum of 40 GB storage, but must be RAID.
- Server system: Single processor Pentium 4 2.4 GHz or better with 1GB RAM, but a dual processor with 2GB RAM is recommend for deployments with heavy workloads.
  - Minimum of 40 GB storage.

NOTE This is the minimum recommended configuration for large enterprise deployments

Multi-machine Installations

- Database: Dual processor Pentium 4 2.4 GHz or better with 2GB RAM or more.
  - Minimum of 80 GB storage, but must be RAID.
- Server systems: Single processor Pentium 4 2.4 GHz or better with 1 GB RAM, but a dual/multi-processor machine with 2GB is recommend for the Dispatch Service box with heavy workloads.
  - Minimum of 80 GB storage on file server.

– Other MP Service machines need 20GB or more.

NOTE This configuration is best for very large high volume deployments with large amounts of data requiring separate File Server and or Dispatcher systems:

Configuration Recommendations

The Grid MP platform can be installed and run on a wide variety of hardware and software combinations. This section provides a summary of the supported platform combinations. For more information on configuration options please contact United Devices Professional Services.

The three key platform components that can be varied are the database server, MP Services and MP Agents. The following table summarizes current supported hardware and software platforms.

Table 3: Supported Software

Database	MP Services	MP Agents
• IBM DB2 V8.2 special running on Red Hat Enterprise Linux ES 3.0 • Oracle 9*i* Patch set 4 version 9.2.0.5 running on Solaris 8 • Oracle 9*i* Patch set 4 version 9.2.0.5 running on Red Hat Advanced Server 2.1	• Red Hat Enterprise Linux ES 3.0	• Windows XP, Windows 2000, Windows NT SP6, Windows 98, Windows ME • Red Hat Linux, version 7.2 or higher; Red Hat Enterprise Linux ES 2.1, ES 3.0 and AS 2.1; SuSe Linux 8.0; Mandrake Linux 9.2 • Sun® Solaris 8 and 9 • IBM AIX 5.2 • Mac OS X 10.3

The MP Services themselves can be run in a distributed manner. Hence a variety of combinations can be used to optimize system performance and availability. The following table summarizes typical configurations. For a non-standard configuration for a specific deployment, please contact the United Devices Professional Services team.

Table 4: Supported Configuration Combinations

	Server 1	Server 2	Server 3	Server 4	Server 5
One Machine	Red Hat Enterprise Linux ES 3.0 running: IBM DB2 V8.2 special Database Server and Client MP Dispatch Service MP Realm Service MP Poll Service MGSI File Service MGSI RPC Service MP Console				
Two Machine	Red Hat Enterprise Linux ES 3.0 running IBM DB2 V8.2 special Database Server or Red Hat Advanced Server 2.1 running Oracle 9i Patch set 4 version 9.2.0.5	Red Hat Enterprise Linux ES 3.0 running: MP Dispatch Service MP Realm Service MP Poll Service MGSI File Service MGSI RPC Service MP Console IBM DB2 V8.2 special Database Client or Oracle Database Client			
Four Machine	Red Hat Enterprise Linux ES 3.0 running IBM DB2 V8.2 special Database Server or Red Hat Advanced Server 2.1 running Oracle 9i Patch set 4 version 9.2.0.5	Red Hat Enterprise Linux ES 3.0 running: MP Dispatch Service IBM DB2 V8.2 special Database Client or Oracle Database Client	Red Hat Enterprise Linux ES 3.0 running: MGSI File Service MGSI RPC Service MP Console IBM DB2 V8.2 special Database Client or Oracle Database Client	Red Hat Enterprise Linux ES 3.0 running: MP Realm Service MP Poll Service IBM DB2 V8.2 special Database Client or Oracle Database Client	
Five Machine	Red Hat Enterprise Linux ES 3.0 running IBM DB2 V8.2 special Database Server or Red Hat Advanced Server 2.1 running Oracle 9i Patch set 4 version 9.2.0.5	Red Hat Enterprise Linux ES 3.0 running: MP Dispatch Service IBM DB2 V8.2 special Database Client or Oracle Database Client	Red Hat Enterprise Linux ES 3.0 running: MGSI RPC Service MP Console IBM DB2 V8.2 special Database Client or Oracle Database Client	Red Hat Enterprise Linux ES 3.0 running: MGSI File Service IBM DB2 V8.2 special Database Client or Oracle Database Client	Red Hat Enterprise Linux ES 3.0 running: MP Realm Service MP Poll Service IBM DB2 V8.2 special Database Client or Oracle Database Client

MP Configuration File

Grid MP platform configuration parameters for all MP Services components and the database variables are in the Grid MP platform configuration file located in:

/usr/local/UD/conf/ud.conf

NOTE	The /usr/local/UD directory contains critical files needed for the Grid MP system to function correctly. Under no circumstances should any files be deleted, added, or modified in /usr/local/UD, except as directed by UD documentation.

If services are deployed across multiple computers, each location will have its own ud.conf file. To consolidate the information, you can put all the configuration parameters in one location and then put copies of it on each additional computer. If parameters are not applicable to a server because the MP Service the parameter affects is not located on the box, that section of the ud.conf is ignored.

Configuration File Syntax

The following list summarizes the ud.conf file syntax:

- The ud.conf file is an ASCII text file.
- The pound (or hash) character (#) marks the beginning of a comment. All characters from the pound character to the end of the line are ignored.
- A configuration parameter declaration consists of the following parts, in left-to-right order:
  a. The name of the configuration parameter, typically in all capital letters
  b. The equals character (=)
  c. The value of the configuration parameter, which must be delimited with either single quote characters (') or double quote characters (") if the value contains blank spaces or tabs
- No part of a configuration parameter declaration can include the pound character (#).

Changing MP Configuration Parameters

Follow these steps to change Grid MP platform configuration parameters in the ud.conf file:

1. Log in as **root** to the service machine.
2. Open /usr/local/UD/conf/ud.conf in a text editor.
3. Add or modify Grid MP platform configuration parameters as desired.
4. Save the ud.conf file and close the text editor.

Changes to the ud.conf file take effect when the service restarts. For more information about managing services, including starting and stopping services, see "Managing Services and Logs" on page 29.

MP ud.conf Configuration Parameters

The ud.conf file is divided into sections containing the parameters for each service. Some parameters have a value for each service, such as the UD_*SERVICENAME*_LOGLEVEL. Other parameters only affect one specific service, such as the UD_DISPATCH_AGENT_BACK_OFF_TIME.

This section describes the most common Grid MP platform configuration parameters and provides a sample of the ud.conf for each service.The ud.conf contains additional parameters that are not described in this document.

NOTE The installer populates the default configuration parameters, which do not, generally, need to be changed. Unless specific instructions are provided in United Devices documentation, you should only modify configuration parameters with assistance from Professional Services.

Administrator Email

During installation, the system sets the email address for the Grid MP Administrator in the ud.conf file. This email address is the mailto address for the administrator link on MP Console Error screens. The default e-mail address is root@localhost. To change the email address, modify the UD_ADMIN_EMAIL value in the ud.conf file.

```
# Grid MP Administrative Contact
# ..............................
UD_ADMIN_EMAIL                          = root@localhost
```

Logging Parameters

The following parameters have values specified in the ud.conf for each of the following services: Realm, Poll, Dispatch, File, and Run_batch. See "Log Location" on page 33 for more information about log levels.

- UD_*SERVICENAME*_LOGLEVEL

  The log level determines how verbose the log generated for the service will be. TRACE, DEBUG, INFO, WARNING, ERROR, or FATAL are possible values. FATAL, for example, will only log Errors that cause the Program to exit. TRACE logs as much as possible. If you increase the verbosity of the logs, you should monitor the amount of free space in /var/log, as verbose logs can generate very large files and impact performance.

- UD_*SERVICENAME*_SYSLOG_FACILITY

  Syslog facility to log to. Defaults to 1.

- UD_*SERVICENAME*_LOG_TO_STDOUT

  Enables or disables logging to stdout. 1 enables logging to stdout; 0 disables logging. Defaults to 0.

- UD_*SERVICENAME*_LOGFILE

  If specified, logging is sent to the filename provided. The value defaults to one of the following paths, corresponding to the service:

  /var/log/ud_realm.log

  /var/log/ud_poll.log

  /var/log/ud_dispatch.log

  /var/log/ud_filegc.log

  /var/log/ud_run_batch.log

Service Execution Parameters

The following parameters affect the way the services execute on the platform. With the exception of the UD_*SERVICENAME*_PIDFILE, which is also a parameter for the MGSI File Service and Run_batch Service, the parameters in this list affects the following services: Realm, Poll, and Dispatch.

- UD_*SERVICENAME*_PIDFILE

  The PID filename of the process that is currently running. Specifying a PID filename prevents more than one service from running by locking the filename. The value defaults to one of the following paths, corresponding to the service:

  - /var/run/ud_realm.pid
  - /var/run/ud_poll.pid

  - /var/run/ud_dispatch.pid
  - /var/run/ud_filegc.pid
  - /var/run/ud_run_batch.pid

- UD_*SERVICENAME*_NUMTHREADS

  The number of threads to create for processing incoming client connections. Each thread you specify has one database connecting handle for which you must have license.

  The default number assigned during installation should be adequate for most configurations. Before changing this number, contact Professional Services. Altering it can impact system performance. Defaults to 20.

- UD_*SERVICENAME*_USERNAME

  The local username to use to run the service after initialization and port binding is complete. The username is case sensitive. The default is "nobody.""nobody" is an unprivileged user, and therefore less of a security risk than "root." For even tighter security, however, you can create separate user accounts for each service.

- UD_*SERVICENAME*_GROUPNAME

  Specifies the name of a local group that should be used to run the server after initialization and port binding is complete. The default is "nobody.""nobody" is an unprivileged user, and therefore less of a security risk than "root." For even tighter security, however, you can create separate user accounts for each service.

Networking Parameters

- UD_*SERVICENAME*_PORT

  The service listening port. A positive integer assigned during installation. The value defaults to one of the following ports, corresponding to the service:

  - Poll: 1077
  - Realm: 1078
  - Dispatch: 1079

- UD_*SERVICENAME*_BINDIP

  Specifies a precise service network interface (IP Address) on which to accept incoming connections if the machine has multiple network interfaces. If you do not set this value in the ud.conf, the default is to bind to all network interfaces. To bind a service to one out of a set of several IP addresses that are all accessible on a machine, you must shut down the appropriate service first, add the UD_*SERVICENAME*_BINDIP parameter and value to the ud.conf, and then restart the service.

  UD_WEB_FILESVR_BINDIP, UD_WEB_WEBSVCS_BINDIP, and UD_WEB_MPMC_BINDIP variables (in addition to the pre-existing

UD_POLL_BINDIP, UD_DISPATCH_BINDIP, UD_REALM_BINDIP variables

- UD_*SERVICENAME*_HOST

  The resolvable hostname of the machine hosting the service

- UD_*SERVICENAME*_PORT_SSL

  The SSL port on which service content is served to browsers (default is 443)

Security Parameters

United Devices recommends changing the following keys post-installation for added security. See the *Installation Guide* for instructions.

- UD_REALM_TOKEN_KEY

  An arbitrary secret key string used for generating and validating realm tokens. The value is randomly generated at install time. If you choose to change the UD_REALM_TOKEN_KEY value in the ud.conf file, you must do so on each MP Service machine and it must be the same value on all service machines.

- UD_MGSI_TOKEN_KEY

  An arbitrary secret key string used for generating and validating MGSI tokens. The value is randomly generated at install time. If you choose to change the UD_MGSI_TOKEN_KEY value in the ud.conf file, you must do so on each MP Service machine and it must be the same value on all service machines.

Realm Service Configuration Parameters

For parameter definitions and expected values, see the descriptions above in "Logging Parameters" on page 20, "Service Execution Parameters" on page 20, and "Security Parameters" on page 22.

```
# Realm Service

# ..........................
UD_REALM_PORT                          = 1078
UD_REALM_NUMTHREADS                    = 4
UD_REALM_LOGLEVEL                      = WARNING
UD_REALM_LOG_TO_STDOUT                 = 0
UD_REALM_SYSLOG_FACILITY               = 1
# UD_REALM_LOGFILE                     = /var/log/ud_realm.log
UD_REALM_TOKEN_KEY                     = 68ac5de5-cea5-4eb0-
   8495-e8f81b052a70
UD_REALM_PIDFILE                       = /var/run/ud_realm.pid
UD_REALM_USERNAME                      = nobody
UD_REALM_GROUPNAME                     = nobody
```

Dispatch Service Configuration Parameters

The following parameter is unique to the Dispatch Service.

- UD_DISPATCH_AGENT_BACK_OFF_TIME

  The amount of time in seconds sent to MP Agents when a backoff needs to be explicitly sent; typically due to unavailability of Workunits. Defaults to 300.

For other parameter definitions and expected values, see the descriptions above in "Logging Parameters" on page 20, "Service Execution Parameters" on page 20, and "Security Parameters" on page 22.

```
# Dispatch Service
# ..........................
UD_DISPATCH_PORT                        = 1079
UD_DISPATCH_NUMTHREADS                  = 20
UD_DATABASE_UPDATE_INTERVAL             = 60

UD_DISPATCH_LOGLEVEL                    = WARNING
UD_DISPATCH_LOG_TO_STDOUT               = 0
UD_DISPATCH_SYSLOG_FACILITY             = 1
# UD_DISPATCH_LOGFILE = /var/log/ud_dispatch.log
UD_DISPATCH_AGENT_BACK_OFF_TIME         = 300
UD_DISPATCH_PIDFILE                     = /var/run/
   ud_dispatch.pid
UD_DISPATCH_USERNAME                    = nobody
UD_DISPATCH_GROUPNAME                   = nobody
```

Poll Service Configuration Parameters

For parameter definitions and expected values, see the descriptions above in "Logging Parameters" on page 20 and "Service Execution Parameters" on page 20.

```
# Poll Service
# ..........................
UD_POLL_PORT                            = 1077
UD_POLL_NUMTHREADS                      = 4
UD_POLL_LOGLEVEL                        = WARNING
UD_POLL_LOG_TO_STDOUT                   = 0
UD_POLL_SYSLOG_FACILITY                 = 1
# UD_POLL_LOGFILE                       = /var/log/ud_poll.log
UD_POLL_PIDFILE                         = /var/run/ud_poll.pid
UD_POLL_USERNAME                        = nobody
UD_POLL_GROUPNAME                       = nobody
```

Run_batch Service

For parameter definitions and expected values, see the descriptions above in "Logging Parameters" on page 20 and "Service Execution Parameters" on page 20.

```
# Run Batch Service
# .........................
UD_RUN_BATCH_LOGLEVEL                    = WARNING
UD_RUN_BATCH_LOG_TO_STDOUT               = 0
UD_RUN_BATCH_SYSLOG_FACILITY             = 1
# UD_RUN_BATCH_LOGFILE = /var/log/ud_run_batch.log
UD_RUN_BATCH_PIDFILE                     = /tmp/ud_run_batch.pid
```

MGSI RPC Service Configuration Parameters

For parameter definitions and expected values, see the descriptions above in "Logging Parameters" on page 20 and "Security Parameters" on page 22.

```
# MGSI Services
# .........................
UD_MGSI_TOKEN_KEY = 769EC7C7F389C404585025EC13A2EA7D838A6830
UD_MGSI_LOGLEVEL                         = WARNING
UD_MGSI_SYSLOG_FACILITY                  = 1
```

MGSI File Service Configuration Parameters

The following parameter is unique to the MGSI File Service.

- UD_FILE_ROOT

  The root directory location for data. An absolute path name defined locally on the MP Services. Defaults to /usr/local/UD/data

For parameter definitions and expected values, see the descriptions above in "Logging Parameters" on page 20.

```
# File Service
# .........................
UD_FILE_ROOT                             = /usr/local/UD/data
UD_FILE_LOGLEVEL                         = WARNING
UD_FILE_SYSLOG_FACILITY                  = 1

# MGSI File Service
# .........................
UD_WEB_FILESVR_HOST                      = localhost
UD_WEB_FILESVR_PORT_SSL                  = 28443
UD_WEB_FILESVR_PORT                      = 28080
UD_WEB_FILESVR_USER                      = nobody
UD_WEB_FILESVR_GROUP                     = nobody
```

MGSI File Service - File Maintenance Service

The following parameters are unique to the MGSI File Service File Maintenance:

- UD_FILEGC_FILES_PER_CHECK

  The number of files to look for before calling a do_getSha1sByRange that meets that range. Defaults to 10.

- UD_FILEGC_SLEEP_PER_CHECK

  The number of seconds to sleep for between calls, in order to reduce load on the database computer. Defaults to 5.

- UD_FILEGC_MAX_DB_RETRIES

  The number of times the File Maintenance utility should attempt to retry the execution of database statements upon a database failure. Defaults to 3.

- UD_FILEGC_SLEEP_PER_DB_RETRY

  The number of seconds to sleep for before retrying, upon a database failure. Defaults to 30.

- UD_FILEGC_FILE_AGE_WAIT

  The File Maintenance utility will wait until the file age is at least this many seconds before considering any deletion. Defaults to 3600.

For other parameter definitions and expected values, see the descriptions above in "Logging Parameters" on page 20 and "Service Execution Parameters" on page 20.

```
# File Maintenance Utility
# ........................
UD_FILEGC_LOGLEVEL                      = WARNING
UD_FILEGC_TO_STDOUT                     = 0
UD_FILEGC_SYSLOG_FACILITY               = 1
# UD_FILEGC_LOGFILE                    = /var/log/ud_filegc.log
UD_FILEGC_PIDFILE                       = /tmp/ud_filegc.pid
UD_FILEGC_FILES_PER_CHECK               = 10
UD_FILEGC_SLEEP_PER_CHECK               = 5
UD_FILEGC_FILE_AGE_WAIT                 = 3600
```

Required Database Variables in ud.conf

The following table lists the environment variables that the services needs to work with the IBM DB2 database and Oracle9*i* databases.

```
# IBM DB2
# .........................
UD_DB_PLATFORM                          = db2
DB2INSTANCE                             = db2inst1
UD_DB_HOST                              = localhost
UD_DB_PORT                              = 50000
UD_DB_NAME                              = uddb
UD_DB_USER                              = db2inst1
UD_DB_PASSWORD                          = ibmdb2
DB2DIR                                  = /opt/IBM/db2/V8.2
LD_LIBRARY_PATH                         = /opt/IBM/db2/V8.2/lib
DB2_INSTALL_TABLEDIR                   = /home/db2inst1/db/uddb
DB2_INSTALL_TYPE                        = local

# Oracle 9i (R2)
# .........................
# UD_DB_PLATFORM                        = oci9i
# UD_DB_HOST                            = localhost
# UD_DB_PORT                            = 1521
# ORACLE_SID                            = ORCL
# UD_DB_NAME                            = uddb
# UD_DB_USER                            = SYSTEM
# UD_DB_PASSWORD                        = oracle
# ORACLE_BASE                           = /opt/oracle
# ORACLE_HOME = /opt/oracle/product/9.2.0
# LD_LIBRARY_PATH = /opt/oracle/product/9.2.0/lib
```

Other Configuration Locations

In addition to the ud.conf configuration file, two other configuration locations exist. To make changes to the following configuration parameters in the system, please contact Professional Services.

CAUTION The defaults for these settings rarely need to be changed, and doing so without assistance from United Devices could negatively affect the user experience of the Grid MP platform.

Database Setting Table

The type of settings managed by the database Setting table include:

- Realm Service token expiration period. This affects how frequently MP Agents must reverify their security identity with the Realm Service, and limits the amount of time a deleted or disabled Devices is permitted to continue communication with other services.
- Amount of time by which results can exceed the theoretical maximum.
- Amount of time that must elapse before a Device is considered to be disconnected or dormant. Measured in seconds. This is used for detecting unresponsive Devices and reclaiming outstanding global resources and rescheduling Workunits.
- Device name recycling. Each MP Device is assigned a Device name when it registers with the Realm Service for the first time. Device name recycling allows the same Device name to be used for a fresh install on the same machine (as in the case of a reformat) or a new machine (in the case of a machine being put out of service for a period of time). This allows the new install to keep the same Device record and avoids the proliferation of stale Device records. By default, Device recycling is turned off.
- Whether or not new user accounts can be registered interactively through the MP Agent.
- Number of seconds for MP Agent data collection period. Controls the resolution of Device performance data transmitted back to the Poll Service.

Service Manager Configuration File

The svcmgrconf.xml is located in /usr/local/UD/conf/. Changes should not be made to the file without assistance from Professional Services. The svcmgrconf.xml manages the following types of settings:

- Service names—The name of each service as it displays in the MP Console in the Services Dashboard. During installation, the names for the MP Services default to the machine hostname and the service type. After installation, the service names are controlled by the svcmgrconf.xml file. Changing the name deletes the previous service and creates a new one, which deletes all of the previously gathered service statistics. Service names must be unique for each Service Manager.
- Service Manager Names—The service manager name is the primary unique identifier for a service manager. It cannot be changed without uninstalling and restarting the service manager.

- IP addresses of all machines running services. The IP addresses must be fixed IP addresses (not DHCP or other dynamic allocation schemes). If you need to change the IP address of a service, you must change the IP addresses within ud.conf and svcmgrconf.xml.

- Path to service management scripts used for starting, stopping, and getting status of individual services

- Level of syslog reporting for the Service Manager

uduserconf File

All machines that will run the mpbatch or ud_mpirun utilities must have a copy of a configuration file that specifies necessary information, such as the location of the MGSI File Service and RPC Service. The installation CD-ROM contains a sample configurations file in /tools/uduserconf. For more information about mpbatch, ud_mpirun, and the uduserconf file, see the *Application User's Guide*.

Chapter 3: Managing Services and Logs

This chapter describes how to manage the Grid MP platform services and logs to better configure and monitor the entire platform.

- An overview of the services is available in Chapter 1, "Understanding the Grid MP Platform," on page 1.
- For more information about configuring services, see Chapter 2, "MP Configuration File," on page 18.
- For information about how the services interact with the MP Agent, see Chapter 4, "Managing MP Agents," on page 37.

Managing Services from the MP Console

You can start, stop, and restart the following services from the MP Console Manage Service screen:

- Dispatch Service
- File Service
- Poll Service
- Realm Service

To Navigate to the Manage Service screen:

1. Log on to the MP Console
2. On the Home Page, click **Manage Services** from the Platform Management list of actions.

To Change the Service Status

1. For each service in the list there is a corresponding Service Action drop-down list. Select the action you want to take, such as Stop or Restart, from the drop-down list and click **Commit Changes**.

2. The system displays an Update Successful screen. Click **Continue** to navigate to the Services dashboard.

NOTE	It may take up to two minutes for your changes to take effect and to display in the dashboard.

Managing Services from the Command Line

There are two commands you can use from a shell prompt to manage services: **`mpservices`** and **`mpwebsvc`**. **`mpservices`** controls the Dispatch, Poll, and Realm Services. **`mpwebsvc`** controls the MGSI RPC Service, the MP Console, and the MGSI File Service.

Managing the services can have the following impact:

- Side Effects:
  - Application services utilizing the MGSI may cease to function and may not restart gracefully
  - Users connected via the MP Console will be disconnected and will have to log on again once the **`mpwebsvc`** restart command takes effect.
- Start and stop requests can take up to 2 minutes to complete.
- The **`mpservices`** and **`mpwebsvc`** commands only apply to the services running on the machine where the command is executed. In multi-machine installs it may be necessary to execute the command separately for each machine.
- Order of operation: You must run the **`mpservices`** command before the **`mpwebsvc`** command.

Command Usage

Use the following command to control the Dispatch, MGSI File, Poll, and Realm Services:

`/sbin/service mpwebsvc` *command*

Use the following command to control the MGSI RPC Service, the MP Console, and the MGSI File Service:

`/sbin/service mpservices` *command*

The *command* you send can be one of the following:

- start
- stop
- restart
- status

Automatically Managed Services

You cannot start and stop the following services manually because a crontab process automatically restarts them:

- Service Manager
- Run_batch Service
- File Maintenance Service (part of the File Service component, but it is automatically restarted).

  If the database is shut down for any reason, a crontab will attempt to restart the above services. Depending on the log level for the services, the Run_batch Service and File Maintenance Service will log an Error and exit each time crontab attempts to launch it unless the crontab is disabled. To temporarily disable the auto restart, edit the root user crontab. Contact Professional Services for assistance.

Service Manager Command

While you cannot start or stop the Service Manager, the **`svcmgr`** utility allows you to control certain Service Manager details. The **`svcmgr`** utility is located in /usr/local/UD/services. It has the following command-line options:

- **`--help`**

  Display the help file, which contains the content presented here.

- **`--version`**

  Print the version of the Service Manager utility.

- **`--configfile=path`**

  If specified, the location of the Service Manager configuration file. The default is /usr/local/UD/conf/svcmgrconf.xml

- **`--pidfile=path`**

  If specified, the location of the Service Manager pid file. The default is /tmp/ud_svcmgr.lock

- **`--debug`**

  Writes all logging to the MP Console as well as syslog, to allow for easier debugging.

- **`--remove`**

  Removes the Service Manager from the MP database. May optionally be used with the **`--configfile`** option to specify a Service Manager to remove. Stopping all the services and disabling the Service Manager crontab are necessary steps before attempting to use the **`./svcmgr --remove`** command. Failure to do so would leave the system in an inconsistent state. See "Changing Service Parameters," on page 34 for more information about using this command.

Managing the System Logs

There are three types of logs available to you to help you manage the system: the messages log, the ud.log, and the Apache logs. While the information contained within the logs can be very useful, it is also important to manage the size of the logs. If you notice that /var/ is utilizing too much disk space, you may need to decrease the size of one or more of the logs or increase the size of /var/.

/var/log/messages

/var/log/messages contains system information, such as startup and shutdown of OS processes and errors, generated by the Red Hat Linux operating system.

/var/log/ud.log

The logging component of the Grid MP platform utilizes the Linux syslogd system utility. All services direct most internally generated messages to the ud.log by default. In addition, to make troubleshooting more efficient, Apache error logs, which provide all HTTP errors for the Web services are redirected to ud.log.

For lightweight systems, the local ud.log file is adequate. For larger Grid MP systems, a centralized logging service might better provide the capacity and centralized manageability needs of the configuration. Like the MP Services, you can devote an entire machine to /var/log/ud.log if necessary for your configuration. For instructions for logging to a different file or to stdout, see "Log Location" on page 33.

The syslogd utility supports both local and remote logging. When logging messages to a local file, configure the utility with the following options:

- Ensure the /var/log/ud.log file name in /etc/syslog.conf begins with a hyphen
- Avoid degrading system response time:
  - Do not allow syslogd to sync to disk every time it writes to the log file
  - Increase the syslogd buffer from 64KB to 1MB

To facilitate error tracing, United Devices recommends that applications that use the MGSI direct internally-generated messages to the ud.log file.

Log Location

You have the choice of logging to /var/log/ud.log, stdout, or any file of your choosing. All three outputs are optional, but it is highly recommended that you make use of this tool. By default, the syslogd utility logs to /var/log/ud.log. The following /usr/local/UD/conf/ud.conf parameters control where the system logs output.

- UD_*SERVICENAME*_SYSLOG_FACILITY

  The SYSLOG_FACILITY parameter must be set to an integer between 0 and 7. If it is not set, logs do not go to syslog. The SYSLOG_FACILITY corresponds to syslog facility LOG_LOCALx, where x is the integer specified.

- UD_*SERVICENAME*_LOG_TO_STDOUT

  If this parameter is set to 1, stdout will also receive the syslogd utility output. If the parameter is set to 0, stdout logging is disabled.

- UD_*SERVICENAME*_LOGFILE

  The LOGFILE parameter is empty by default. You can supply a string path to the file of your choice.

Loglevel

The amount of information in the ud.log depends on the log level set for each of the UD_*SERVICENAME*_LOGLEVEL parameters in the ud.conf configuration file. There are six logging levels, listed in order of decreasing verbosity below. The ud.conf parameter value is first; the mapping to syslogd level is in parenthesis.

- TRACE (LOG_DEBUG)—Logging at the TRACE level can affect system performance, as the amount of output is quite large.
- DEBUG (LOG_INFO)—Logging at the DEBUG level can affect system performance, as the amount of output is quite large.

- INFO (LOG_NOTICE)—This is the default log level for the MGSI RPC Service.
- WARNING (LOG_WARNING)—This is the default log level for most services.
- ERROR (LOG_ERR)
- FATAL (LOG_CRIT)

NOTE If you increase the verbosity of the logs, monitor the amount of disk space remaining on the that /var partition periodically to ensure it has enough space remaining to contain the logs. You might also increase the logrotate threshold in /etc/logrotate.d/mpservices and the frequency with which it rotates, which is controlled by a crontab entry.

For more information about the ud.conf file, see "MP Configuration File" on page 18.

Apache Access Logs

You can access standard Apache error and access logs for MP Services. Access logs provide you with information concerning client connections and error logs provide all HTTP errors for the services. Logs for the following services can be found in the /var/log/UD/inetpub/host/:

- MGSI RPC Service—Logs can be found in /var/log/UD/inetpub/log/host/websvcs
- MGSI File Service—Logs can be found in /var/log/UD/inetpub/log/host/filesvr
- MP Console—Logs can be found in /var/log/UD/inetpub/log/host/mpmc

NOTE Apache error logs log to the MP System Log, /var/log/ud.log.

Changing Service Parameters

At some point you might need to change MP Services parameters on the Grid MP platform, either by changing the IP address or port number assigned to a service, or by changing the actual machine on which the service is installed. United Devices suggests working closely with a Professional Services representative for this type of work. The following instructions are provided as a guide to assist you in understanding what is involved in the process.

Changing Service Manager Name

1. Shut down services on the machine(s) affected.
2. Disable the crontab that automatically restarts the Service Manager to keep the Service Manager from re-registering the old Service Manager name between the time when you run **`svcmgr --remove`** and when you save the changed name to svcmgrconf.xml:
   a. To edit the crontab, as root issue the command **`crontab -u root -e`**. This will place you into the vi editor with the crontab file loaded.
   b. To disable a crontab entry insert a pound sign (#) at the beginning of the line for that entry, and then save the file and exit.
3. Run **`./svcmgr --remove`** on the machine(s) affected to de-register the old Service Manager record from the database (so the MP Console will not continue to display the old information).
4. Open the svcmgrconf.xml file and change the value for the name parameter under the Service Manager heading. Save and close the file.
5. Enable the crontab entry
   a. As root issue the command **`crontab -u root -e`**. This will place you into the vi editor with the crontab file loaded.
   b. To enable a crontab entry remove the pound sign (#) from the beginning of the line for that entry, and then save the file and exit.
6. Restart services on the machine.
7. Check the MP Console to ensure the changes were made successfully.

Changing the IP Address or Port for a Service

If the hostname or IP address of a service needs to change, the URLs within svcmgrconf.xml and ud.conf must be updated. During install, the URLs in those files are automatically populated with correct initial settings. To change the information after installation:

1. Shut down the services on all machines.
2. Disable the crontab that automatically restarts the Service Manager to keep the Service Manager from re-registering the old Service Manager information:
   a. To edit the crontab, as root issue the command **`crontab -u root -e`**. This will place you into the vi editor with the crontab file loaded.
   b. To disable a crontab entry insert a pound sign (#) at the beginning of the line for that entry, and then save the file and exit.
3. Specify the new ports for the services in /usr/local/UD/conf/ud.conf file and usr/local/UD/conf/svcmgrconf.xml file on each machine.

4. Enable the crontab entry
   a. As root issue the command **`crontab -u root -e`**. This will place you into the vi editor with the crontab file loaded.
   b. To enable a crontab entry remove the pound sign (#) from the beginning of the line for that entry, and then save the file and exit.
5. Restart all services on all machine.

Moving Services to a New Machine

If you want to move all services on a machine to a different machine, follow these steps:

1. Shut down services on the affected service machines.

   NOTE Shutting down a service may cause dependent services to fail. The Grid MP platform is robust enough to handle a service being down, causing workload to queue or back off until the service is once again available.

2. Use the uninstaller script provided on the MP Installation CD-ROM. The uninstaller automatically removes all MP components from the computer. The script is located in /usr/local/UD/uninstaller.sh.
3. On the new machine, use the installer script to install the services. The script is located in /mnt/cdrom/installer.sh. The installer automatically starts services on the new machine.
4. Restart services on other machines.

NOTE If you want to remove only one service from a machine hosting two or more services, contact Professional Services.

Chapter 4: Managing MP Agents

The MP Agent is a lightweight software program that is installed on all Grid MP platform Devices. The MP Agent communicates with various MP Services, supervises the execution of Workunits on the Device, ensures that the Device preferences are being respected, manages all Grid MP related files that are cached on disk, and ensures the integrity of the data in these files.

This chapter discusses the MP Agent in more detail and provides instructions for managing the MP Agent.

Installing and Configuring the MP Agent

The MP Agent software operates as a native Microsoft Windows service once installed on supported Microsoft operating systems. On Linux machines, the software runs as a background daemon. Running in the background allows Jobs to run on the Device whether or not a user is logged on to the machine, and ensures the MP Agent is unobtrusive while a user is logged on.

Supported Operating Systems

The MP Agent requires an x86-compatible computer running one of the following operating systems:

- Windows 98
- Windows Me
- Windows XP
- Windows 2000
- Windows NT 4.0, Service Pack 5 or higher

- Windows Server 2003

NOTE Windows computers must have NTFS disk format in order for Agents to be able to handle files greater than 2 GB.

- Red Hat Linux, version 7.2, 7.3, 8.0, and 9.0
- Red Hat Enterprise Linux ES 2.1 and ES 3.0
- Red Hat Enterprise Linux AS 2.1
- Fedora™ Core 2
- Debian® 3.0

NOTE You cannot install the MP Agent on Debian using RPM; it must be installed via manual copying.

MP Agent versions are also available for the following operating systems:

- IBM AIX 5.2
- Sun Solaris 8 and 9
- Mac OS X 10.3

MP Agent Installation

The installer registers the MP Agent module with the Grid MP platform to load the Microsoft Windows MP Agent binary or Linux version. The installation package can be modified to automatically assign the Device running the MP Agent to a specific Device Group or Device Profile. Other configuration options include username and password registration for the Device to access the Grid MP platform, and the public key used by the MP Agent to verify Program Module executable and MP Agent module downloads from the File Service. For more information about MP Agent packaging and installation instructions, see Chapter 6 of the *Installation Guide*.

Updating the MP Agent

The MP Services automatically update the MP Agent software and the Jobs it manages when these conditions are present:

- A different version of a Program Module executable or the MP Agent software is available in the database.
- The MP Agent contacts the MP Services and its software version or the Program Module Version does not match the version number of the active MP Agent software or Program Module Version.

MP Agent Communication with MP Services

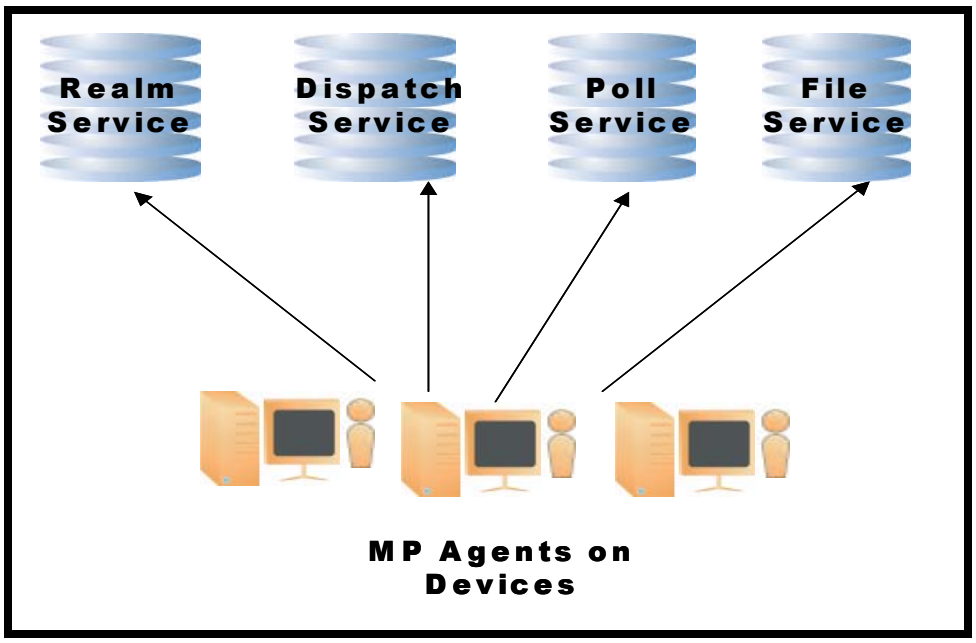


Figure 2. Agent to Service Communication

MP Agent to Realm Service

During initial start up, the MP Agent must first connect with the Realm Service to register its Device account. The address of the Realm Service is specified in the MP Agent's initialization file.

After initially registering with the Realm Service, the Agent must obtain an authentication token for the Device account from the Realm Service and details about the Device Group and Device Profile to which the Device is assigned. This includes

the addresses of the Dispatch Service, Poll Service, and File Service, the polling interval, and a time window for computation and communication.

MP Agent to Poll Service

The MP Agent connects to the Poll Service at the configured time interval to report load data and receive any pending commands. MP Agents report the following system-load information about the Device to the Poll Service:

- Device ID, User ID of Agent (supplied via authentication token)
- Current Workunit IDs actively in progress
- Additionally queued Workunit IDs not yet in progress
- Agent/Device snooze status
- CPU load average on MP Agent

If the MP Agent is deployed to poll, it will accept the following information from the Poll Service:

- Commands (kill a Job, clean-up files, re-login, snooze)
- Pause and restart of running Job(s)
- New polling interval and other relevant service information

NOTE The poll period is set at the Device Group level and is optional. MP Agents installed on Devices that belong to a Device Group with no poll period specified will communicate with the Poll Service at Workunit completion.

MP Agent to Dispatch Service

The MP Agent connects to the Dispatch Service when it is necessary to retrieve additional Workunits, or when it needs to indicate that Results have been uploaded. Once a Workunit has been received from the Dispatch Service, the MP Agent runs the Workunit. After returning Results via the File Service, the MP Agent connects to the Dispatch Service and sends back information about the Result. After returning a Result, the MP Agent gets another Workunit from the Dispatch Service.

The Dispatch Service is also responsible for sending MP Agent module upgrades. The actual upgrade files are always sent to the Agent by the File Service.

MP Agent to File Service

After receiving details about an additional Workunit from the Dispatch Service, the Agent may need to retrieve the actual files from the File Service(s) associated with the Device Group.

After completing a Workunit, the MP Agent uploads the Result file to the File Service. If the File Service indicates that it already has a file corresponding to the same sha1 hash, then the Result file upload is not necessary. In either case, the Agent will then communicate with the Dispatch Service to indicate that the Result file is uploaded and provide it with the sha1 hash, CPU time, Result code, and other information associated with the Result.

Data Management on the MP Agent

MP Agents perform the following key functions with regard to receiving and maintaining data:

- Receiving Workunit Data—The MP Agent receives a token that a new Workunit is available to run from the Dispatch Service. All files are downloaded from the File Service or a URL provided by the Job creator.
- Managing files on the MP Agent—The MP Agent manages the MP Data Cache where it keeps and tracks all executables and Data it needs to process Workunits.
- Digital signatures—Program modules can be digitally signed for authenticity using a custom private/public key pair. The MP Agent can be configured during installation to only accept Program Modules that are signed using a specified key.

Employing Digital Signatures

You can utilize digital signatures to secure the Job submission process. When an MP Agent communicates with the File Service and receives a Program Module executable, it can use a public key to verify whether the executable has a valid digital signature. To utilize this key security, you employ udsign, a Program included on the installation CD-ROM, to create the following keys:

- A public_key value for MP Agent installations. Create the public_key value prior to installing the MP Agent on the client machine(s). Then use the value to define the INITUD_SIGN_PUBLIC_KEY (or sign_public_key for Linux installs) parameter in the init.ud file.
- A private key file for signing executables. Create this key after you create the public key. United Devices recommends that application developers send executables to the administrator in charge of installations to have the executable

file “signed” by udsign. During installation of the MP Agent, the administrator can specify the public key to use. If the public key is used, then all executables must be signed by the corresponding private key.

For help using udsign, see Chapter 5 of the *Installation Guide*.

Controlling the MP Agent

Depending on what you want to accomplish, you can control the MP Agent in different ways. You can send simple commands and check MP Agent status from the MP Agent user interface or you can start and stop the MP Agent service on the Device.

The MP Agent user interface and service commands are slightly different depending on the Device operating system.

The MP Agent User Interface

The MP Agent user interface executables allow Device users to monitor and manage the MP Agent on their machines. Administrators can push the file out to the Device machines or inform users of a location from which they can download it. The executables are not installed as part of the mpagent installer and will not be auto-updated in future releases. The executable files are included in the mpagent directory on the Grid MP Installation CD-ROM in the following locations:

- Windows MP Agent GUI: mpagent\win32\agent\mpatray.exe
- Windows MP Agent command-line interface: mpagent\win32\agent\mpactl.exe
- Linux MP Agent command-line interface: /mnt/cdrom/mpagent/linux/agent/mpactl
- Aix MP Agent command-line interface: /mnt/cdrom/mpagent/aix/agent/mpactl
- Solaris MP Agent command-line interface: /mnt/cdrom/mpagent/solaris/agent/mpactl
- Macintosh MP Agent command-line interface: /mnt/cdrom/mpagent/macosx/agent/mpactl
- Macintosh MP Agent GUI: /mnt/cdrom/mpagent/macosx/tools/mpatray_Archive.dmg

The executable can be started from any directory on an MP Agent Device.

NOTE	Device Administrators can send commands to Devices from the MP Console to abort Workunits, snooze the MP Agent, and so on. For more information, see “Send Device Commands” on page 66.

Windows MP Agent GUI

The MP Agent taskbar executable (mpatray.exe) provides the user with a graphical interface and is accessible from the Windows taskbar.

NOTE	The Windows MP Agent GUI will not run on the Windows 98 or Windows Me operating systems.

The user must have Microsoft Windows power user privileges to access the start, stop, and pause commands. Without power user privileges, the user can see the MP Agent status and read the help file. Click **Start** > **Programs** > **Grid MP Agent Tray Icon** and then click on the **Grid MP Agent Tray Icon** option; the Grid MP Agent tray icon appears in the Windows taskbar. To use it, the Device user can either click or right-click the icon in the taskbar.

Macintosh MP Agent GUI

The Macintosh MP Agent executable (mpatray) is accessible from the status bar at the top of the screen.

NOTE	The Macintosh MP Agent GUI will not run on the Mac OS 10.2 operating systems.

MP Agent Interface Elements

Clicking the icon displays the MP Agent status window, which includes the following information:

- Device Name
- Status
- Workunit and Program information

Right-clicking the icon displays a menu with the following commands:

- Current State—Displays the status of the MP Agent, whether Unknown, Stopped, Running, or Snoozing.
- Stop—Completely stops the MP Agent. Currently running Jobs are aborted. Further Jobs will not be sent to the Device until the MP Agent is restarted. If the Device is rebooted, the MP Agent will restart automatically.
- Start—Starts the MP Agent. Prior Jobs that have been aborted by a Stop command will restart. New Jobs can be dispatched to the Device.
- Snooze—Suspends the Job execution process flow for 5 minutes. After 5 minutes have passed, the MP Agent automatically resumes the processes.
- Preferences—Allows configuration of the Snooze interval. Snooze can be disabled or the snooze interval can be set for the shortest duration of one minute to the longest of 10 hours.
- Hide Icon—Stops the mpatray and removes the Grid MP Agent Icon from the Windows taskbar.
- Show Status—Opens the MP Agent window. The MP Agent window displays the Device name, the status of the MP Agent, and any Job Workunits currently running on the Device. The following status levels exist:
  - Unknown
  - Stopped
  - Running
  - Snoozing
- About the MP Agent—Opens a help window that describes the commands.

MP Agent Command Line Interface

The mpactl.exe and mpactl tools allows you to start, stop, snooze, and retrieve status information about the MP Agent from the command line. To run the tool, type one of the following commands:

For Windows:

`mpactl.exe` *command*

For Linux, Aix, Solaris, and Macintosh:

`./mpactl` *command*

Replace *command* with one of the following options:

- **`start`**
- **`stop`**
- **`snooze`**
- **`status`**

Controlling the MP Agent Service

Controlling the Windows MP Agent Service

From Windows 2000, Windows NT 4.0, and Windows XP, there are two ways to start and stop the MP Agent as any Administrator or Power user:

1. From the command-line interface:
   - **`net start mpagent`**
   - **`net stop mpagent`**
2. From the Services Control Panel:
   - Click Start Menu>Settings>Control Panel>Administrative Tools>Services. In the Services window, find MP Agent and select **Start** or **Stop**.

To check the status of the MP Agent, type the following command from the Windows command line:

```
net status mpagent
```

Controlling the Linux MP Agent Service

From the Linux command line, type one of the following commands to start or stop the MP Agent as root.

- **`service mpagent start`**
- **`service mpagent stop`**

To check the status of the MP Agent, type the following command from the Linux command line:

```
service mpagent status
```

NOTE The above commands will only work if the MP Agent was installed via RPM.

Monitoring Agents

The MP Agent logs transactions, such as successful communication with services, downloads and uploads, and errors to an encrypted cslg.ud file, which resides in the same directory as the MP Agent executable (mpagent.exe for Windows and mpagent for Linux). United Devices provides you with a decryption tool in the form of decryptlog for Red Hat Linux and decryptlog.exe for Microsoft Windows. You can find these tools on the installation CD-ROM in the misc/ directory.

To use the decryption tool on Linux machines type the following command from the MP Agent directory:

```
./decryptlog -f cslg.ud
```

To use the decryption tool on Windows machines, type the following command from the MP Agent directory:

```
decryptlog.exe -f cslg.ud
```

In both cases, the system will display the decrypted cslg.ud log entries. Using the **`-f`** option allows you to monitor the log as transactions are written to the file. Remove the **`-f`** option to see only the last 10 lines.

NOTES

A cslg.ud file is created when the MP Agent first communicates with one of the MP Services.

On Windows 9x and Windows Me, the cslg.ud file may show error entries even if the Jobs executed successfully. This is because collection of some types of information is not supported by the MP Agent under Windows 9x and Windows Me environments.

Managing Agents in the MP Console

The Grid MP platform Version 4.2 supports the use of multiple versions of the MP Agent to allow for testing with different Device Groups. For example, when introducing a new version of the MP Agent, you might select a population of Devices to introduce to it, while continuing with the older version for the majority of your resources. This allows your computing project to continue uninterrupted, while you make the necessary upgrades. Creating new MP Agent versions and modules, deleting and viewing, however, are not frequently performed tasks.

View Agent Versions

You can view a list of the existing versions of the MP Agent in the system through the MP Console from the MP Agent screen. The screen lists the current versions, the number of Device Groups using the version, and the date the version was created. From this list, you can link to more detailed views of specific versions.

Where to Start

1. Log on to the MP Console.
2. Click Start > Platform > MP Agent. The system displays the MP Agent screen

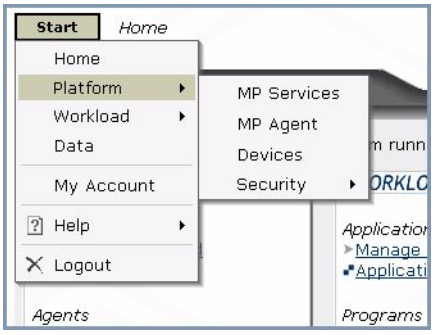


Figure 3. Start Menu

Using the Screen

- Click a version name to navigate to a detailed view of a specific version.
- Use the arrows to sort the list by name or created date.

View Version Details

You can view a list of the existing versions of the MP Agent in the system through the MP Console from the MP Agent screen. The screen lists the current versions, the number of Device Groups using the version, and the date the version was created. From this list, you can link to more detailed views of specific versions.

Where to Start

1. Log on to the MP Console.
2. Click Start > Platform > MP Agent. The system displays the MP Agent screen

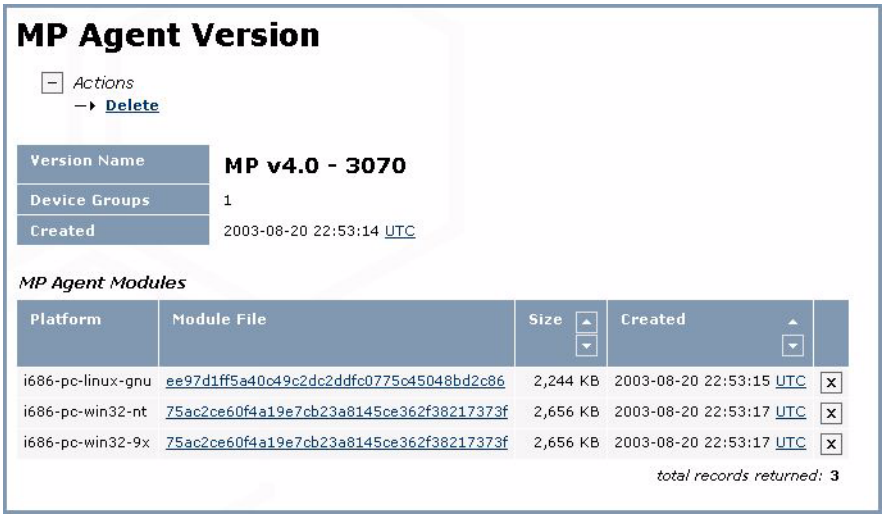


Figure 4. MP Agent Version Screen

Using the Screen

- Click a module file to download the file to your hard disk.
- Use the arrows to sort the list by size or created date.

Delete MP Agent Versions

Once an MP Agent version is no longer useful, you can delete it from the MP Console Delete MP Agent screen.

Where to Start

1. Log on to the MP Console.
2. Click Start > Platform > MP Agent. The system displays the MP Agent screen.
3. Click the name of the version for which you want to view details. The system displays the MP Agent Version screen
4. Click **Delete**. The system displays the Delete MP Agent screen.
5. Click **Delete**. The system prompts you to confirm the delete action.
6. Click **OK** to delete.

Using the Screen

- Before you can delete an MP Agent version in use by one or more Device Groups, you must first edit the Device Groups to use a different MP Agent Version.
- Delete actions can not be undone.
- From the Delete MP Agent screen, click **Cancel** to return to the MP Agent details screen.
- From the Delete confirmation prompt pop-up window, click **Cancel** to return to the Delete MP Agent screen.

Delete Agent Modules

Once they are no longer useful, you can delete MP Agent modules from the MP Console Delete MP Agent screen.

NOTE	If Devices that were using the deleted MP Agent module attempt to connect to the Dispatch Service, the MP Agent software will back the Device off.

Where to Start

1. Log on to the MP Console.
2. Click Start > Platform > MP Agent. The system displays the MP Agent screen.
3. Click the name of the version containing the module(s) you want to delete. The system displays the MP Agent Version screen
4. Click the **X** corresponding to the module you want to delete. The system displays the Delete Agent Module screen.
5. Click **Delete**. The system displays a confirmation window.

- Click **Ok** to complete the delete process.

Figure 5. Delete Module Screen

Using the Screen

- Delete actions can not be undone.
- From the Delete MP Agent Module screen, click **Cancel** to return to the MP Agent details screen.
- From the Delete confirmation prompt pop-up window, click **Cancel** to return to the Delete MP Agent Module screen.

Chapter 5: Managing Devices

A Device in the Grid MP platform is a computer running the MP Agent software. Devices can be grouped into Device Groups to allow Device administrators to manage many Devices at once. Administrators employ Device Profiles to control the types of Programs a subset of Devices can run, the scheduling of Jobs for the Devices, and the amount of Device disk space Programs can utilize.

This chapter discusses the following Device management objects and concepts:

- Devices
- Device Groups
- Device Profiles
- Job scheduling issues
- Device monitoring and Workunit rescheduling
- Device management tasks in the MP Console

Devices

A Device in the Grid MP platform is a computer running the MP Agent software. To display in the MP Console, a Device must first be registered by installing the MP Agent software on the physical machine and allowing it to connect to the Grid MP platform. When the Device first connects, the system will automatically add it to either to the default Device Group, or a Device Group specified during the MP Agent installation configuration process.

A Device can have one of the following connection levels:

- Connected—As of the last poll, the Device was connected.
- Disconnected—The Device has not connected via the MP Agent in 180 seconds
- Dormant—The Device has not connected in 36000 seconds (ten hours)

Device administrators set the poll period at the Device Group level. If the Device Group does not have a polling period specified, the defaults listed above are used. Contact Professional Services for help changing the thresholds that define the status of Devices.

Device Properties

Device Group and system administrators can edit the following attributes for a Device:

- State—The state of the Device:
  - Disabled

    This Device can not receive more Workunits
  - Enabled

    This Device can receive Workunits

> **NOTE** Disabling a Device will prevent it from receiving Workunits and using a Grid MP platform license. For more information about licensing, see "Uploading a New License File" on page 119.

- Device Name—The name of this Device. This field is only unique if the system-wide Device recycling feature has been turned on. For information about the Device recycling feature, see "Device Recycling" on page 54.
- Description: A free-form textual description of this Device.
- Location: A free-form textual description of the physical location of this Device.

The following attributes are either assigned by the system or retrieved from the Device by the MP Agent at poll time:

- GUID—A unique identifier for each Device in the Grid MP platform. The MP Console does not display GUIDs unless the User chooses the Advanced view when logging on to the MP Console.
- Device Profile GUID—The Device Profile to which this Device belongs. The MP Console does not display GUIDs unless the User chooses the Advanced view when logging on to the MP Console.
- Creation Time—The time the Device first registered with the database via the MP Agent.
- Last Modified Time—The timestamp at the last update to the Device record.
- Platform: A text-string specifying the platform in terms of the hardware architecture and the Operating System. The following are valid for this release:

  - Windows NT, 2000, XP running on x86: i686-pc-win32-nt
  - Windows 98, ME running on x86: i686-pc-win32-9x
  - Red Hat Linux running on x86: i686-pc-linux-gnu
  - IBM AIX: powerpc-ibm-aix5.2.00
  - Sun Solaris: sparc-sun-solaris
  - Macintosh: powerpc-apple-macosx10.3

- Number of CPUs—The number of processors installed on the Device. 1=single processor, 2=dual processor.
- CPU Clockrate—The approximate processor speed of Device in megahertz
- CPU Cache—The size of processor L2 cache in bytes
- Physical RAM—Amount of total physical RAM installed on Device (in megabytes)
- Virtual Swap Space—Current amount of total possible virtual memory swap space (in megabytes)
- Disk—Total size in megabytes of the partition on which the MP Agent is installed
- CPU Vendor—Name of the manufacturer of the processor (i.e.: "Intel", "AMD" etc.)
- CPU Model—Name of the processor model (i.e.: "Pentium 4", "K6", etc.)
- OS Name—Name of the operating system (i.e.: "Windows XP", "Windows 98", "Linux", etc.)
- OS Version—Textual representation of the operating system version number
- Computer Vendor—Name of the computer vendor, if known (i.e.: "Dell", "Gateway").
- Computer Model—Name of the computer vendor model, if known
- CPU Architecture Type—Processor architecture type
- Available ISAs—List of Instruction Set Architectures available. This space-separated list of keywords indicates processor capabilities, such as MMX extensions or the availability of an FPU.
- Installed NICs—List of network interface adapters installed

- UTC Offset—The number of minutes to add to UTC to get the local time. For example CST is six hours behind UTC, so this value is -6*60 = -360
- Agent Version—The MP Agent version descriptor of the Device
- CPU Whetstones—The whetstone rating of the Device
- Free Disk Space—The total number of free megabytes available to the MP Agent without deleting items from the cache
- Disposable Free—The total number of megabytes available to the MP Agent if it deletes all items from the cache
- Last Contact Time—The time the Device last contacted the Dispatch Service
- IP Address—The last known IP address for the Device

Some of the above information collected by the MP Agent can be used by application administrators to target Devices with specific resources. Application administrators specify resources such as minimum free disk space, CPU clockrate, or physical RAM when creating Programs. The Dispatch Service then uses those requirements as part of the scheduling process. Other information about Device load, such as memory and disk usage, can be monitored and used to decide when it is appropriate to abort a job and reschedule it to another device.

Device Recycling

Each MP Agent Device is assigned a Device name when it registers with the Realm Service for the first time. Device name recycling allows the same Device name to be used for a fresh install on the same machine (as in the case of a reformat) or a new machine (in the case of a machine being put out of service for a period of time). This allows the new install to keep the same Device record and avoids the proliferation of stale Device records. By default, Device recycling is turned off. Turning it on requires a change to the Database SETTING Table, with the assistance of a Professional Services team member. For more information about the Database Setting table, see “Database Setting Table” on page 27.

Device Groups

Every Device must belong to one and only one Device Group. The installation process creates one default Device Group. Devices that register with the Grid MP platform automatically join the default Device Group unless you configure the MP Agent installer package to add the Device to a different group.

You can manage multiple Devices by utilizing Device Groups. Operations can be applied to many Devices at once. Device administrators can specify which Applications and/or Programs can run on a Device Group. Applications and Programs may be excluded from a Device Group either due to administrative policies or due to resource limitations in the Device Group.

Device Group Properties

Device group and system administrators can edit the following attributes for a Device Group:

- State—The state of the Device Group:
  - Disabled

    Devices in this Device Group can not receive more Workunits
  - Enabled

    Devices in this Device Group can receive Workunits
- Device Group Name—The unique name of the Device Group. Required field. Name cannot have leading or trailing spaces.
- Description—The free-form textual description of this Device Group.
- Poll Interval—The interval (in seconds) at which Devices in this group send information to the Poll Service via the MP Agent. You can also set polling to be in conjunction with the completion of each Workunit.

  The poll interval directly affects the reporting of Device status. For more information about Device status see “Devices” on page 51.
- Default Priority—The priority by which Jobs will run on this Device Group if the Job submitter has no other priority setting on the Device Group. The default priority must be between 0 and 100.

  NOTE The individual User or User Group priority always takes precedence over the default Device Group priority even if it is lower. See “Job Scheduling Priority” on page 56 for more information about the use of priority in scheduling.
- Max Workunit CPU Timeout—The maximum value any Job Step's wu_cpu_timeout field may have on this Device Group. Zero allows any timeout. The Max Workunit CPU Timeout must be less than or equal to the Max Workunit Clock Timeout.
- Max Workunit Clock Timeout—The maximum value any Job Step's wu_clock_timeout field may have on this Device Group. Zero allows any timeout.

- Default Device Profile GUID—The Device Profile which Devices with no other associated Device Profile will use.
- Agent Version GUID—The version of the MP Agent which Devices in this Device Group use.

The following attributes are assigned by the system:

- GUID—A unique identifier for each Device Group in the Grid MP platform. The MP Console does not display GUIDs unless the User chooses the Advanced view when logging on to the MP Agent.
- Creation Time—The time this Device Group was created.
- Last Modified Time—The timestamp when the Device Group record was last modified.

Device Group Credentials

The Device Group Credentials functionality allows you to specify a Unix username to be used to run Programs on all Devices within a Device Group. This is especially useful when running MPI programs, as users often stage input data in their home directories, and need to switch to a user account that has access to the home directory. In addition, in configurations where multiple users share one cluster, it helps them avoid overwriting each other's data by allowing them to use their own username to run programs. Device Group Credentials are currently supported on Unix-type operating systems only. See "Set Device Group Credential," on page 74 for instructions about setting Device Group Credentials.

Job Scheduling Priority

Device Group Managers can specify Job priority limits for each User or User Group that has permission to run Jobs on a Device Group. When a new Device Group is created, its initial default scheduling priority is a copy of the Default Device Group scheduling priority.

The MP Dispatch Service's scheduler manages scheduling work across the Device Group such that it honors the individual User or User Group priorities. If a User belongs to more than one User Group which has Job priorities specified for a Device Group, the scheduler assigns the highest of the assigned priorities to the Job.

The Job scheduling priority, along with Device Profiles, and Workunit time outs, allow Device Group Managers to control access and usage patterns for their Devices. The MP Console also provides an option to set the priority for a User or User Group to

"0 (No Access)". This is used to indicate that the specified User Group will not have access to run Jobs on the Device Group.

Device Profiles

Device Profiles are configured by Device Administrators and applied to Devices to control the maximum disk space Grid MP platform Workunits can utilize, the times of day a Device is available for work and polling, and the Programs and Applications it can run. Administrators can set up multiple Device Profiles per Device Group, but only one Device Profile can apply to each Device. When Devices are moved into the Device Group, they inherit the default Device Profile. Since only one Device Profile can apply to a Device, a Device cannot belong to more than one Device Group at a time.

Device Profile Properties

Device group and system administrators can edit the following attributes for a Device Profile:

- Device Profile Name—The unique name of the Device Group. The name is a required value and must not have leading or trailing spaces.
- Execution Schedule—For each hour of the week, starting at 00:00 on Monday and ending at 23:00 on Sunday, you can specify the hours Devices using this Device Profile are available to process Jobs.
- Communication Schedule—For each hour of the week, starting at 00:00 on Monday and ending at 23:00 on Sunday, you can specify the hours Devices using this Device Profile are available to communicate with the MP Services.
- Max Disk Space—The maximum number of megabytes the MP Agent is allowed to use on the associated Device. Only the partition on which the MP Agent resides is counted.
- Max Disk Percent—The percent of the total disk the MP Agent is allowed to use. Only the partition on which the MP Agent resides is counted.
- Min Free Disk Space—The minimum number of megabytes the MP Agent must leave free on the disk of the associated Device. Only the partition on which the MP Agent resides is counted.
- Min Free Disk Percent—The percent of the total disk the MP Agent must leave free. Only the partition on which the MP Agent resides is counted.

- Run New Applications—If this flag is true, new Applications can run on Devices utilizing the Device Profile.
- Run New Programs—If this flag is true, new Programs can run on Devices utilizing the Device Profile.
- Monitor User Activity—If this flag is set to true, the MP Agent will actively monitor user activity and potentially trigger Program suspension.
- Monitor CPU Max Percent—If non-zero, this specifies the threshold of CPU utilization by non-MP Agent processes at which Program suspension will potentially be triggered.
- Monitor Max Memory Utilization—If non-zero, then specifies the threshold for system-wide RAM utilization at which Program suspension will be potentially triggered.
- Monitor Disk Use—If this flag is true, the MP Agent should actively monitor disk utilization while Programs are running, otherwise only the disk cache utilization will be enforced while fetching Data files. When enabled and disk utilization has exceeded the configured limits, disk cache clearing will first be attempted, followed by Program abortion if disk usage is still too high.
- Monitor Page Rate—If non-zero, this specifies the system-wide disk paging rate (in pages/sec) threshold at which Program suspension will potentially be triggered.
- Keep Agent Priority—If true, the Agent will not run Programs at idle priority on the Device and will instead run the Program at the unaltered priority of the Agent process itself.

The following attributes are assigned by the system:

- Device Profile GUID—The primary unique identifier of this object.
- Device Group GUID—The Device Group to which this Device Profile belongs.
- Creation Time—The timestamp when the Device Profile was created.
- Last Modified Time—The timestamp when the Device Profile record was last modified.

Scheduling

The Dispatch Service includes a workload scheduler that sends Workunits to Devices using the Grid MP platform dispatch algorithm. The algorithm takes the following properties into account when scheduling a Job:

1. The following factors are taken into consideration to create a list of qualified Jobs:
   - Workunit Timeout—Job Creators can set the maximum amount of time a Workunit can take before it is aborted. Device Managers can also specify maximum Workunit timeouts for Device Groups. The workload scheduler will only send Jobs to Device Groups with a maximum Workunit timeout equal to or greater than the Job's maximum Workunit timeout.
   - Workload Thresholds—Job Managers can specify the following properties at the Job Step level to ensure Results are dependable:
     - Number of Results—The minimum number of Results a Workunit must have in order to be considered complete.
     - Maximum Number of Errors—The maximum number of Errors a Workunit can receive before it fails.
     - Maximum Concurrent Workunits Dispatched—The maximum number of times any one Workunit can be dispatched at once.
   - Resource Constraints—Application administrators set specific resource requirements at the Program level, such as the minimum free disk space, CPU clockrate, or physical RAM a Device must have to run the Program. Device Administrators specify maximum utilization thresholds for their Devices, which restricts which Jobs can run on the Devices.
   - Device Preferences—Device Administrators set the Application and Programs a Device or Device Group can run with a Device Profile.
   - Device Group Targeting—Job creators can target specific Device Groups for their Jobs. If a Job is targeted to Device Groups, it will only run on those Device Groups. If a Job has no targeted Device Groups, it can run on any Device Group that meets its resource constraints.
2. From the list of qualified Jobs, User scheduling priorities at the Device Group level are compared to stochastically select a User. This priority setting determines the service rate of all Jobs for a User or User Group as compared to other Users or User Groups submitting Jobs to the Device Group in question. Device Administrators set this priority level at the Device Group level.
3. From the qualified Jobs submitted by the selected User, Job priorities are compared to stochastically select a Job. This priority allows the Job creator to prioritize among their Jobs. Job creators set this priority level when creating a Job in the MP Console. Priority can also be set for mpsub and ud_mpirun Jobs.
4. Optimal Workunit Selection is applied to find the best Workunit for the selected Job. The scheduler attempts to give higher preference to a Workunit that uses a Data file the MP Agent on the Device has previously downloaded. This reduces

the amount of network traffic used when downloading the files for the Workunit, since the MP Agent may have cached some of them.

Using all these constraints a Job and its associated Workunits will be scheduled to run on the target set of Devices at the appropriate priority. Once a Job is running, a User with the necessary Privileges may alter various runtime parameters, such as the Job's priority, scheduled end time, timeouts, minimum Results and maximum Errors.

Workunit Rescheduling

Once scheduled, Workunits will automatically be rescheduled if any of the following conditions occur:

- The MP Agent determines that the Job Step's Workunit Clock Timeout or Workunit CPU Timeout have elapsed since the Workunit was received.
- The Workunit encounters any failure that returns an Error record.
- The Device running the Workunit becomes dormant. By default, Devices transition into dormant status after 10 hours of not communicating with the Poll Service. The Database Setting table controls this threshold. For more information about the Database Setting table, see "Database Setting Table" on page 27.
- The MP Agent suspends the Workunit for longer than the system allows. The Database Setting table controls how long a Workunit can be suspended. For more information about the Database Setting table, see "Database Setting Table" on page 27.

Device Monitoring

Device Monitoring functionality offers unobtrusiveness features to reduce the detectable impact upon a Device. The MP Agent monitors the following load parameters on Devices and suspends Workunit execution on a Device if any exceed threshold settings. Thresholds are set at the Device Profile level.

NOTE The MP Agent monitors resources at a configurable sampling frequency between one and 15 minute intervals. The interval is set in the database Settings table. For more information about this table, see "Database Setting Table," on page 27.

- Min Free Disk/Max Disk Utilization—The minimum number of megabytes the MP Agent must leave free on the disk of the associated Device and the maximum number of megabytes the MP Agent is allowed to use on the associated Device. Only the partition on which the MP Agent resides is counted.

- Min Free Disk Percent/Max Disk Percent—The percent of the total disk the MP Agent must leave free and the percent of the total disk the MP Agent is allowed to use. Only the partition on which the MP Agent resides is counted.
- Monitor User Activity—If this flag is set to true, the MP Agent will actively monitor user activity and potentially trigger Program suspension.
- Monitor CPU Max Percent—If non-zero, this specifies the threshold of CPU utilization by non-MP Agent processes at which Program suspension will potentially be triggered.
- Monitor Max Memory Utilization—If non-zero, this number is the threshold for system-wide RAM utilization at which Program suspension will be potentially triggered.
- Monitor Disk Use—If this flag is true, the MP Agent should actively monitor disk utilization while Programs are running, otherwise only the disk cache utilization will be enforced while fetching Data files. When enabled and disk utilization has exceeded the configured limits, disk cache clearing will first be attempted, followed by Program abortion if disk usage is still too high.
- Monitor Page Rate—If non-zero, this specifies the system-wide disk paging rate (in pages/sec) threshold at which Program suspension will potentially be triggered.

Device Actions

The following section describes commonly performed Device-related tasks you can perform in the MP Console. Each task section explains how to navigate through the necessary screens to perform the task and provides tips for using the screen or screens involved. For detailed MP Console field and screen element descriptions, see the online help by clicking the **Help** link from any page in the MP Console.

View Devices

Basic information about Devices is available in a Device dashboard format. You can view all Devices or just the Devices that belong to a specific Device Group.

Where to Start

1. Log on to the MP Console.
2. To display all Devices, click **Manage all Devices** from the Grid MP platform homepage. The system displays a list of all the Devices. The system defaults to display 20 Devices per screen. You can adjust the number of records per page.

3. To display only the Devices in a specific Device Group, click Start > Platform > Devices. The system displays the Device Groups screen.
4. Click the Device Group name to display the Device Group details screen.

> **NOTE** If you cannot easily locate the Device Group in a list, use the Filter Options form to search for it by name.

5. From the Device Group details screen, click **View Devices.** The system displays the Devices screen.

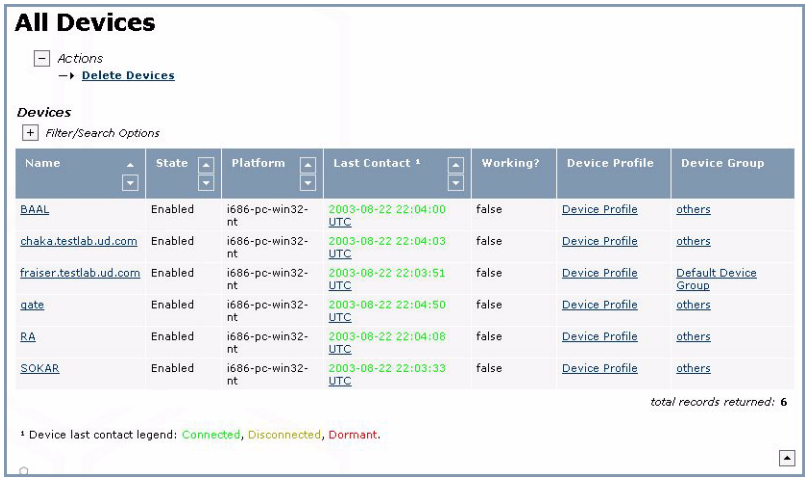


Figure 6. All Devices Screen

Using the Screen

- Click **Move Devices** to navigate to a form you can use to move multiple Devices to a new Device Group and Device Profile.
- The Last Contact column utilizes color-coding to make it easier to spot disconnected and dormant Devices.

View Device Details

More detailed information about a Device, such as Device resources and configuration information, is available from the Device Details screen.

Where to Start

1. Log on to the MP Console.
2. Follow the instructions under "View Devices" on page 61 to list either all Devices in the system or for a specific Device Group.

3. Click the name of the Device for which you want to display more information. The system displays the Device details screen.

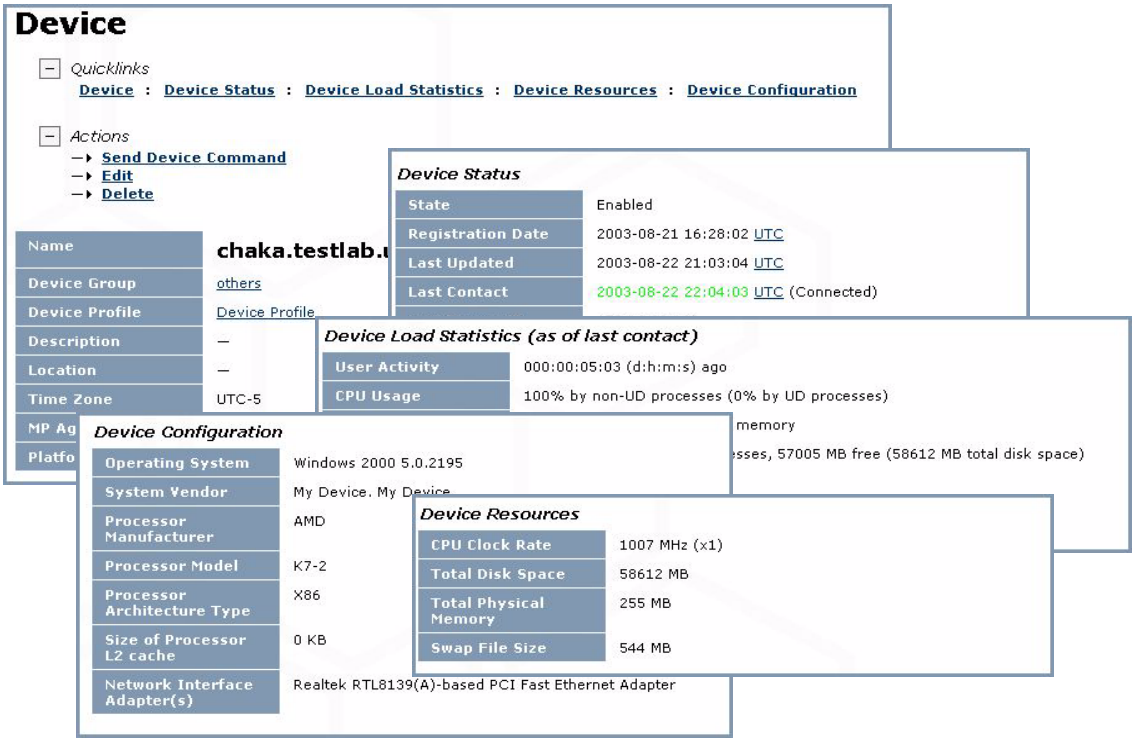


Figure 7. Device Details Screen

Using the Screen

- The screen is split into four sections: Device details, Device Status, Device Resources, and Device Configuration. Click one of the Quicklinks to navigate within the Device details screen.

- If the Device is currently running a Job, the Job and Workunit information display in the Device Status section.

Edit a Device

From the Edit Device screen, you can change settings including the Device Profile, which alters what kind of Jobs a Device can run and when it can run them, the

MP Agent version, and the Device state, which controls whether or not new Workunit can be dispatched to the Device.

NOTE If you change a Device's name from the default, it will no longer match the Device hostname. If you have Device recycling turned on, and you attempt to re-register the Device, recycling will not occur because the database will not be able to match the hostname and Device name. This will result in the Device receiving a new Device record at re-registration.

Where to Start

1. Log on to the MP Console.
2. Follow the instructions under "View Devices" on page 61 to list either all Devices in the system or for a specific Device Group.
3. Click the name of the Device for which you want to display more information. The system displays the Device details screen.
4. Click **Edit** to display the Edit Device screen.

Using the Screen

- Click the Device Group name to display the Device Group details screen.
- Click **Update** to save your changes.
- Click **Reset** to return the form to the last saved values. Click **Cancel** to return to the Device details screen.

Delete Device

Devices register with the database when they connect via the MP Agent. Once a Device is visible in the MP Console, you can delete it from the Delete Device screen.

NOTE You can delete multiple Devices at once by clicking the **Delete Devices** link from the All Devices screen.

Where to Start

1. Log on to the MP Console.
2. Follow the instructions under "View Devices" on page 61 to list either all Devices in the system or for a specific Device Group.

3. Click the name of the Device you want to delete. The system displays the Device details screen.
4. Click Delete. The system displays the Delete Device screen.

Using the Screen

- Click the Device name or Device Group name to return to the corresponding details screens without deleting the Device.
- Click **Cancel** to return to the Device details screen without deleting the Device.

Move Device to New Device Group

A Device can belong to only one Device Group. The Device Group controls Device operation and Job scheduling parameters such as the MP Agent version a Device uses, how often the Poll Service collects data from the Device, and the maximum amount of time a Job Step can run on the Device. To move a Device or multiple Devices from one group to another, use the Move Devices function.

Where to Start

1. Log on to the MP Console.
2. Follow the instructions under "View Devices" on page 61 to list Devices in the system for a specific Device Group.
3. From the Devices screen, click **Move Devices**. The system displays Step 1 of the Move Devices process.
4. Specify whether you want to move all Devices in the Device Group or individual Devices.
5. Click **Next** to display Step 2.
6. Select a new Device Profile only, or a Device Group and Device Profile combination. Click **Move** to save your changes.

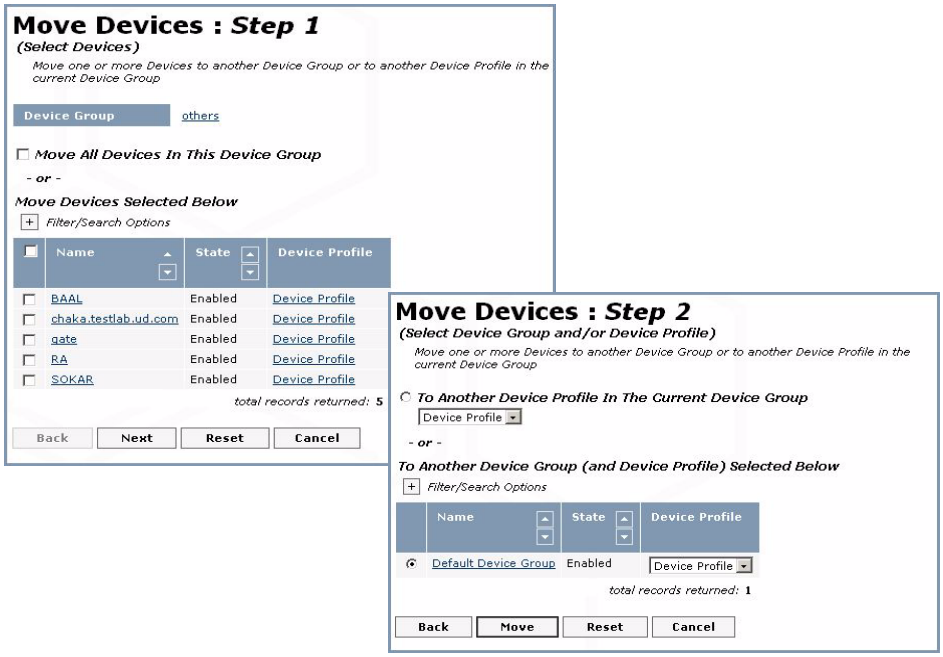


Figure 8. Move Devices Screens

Using the Screen

- In the list of Device Groups, click a Device Group name to navigate to the Device Group details screen.
- Use the **Back** and **Next** buttons to move between Step 1 and Step 2 of the Move Devices process.
- Click **Cancel** to return to the Devices screen.

Send Device Commands

The Device Commands screen allows you to send commands, such as Snooze, or Abort Workunit, to a specific Device, a Device Group, or a list of Devices.

Where to Start

1. Log on to the MP Console.
2. Since the Send Device Commands screen is accessible in multiple places, use one of the following paths to get to it:
   - Follow the instructions in "View Devices" on page 61 or to list all Devices.

- Follow the instructions in "View Device Details" on page 62 to display one Device.
- Follow the instructions in "Device Groups Screen" on page 69 to display a Device Group.

3. From one of the screens described in Step 2, click **Send Device Commands**.

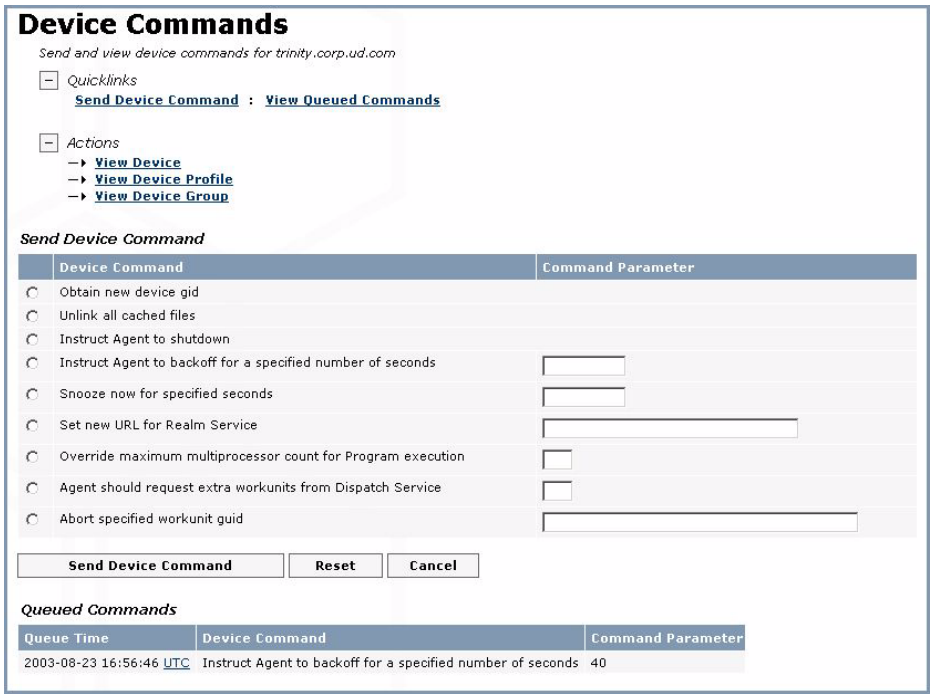


Figure 9. Device Commands Screen

Using the Screen

- Select one of the commands and, if necessary, provide the requested parameter for the command, such as the number of seconds to snooze the Device.

- The following commands can be sent to a Device or a group of Devices:
  - Obtain new Device GID—This can be useful for troubleshooting or in an attempt to correct abnormal MP Agent behavior.
  - Unlink all cached files—Cached files impact scheduling due to data affinity and may promote unexpected behavior when one is trying to diagnose Workunit scheduling.
  - Instruct Agent to shutdown—The MP Agent on the Device is shutdown for the number of seconds specified.
  - Instruct Agent to backoff for a specified number of seconds—Backing off a Device continues computation, but not network communication.
  - Snooze now for specified seconds—Snoozing halts computation and network communication.

  - Sets new URL for Realm Service—This command aids the migration to (or establishment of) a new Realm Service and is just one of the steps in the sequence that must be performed. For United Devices Professional Services use only.
  - Override maximum multiprocessor count for Program execution—By default, the MP Agent will attempt to use up to the number of processors available on the Device. This option lets you force the MP Agent to use fewer processors than what it has detected. This may be necessary if a deployment is running an Application that is known to cause problems if multiple instances of it are run at the same time on a single machine.
  - Agent should request extra Workunits from Dispatch Service—For United Devices Professional Services use only.

- Commands sent to Devices but not yet executed display in the Queued Commands list.

Device Group Actions

View Device Groups

Basic information about Device Groups is available in a dashboard format. You can easily see the status of Devices in the groups, as well as each group's combined memory.

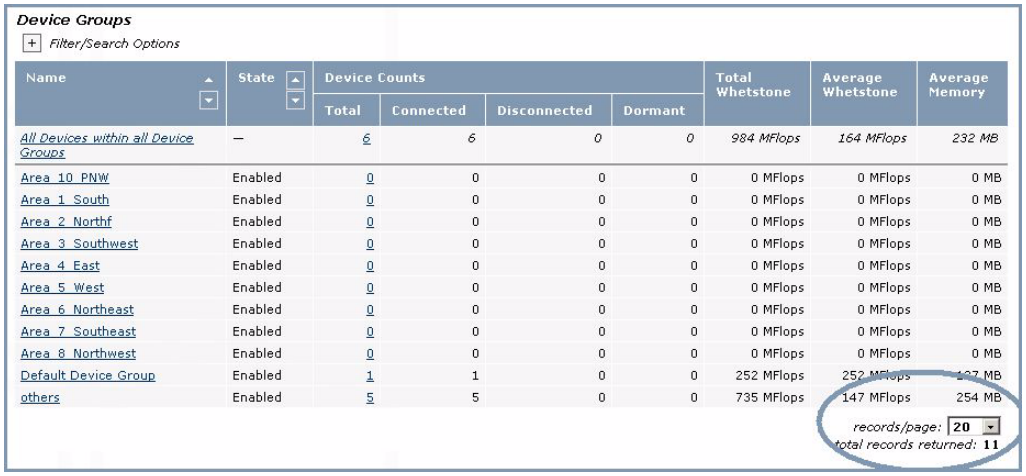
Where to Start

1. Log on to the MP Console.
2. Click **Manage Device Groups** from the Grid MP platform homepage. The system displays a list of all the Device Groups. The system defaults to display 20 Devices per screen. You can adjust the number of records per page.

Using the Screen

- Click a Device Group name to display the Device Group details screen.
- Click **All Devices within All Device Groups** to display a list of every Device in the Grid MP platform.
- Click **Create Device Group** to add a new group to the Grid MP platform.

- The Device Counts columns display the number of Devices in each group that are currently connected, disconnected, or dormant.



Device Groups

Filter/Search Options

Name	State	Device Counts				Total Whetstone	Average Whetstone	Average Memory
		Total	Connected	Disconnected	Dormant			
All Devices within all Device Groups	—	*6*	*6*	*0*	*0*	*984 MFlops*	*164 MFlops*	*232 MB*
Area_10_PNW	Enabled	0	0	0	0	0 MFlops	0 MFlops	0 MB
Area_1_South	Enabled	0	0	0	0	0 MFlops	0 MFlops	0 MB
Area_2_Northf	Enabled	0	0	0	0	0 MFlops	0 MFlops	0 MB
Area_3_Southwest	Enabled	0	0	0	0	0 MFlops	0 MFlops	0 MB
Area_4_East	Enabled	0	0	0	0	0 MFlops	0 MFlops	0 MB
Area_5_West	Enabled	0	0	0	0	0 MFlops	0 MFlops	0 MB
Area_6_Northeast	Enabled	0	0	0	0	0 MFlops	0 MFlops	0 MB
Area_7_Southeast	Enabled	0	0	0	0	0 MFlops	0 MFlops	0 MB
Area_8_Northwest	Enabled	0	0	0	0	0 MFlops	0 MFlops	0 MB
Default Device Group	Enabled	1	1	0	0	252 MFlops	252 MFlops	127 MB
others	Enabled	5	5	0	0	735 MFlops	147 MFlops	254 MB

records/page: 20
total records returned: 11

Figure 10. Device Groups Screen

View Device Group Details

Device group details include Device operation and Job scheduling parameters such as the MP Agent version a Device uses, how often the Poll Service collects data from the Device, and the maximum amount of time a Job Step can run on the Device. From the Device Group details screen, you can also link to screens that control the priority level for Jobs submitted to the Device as well as Device Profile screens.

Where to Start

1. Log on to the MP Console.
2. Click **Manage Device Groups** from the Grid MP platform homepage. The system displays a list of all the Device Groups.
3. Click the name of the Device Group for which you want to view more details. The system displays the Device Group details screen.

Using the Screen

- The screen is split into three sections: Device Group details, Device Operation, and Job Scheduling. Click one of the Quicklinks to navigate within the Device Group details screen.

- Click one of the **Manage Privilege** links to display a screen you can use to grant Users or User Groups the specified Privilege (Read, Update, or Delete) for the Device Group. See "Grant and Revoke Privileges" on page 104 for more information about how you can grant Privileges.

- Click **Manage Job Scheduling** to display a screen you can use to assign default priorities for Jobs created by specific Users or User Groups.

Create Device Group

You cannot create Devices. Instead, Devices are automatically added to the Grid MP platform when they register via the MP Agent. The system creates a default Device Group during installation and adds all Devices to it. MP Administrators and Device Group Managers can create new Device Groups and move Devices between them in the MP Console.

Where to Start

1. Log on to the MP Console.
2. Click **Manage Device Groups** from the Grid MP platform homepage. The system displays a list of all the Device Groups.
3. Click **Create Device Group**. The system displays the Create Device Group screen.

Using the Screen

- You must provide a Device Group name. You can provide values for the other attributes or accept the defaults.
- Click **Create** to save the new Device Group.
- You can provide a polling interval or specify that the Poll Service should only collect data when Workunits complete.
- The Maximum Workunit CPU Timeout must be less than or equal to the Maximum Workunit CPU Timeout.

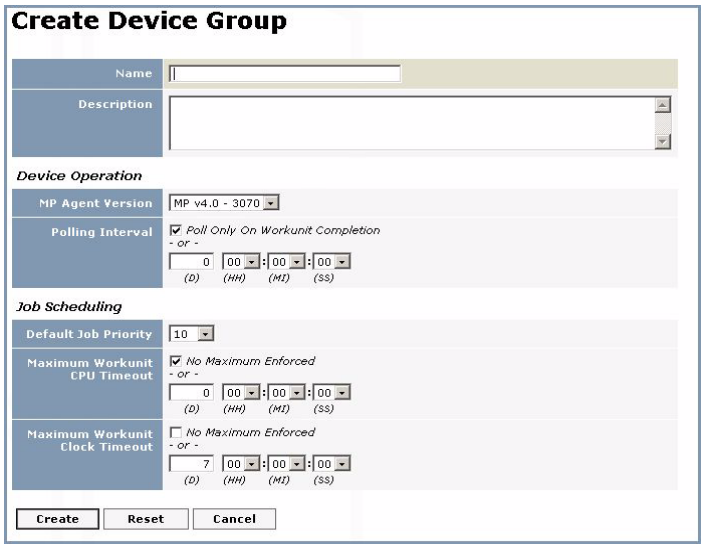


Figure 11. Create Device Group Screen

Edit Device Group

From the Edit Device Group screen, you can change the following crucial parameters for scheduling and reporting:

- Poll Period—The amount of time between connections with the Poll Service. This controls the connection status for a Device and the rescheduling of Workunits.
- Default Job Priority—The priority by which Jobs will run on the Device Group if the Job submitter has no other priority setting on the Device Group.
- Maximum Workunit Timeouts—The maximum amount of clock or CPU time allowed for any Job Step to run on Devices in this Device Group. If the Workunit timeout settings for a Job Step exceed the setting for the Device Group, the Job Step will not be dispatched to Devices in this group. If the actual amount of time a Job Step takes to complete exceeds this value, it will be rescheduled.

You can also change the Device Group state. If you disable the Device Group, all Devices within the group become disabled as well. The Dispatch Service does not send Workunits to disabled Devices.

Where to Start

1. Log on to the MP Console.
2. Click **Manage Device Groups** from the Grid MP platform homepage. The system displays a list of all the Device Groups.

3. Click the name of the Device Group you want to edit. The system displays the Edit Device Group screen.
4. Change information as desired and click **Update** to save changes.

Using the Screen

- Click **Reset** to return the form to the last saved values.
- The Maximum Workunit CPU Timeout must be less than or equal to the Maximum Workunit CPU Timeout.

Delete Device Group

Deleting a Device Group automatically deletes any Device Profiles that belong to the group. The delete function will fail if any Devices refer to the Device Group.

NOTE You cannot delete the default Device Group. The system automatically adds all newly registered Devices to the default group.

Where to Start

1. Log on to the MP Console.
2. Click **Manage Device Groups** from the Grid MP platform homepage. The system displays a list of all the Device Groups.
3. Click the name of the Device Group you want to delete. The system displays the Device Group details screen.
4. Click **Delete**. The system displays the Delete Device Group screen.
5. Click **Delete**. The system displays a confirmation window.
6. Click **OK** to complete the delete action.

Using the Screen.

- Click **Cancel** to return to the Device Group details screen without deleting the Device.

Assign Priority to Jobs from Users or User Groups

When you create a Device Group, you assign a default priority to it. This priority is assigned to all Jobs created by Users and User Groups to which you have not assigned a User- or User-Group-specific priority. To assign a different priority to specific Users

or User Groups, use the Manage Job Scheduling screens in the MP Console. For more information about priority and scheduling, see “Scheduling” on page 59.

You can assign priority to an individual User or to a User Group. If you assign a priority to a User Group, all Users within the group inherit the priority.

Where to Start

1. Log on to the MP Console.
2. Click **Manage Device Groups** from the Grid MP platform homepage. The system displays a list of all the Device Groups.
3. Click the name of the Device Group for which you want to assign priority. The system displays the Device Group details screen.
4. Click **Manage Job Scheduling**. The system displays the Manage Job Scheduling for Device Group screen.

NOTE	The following instructions describe how to assign priority to individual Users. Follow the on-line help for the Manage Job Scheduling for Device Group screen to assign priority to a User Group.

5. From the Manage Job Scheduling for Device Group screen, click **Manage Users**. The system displays the Manage Job Scheduling for Device Group (Users) screen, which contains a list of the Users who have already been assigned a priority for the Device Group.
6. Click **Add Users**. The system displays the Add Users screen, which contains a list of all the Users in the Grid MP platform.

Using the Screen.

- Select the checkbox corresponding to the User(s) you want to assign a priority and choose a priority from the drop-down list box.
- Click **Add Selected** to save your changes.
- Click **Reset** to return the form to the last saved values.
- Click the User name to see the User details screen, which contains a list of the Role assignments the User has.

Set Device Group Credential

The Device Group Credentials functionality allows you to specify a Unix username to be used to run Programs on all Devices within a Device Group. For more information about setting Credentials, see “Device Group Credentials,” on page 56.

Where to Start

1. Log on to the MP Console.
2. Click **Manage Device Groups** from the Grid MP platform homepage. The system displays a list of all the Device Groups.
3. Click the name of the Device Group for which you want to create Device Group Credentials. The system displays the Device Group details screen.
4. Click **Manage Job Scheduling**. The system displays the Manage Job Scheduling for Device Group screen.
5. From the Manage Job Scheduling for Device Group screen, click **Manage Users**. The system displays the Manage Job Scheduling for Device Group (Users) screen, which contains a list of the Users who have already been assigned a priority for the Device Group.
6. Click **Add Users**. The system displays the Add Users screen, which contains a list of all the Users in the Grid MP platform.

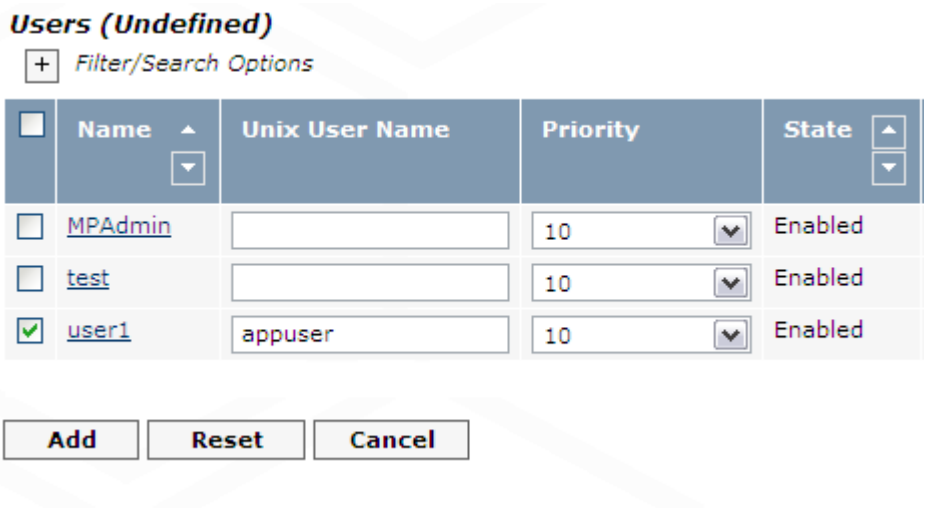


Figure 12. Add Users Screen - Create Device Group Credentials

Using the Screen

- Type the Unix user name you want to associate with one of the Grid MP Users listed.

- Click **Add** to save the Device Group Credential. From this point on, all Jobs submitted by the User will run under the Unix user name you supplied.

- To remove a Device Group Credential, follow steps 1-5 above to navigate to the Manage Users screen, which displays existing Credential relationships. Remove the Unix user name corresponding to the MP User you want to return to default and click **Update**.

View Device Profiles

Device Profiles belong to a Device Group and cannot be shared across groups. The list of Device Profiles displays the number of Devices within the group that utilize the Device Profile.

Where to Start

1. Log on to the MP Console.
2. Click **Manage Device Groups** from the Grid MP platform homepage. The system displays a list of all the Device Groups. The system defaults to display 20 groups per screen. You can adjust the number of records per page.
3. Click the Device Group for which you want to view Device Profiles. The system displays the Device Group details screen.
4. Click **View Device Profiles** to display the Device Profiles screen.

Using the Screen

- Click a Device Profile name to display the Device Profile details screen.

- Click **Create Device Profile** to add a new profile to the Grid MP platform.

View Device Profile Details

Device Profile details include Device operation and Job scheduling parameters such as the times of day the Devices using the Device Profile are available for Jobs and polling and the specific Applications and Programs the Devices will accept.

Where to Start

1. Log on to the MP Console.
2. Click **Manage Device Groups** from the Grid MP platform homepage. The system displays a list of all the Device Groups. The system defaults to display 20 groups per screen. You can adjust the number of records per page.

3. Click the Device Group for which you want to view Device Profiles. The system displays the Device Group details screen.
4. Click **View Device Profiles** to display the Device Profiles screen.
5. Click the name of the Device Profile for which you want to view details. The system displays the Device Profile details screen.

Using the Screen

- The screen is split into five sections: Device Profile details, Device Operation, Device Load Thresholds, Application Execution, and Program Execution. Click one of the Quicklinks to navigate within the Device Profile details screen.
- Click **Edit** to make changes to the Device Profile.

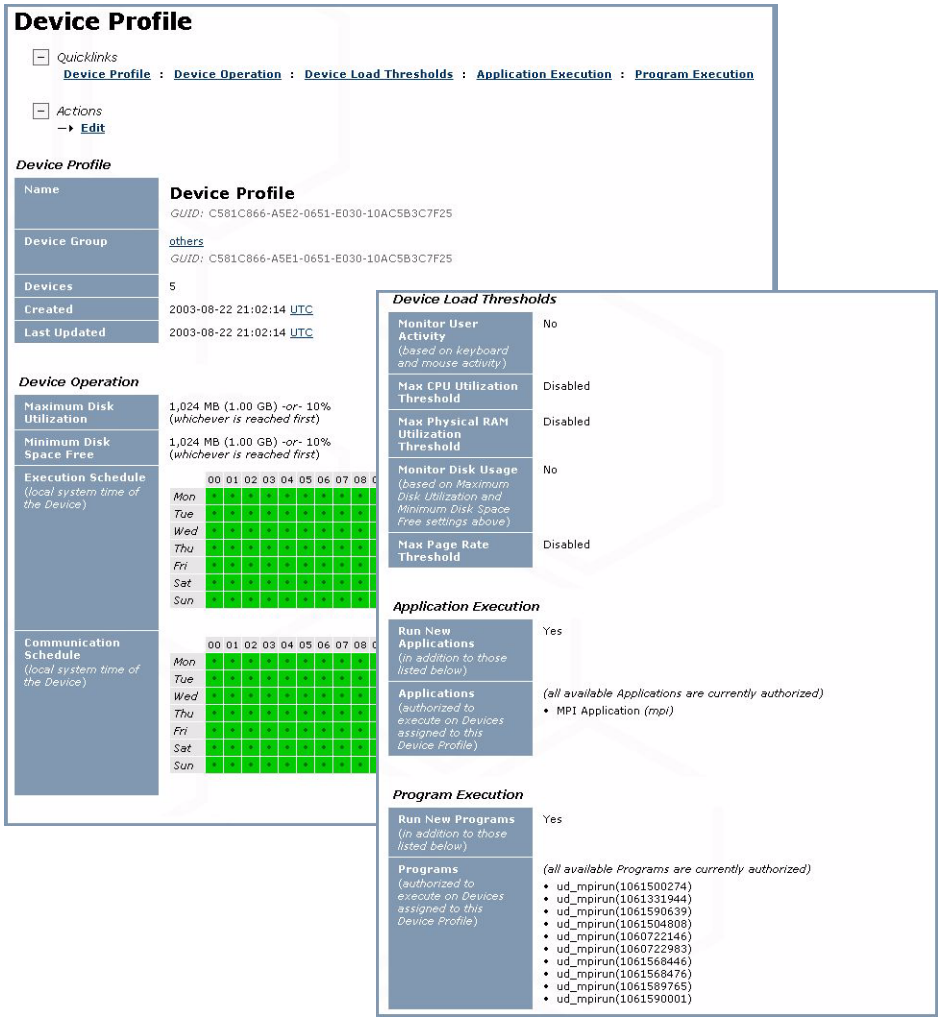


Figure 13. The Device Profile Screen

Create Device Profile

Each Device can belong to only one Device Group and use only one Device Profile. The system automatically assigns newly registered Devices to the default Device Group and Device Profile. You can create new Device Profiles and assign them to existing Devices and Device Groups.

Where to Start

1. Log on to the MP Console.
2. Click **Manage Device Groups** from the Grid MP platform homepage. The system displays a list of all the Device Groups. The system defaults to display 20 groups per screen. You can adjust the number of records per page.
3. Click the Device Group for which you want to create a new Device Profile. The system displays the Device Group details screen.
4. Click **View Device Profiles** to display the Device Profiles screen.
5. Click **Create Device Profile**. The system displays the Create Device Profile screen.
6. You must provide a Device Profile name. You can provide values for the other attributes or accept the defaults.
7. Click **Create** to save the new Device Profile.

Using the Screen

- You can select or clear a row or column in the Execution Schedule and Communication Schedule by clicking the row or column header. Checked boxes represent active times for running Jobs or communicating with the Grid MP platform.

- If you select “No” for Run New Programs (and/or Applications), you must specify which Programs (or Applications) are authorized to run.

Edit Device Profile

From the Edit Device Profile screen, you can change the times of day Devices can and cannot be utilized to run Jobs, the Applications and Programs the Device is authorized to run, and the maximum amount of disk space Jobs can use.

Where to Start

1. Log on to the MP Console.
2. Click **Manage Device Groups** from the Grid MP platform homepage. The system displays a list of all the Device Groups. The system defaults to display 20 groups per screen. You can adjust the number of records per page.
3. Click the Device Group that utilizes the Device Profile you want to edit. The system displays the Device Group details screen.
4. Click **View Device Profiles** to display the Device Profiles screen.The system displays a list of all the Device Profiles.
5. Click the name of the Device Profile you want to edit. The system displays the Edit Device Profile screen.
6. Change information as desired and click **Update** to save changes.

Using the Screen

- Click **Reset** to return the form to the last saved values.
- You can select or clear a row or column in the Execution Schedule and Communication Schedule by clicking the row or column header. Checked boxes represent active times for running Jobs or communicating with the Grid MP platform.
- If you select “No” for Run New Programs (and/or Applications), you must specify which Programs (or Applications) are authorized to run.

Delete Device Profile

The delete function will fail if any Devices refer to the Device Profile.

NOTE	You cannot delete the default Device Profile. The system automatically assigns all newly registered Devices to the default Device Profile.

Where to Start

1. Log on to the MP Console.
2. Click **Manage Device Groups** from the Grid MP platform homepage. The system displays a list of all the Device Groups. The system defaults to display 20 groups per screen. You can adjust the number of records per page.
3. Click the Device Group that utilizes the Device Profile you want to delete. The system displays the Device Group details screen.

4. Click **View Device Profiles** to display the Device Profiles screen.The system displays a list of all the Device Profiles.
5. Click the name of the Device Profile you want to delete. The system displays the Device Profile details screen.
6. Click **Delete**. The system displays the Delete Device Profile screen.
7. Click **Delete**. The system displays a confirmation window.
8. Click **OK** to complete the delete action.

Using the Screen

- Click **Cancel** to return to the Device Profile details screen without deleting the Device.
- Click the Device Profile or Device Group name to return to the corresponding details screen without deleting.

Chapter 6: Managing Access Control

Introduction to Access Control

The Grid MP platform utilizes Users and User Groups to manage the people who access the system, and Roles and Privileges to manage what the Users and User Groups can do with the Grid MP platform.

You create User accounts to allow people to log on to the system with a username and password. You can then assign Users to predefined User Groups that have been assigned predefined Roles. User groups make managing multiple Users who perform similar functions easier.

Getting Started with Access Control

This section provides you with the information necessary to quickly enable Users to log on to the Grid MP platform by utilizing the MP Console to create User accounts and assign them to predefined User Groups.

See "Advanced Access Control Options" on page 84 for more information about access control components.

Users

The first step in providing access control in the Grid MP platform is to create a User account. Once a User account is created, Users can log on to the MP Console. Roles are required for most additional access to objects in the system.

See "Create a New User" on page 92 for step-by-step instructions for creating a User account.

NOTE During the installation process, you are required to create a User with no Roles or Privileges for the MP Agent to use to connect with the Grid MP platform, prior to installing the MP Agent.

User Object Attributes

System administrators can edit the following attributes for a User. Users can also edit their own profiles.

- User Name—The unique User name. The User name is required and must have no leading or trailing spaces.
- Password—The User password. Password must be at least 6 characters in length and contain both letters and numbers.
- State—The state of the User object. Valid states:
  - Disabled—The User is not allowed to log on to the system.
  - Enabled—The User is allowed to log on to the system.
- Email Address—The email address for the User
- Real Name—The name of the User
- Postal Address—The postal address of the User
- Telephone—The telephone number of the User
- Organization—The organization to which this User belongs
- Personal Information—Personal information about the User

The following attributes are assigned by the system:

- User GUID—The primary unique identifier of the User object
- Created Time—The timestamp when the User was created
- Last Modified—The timestamp when this record was last modified

User Groups

To make managing multiple Users who perform similar functions easier, you can add Users to User Groups. User groups allow you to apply Roles and Privileges to a group of Users. Users can belong to zero or more groups.

Predefined User Groups

You can assign Users to any of the following preconfigured default User Groups.

See "Add User to User Group" on page 100 for help adding an existing User to a predefined User Group.

- MP Administrators—The MP Administrators User Group has the MP Administrator Role, which allows Users in the group to do anything in the Grid MP platform without restriction. This group is best for system administrators.

- Application Administrators—Application Administrators can create, view, update, and delete all Applications, Programs, and Jobs, and can view all Device Groups. This group is best for Users who will port Applications and upload them into the system, as well as manage Jobs.

- Application Users—Application Users can create and view all Jobs and Job-specific information, and view all Applications, Programs, and Device Groups. This User Group is best for Users who will create and submit Jobs, but who do not need to create or edit Applications or global Data Sets.

- Device Administrators—Device Administrators can view, create, edit, and delete all Device Groups, view all Applications and Programs, and create and manage all resources. This group is best for Users who manage a group of Devices but who do not need to create Applications, Programs, or Jobs.

- Everyone—The Everyone group automatically contains every User added to the Grid MP platform. By default, the Everyone group is not granted any Privileges on newly created objects. However, the administrator may assign additional default Privileges to the Everyone group. For example, it might be useful to assign Read Application and Read Job to the Everyone group. In this way, all Users will be able to view all Jobs in the system.

NOTE User group access control affects ALL objects of a class. For example, Application Administrators can create, view, update, and delete ALL Applications. Device Administrators can view, create, and delete ALL Device Groups. To grant Users or User Groups access to specific objects, you utilize Roles and Privileges. For more information, see "Advanced Access Control Options," on page 84.

User Group Object Attributes

System administrators can edit the following attributes for a User Group:

- User Group Name—The unique User Group name. The User Group name is required and must have no leading or trailing spaces.

- State—The state of the User Group object. Valid states:

  - Disabled—Users cannot access Roles and Privileges granted to them through this User Group.
  - Enabled—Users cannot access Roles and Privileges granted to them through this User Group

- Description—A short description of the User Group object.
- Annotation—A longer free-form annotation of the User Group object.

The following attributes are assigned by the system:

- User Group GUID—The primary unique identifier of the User object.
- Created Time—The timestamp when the User record was created.
- Last Modified—The timestamp when the record was last modified.

Advanced Access Control Options

Users and predefined User Groups provide a mechanism for System Administrators to quickly get started with access control in the Grid MP platform. Privileges and Roles are the more advanced components of access control and provide you with more versatility.

NOTE To create special User Groups, or change Privileges and Roles for default User Groups, contact United Devices Professional Services.

Privileges

The core of the Grid MP access control model is based on relationships called Privileges. Privileges connect Users with a specific object at a specific access level. For each object, the system contains a list of Users and the Privileges they hold on the object.

Table 5: Test Lab Device Group

User or User Group	Privilege
Alice	Read Device Group
Alice	Update Device Group
Bob	Read Device Group
Device Group Administrators	Read Device Group
Device Group Administrators	Update Device Group

Table 5: Test Lab Device Group

Device Group Administrators	Delete Device Group

In the example above, the User Alice can both read and update the Test Lab Device Group, and Bob can only read it. Members of the Device Group Administrators User Group, however, can read, update, and delete the Device Group.

For every operation that affects an object, the system will check to make sure that the calling User is permitted to perform the operation. If the User does not have the requested Privilege, an Error is returned to the User.

The following Privileges exist in the Grid MP platform:

Table 6: Grid MP Privileges

Privilege Name	Object Type	Description
Read Application	Application	Users who hold this Privilege on an Application may view the Application.
Update Application	Application	Users who hold this Privilege on an Application may change the Application. Users who have this Privilege should also hold the Read Application Privilege.
Delete Application	Application	Users who hold this Privilege on an Application may delete the Application.
Create Job	Application	Users who hold this Privilege on an Application may create a new Job using the Application.
Read Program	Program	Users who hold this Privilege on a Program may view the Program.
Update Program	Program	Users who hold this Privilege on a Program may change the Program. Users who have this Privilege should also hold the Read Program Privilege.
Delete Program	Program	Users who hold this Privilege on a Program may delete the Program.
Read Job	Job	Users who hold this Privilege on a Job may view the Job.
Update Job	Job	Users who hold this Privilege on a Job may change the Job. Users who have this Privilege should also hold the Read Job Privilege.
Delete Job	Job	Users who hold this Privilege on a Job may delete the Job.
Read Device Group	Device Group	Users who hold this Privilege on a Device Group may view the Device Group.
Update Device Group	Device Group	Users who hold this Privilege on a Device Group may change the Device Group. Users who have this Privilege should also hold the Read Device Group Privilege.
Delete Device Group	Device Group	Users who hold this Privilege on a Job may delete the Device Group.

Table 6: Grid MP Privileges

Privilege Name	Object Type	Description
Read Data	DataSet	Users who hold this Privilege on a Data Set may view the Data Set or use it in a Job.
Update Data	DataSet	Users who hold this Privilege on a Data Set may change the Data Set. Users who have this Privilege should also hold the Read Data Privilege.
Delete Data	DataSet	Users who hold this Privilege on a Job may delete the Data Set.
Manage Resource	Resource, GlobalResource	Users who hold this Privilege on a resource may read, change, or delete the resource.

When a Privilege is assigned to a user group for an object type, the group has that privilege for all newly created objects of that type in the system. To specify a privilege for a single object, such as a specific application, you can assign the privilege directly to a user. In addition, users who create objects can grant other users privileges on the objects, as well as permission to grant privileges themselves.

Viewing List of Privileges

You can view the list of privileges that Users and User Groups have on an object by running a command-line script named dumpsec.pl. When run, dumpsec.pl lists all the privileges that Users and User Groups have on a specific object in the Grid. This is a convenient utility when you are trying to set the security ACLs for a certain object.

dumpsec.pl is located in the sdk in /mgsi/perl/ directory and the pared versions are in:

- **For Windows**—/mgsi/win32/dumpsec.exe
- **For Linux**—/mgsi/i686-pc-linux-gnu/dumpsec_i686-pc-linux-gnu

Using the dumpsec.pl script

- In order to successfully run the dumpsec.pl script a uduserconf file must reside in the home directory.

  For information about uduserconf, refer to “uduserconf File” on page 28.

- It takes object GUID or name as parameter. If name is passed, it takes it as a substring and tries to match it with every object. You can then select the object for which you want to view the privileges of.

For example,

```
D:\UDShared\SDK3508\UDsdk_v4.2\mgsi\perl>dumpsec.pl hmm
Your request "hmm" matches the following multiple objects:

hmmer_test41 (data_set, CEDB6686-99D1-11D8-8675-
4C0010071B38)
hmmer_test4 (job, E96239AC-99C8-11D8-8675-4C0010071B38)
hmmer_test4 (job, F44A66E4-99D4-11D8-8675-4C0010071B38)
hmmerapphmmsrch (program, 0BFC1108-99C0-11D8-81AE-
4C0010071B38)
```

- It then returns the properties of the specified object, such as its name, guid, usergroups having privileges on the object, users associated to it and also specifies which administrator can grant privileges (Grantable Yes/No).

- dumpsec.pl works only for the following objects:-
  - agent_version
  - application
  - data_set
  - device_group
  - job
  - program
  - resource
  - global_resource

- It uses the MGSI_XMLRPC_URL. Specify the MGSI_XMLRPC_URL in the uduserconf file.

Usage

On Linux: **`$ ./dumpsec.pl`** *object* **`...`**

On Windows: **`dumpsec.pl`** *object* **`...`**

Where

- **`dumpsec.pl`** is the dumpsec script.

  You can also use the following pared versions to run dumpsec. These executables do not require a perl environment.

  - **`dumpsec.exe`**—For Windows

– **`dumpsec_i686-pc-linux-gnu`**—For Linux

> **NOTE** The platform-specific utility binary versions may not work on some AIX or Solaris computers. If the PAR executables do not work, run the Perl (*.pl) version of the script. Before running the perl version of the script, ensure that the dependent Perl CPAN modules are installed on the machine where you plan to run the script.

- *object* can be a guid or any object name regular expression.

The following output is an example of running dumpsec.pl to display the list of privileges for an object:

```
D:\UDShared\SDK3508\UDsdk_v4.2\mgsi\perl>dumpsec.pl  2A854A46-
99C4-11D8-81AE-4C0

010071B38

Object 2A854A46-99C4-11D8-81AE-4C0010071B38:

  Type: data_set

  Name: HMMER_WIN


Name                        | Privilege   | Grantable

----------------------------+-------------+----------

Application Administrators | Read Data   | no

Application Administrators | Update Data | no

Application Administrators | Delete Data | no

Application Users          | Read Data   | no

MPAdmin                    | Read Data   | yes

MPAdmin                    | Update Data | yes

MPAdmin                    | Delete Data | yes
```

Roles

Roles enable Users to create a class of objects. When a User with an appropriate Creator Role creates a new object, the User is automatically assigned all applicable Privileges on that object.

The following Roles exist in the Grid MP platform:

- MP Administrator—Manages and maintains all aspects of the Grid MP platform. Has access to all MP Console screens and MGSI calls.
- Application Creator—Allows a User to create Applications.
- Program Creator—Allows a User to create Programs.
- Device Group Creator—Allows a User to create Device Groups.
- Data Creator—Allows the User to create Data Sets and Data in the Grid MP platform.
- Resource Creator—Users who hold this Role may create new Resource and GlobalResource objects. In order to assign a Resource to a Program (via a ResourceRequirement) or a Device (via a ResourceAvailable), the User must then have Update Program or Update Device Group, respectively.

Creating and Editing User Groups

"Getting Started with Access Control," on page 81 briefly discusses the five predefined User Groups. Many deployments of the Grid MP platform can successfully use only the predefined User Groups. If the User Groups do not meet your needs, however, contact United Devices Professional Services to create new User Groups or to edit the predefined groups.

NOTE Editing existing user group privileges affects all users in the group and any new users added to the group. Reverting changes is not trivial and includes changing the user privileges assigned to the group, as well as individual privileges for all objects created while privileges are in flux.

MP Console User Actions

The following sections describe commonly performed User-related tasks you can perform in the MP Console. Each task section explains how to navigate through the necessary screens to perform the task and provides tips for using the screen or screens

involved. For detailed MP Console field and screen element descriptions, see the online help by clicking the **Help** link from any page in the MP Console.

Simple vs. Advanced Mode

Throughout the instructions in this chapter, you will be asked to log on to the Grid MP Console. At the log on screen, you can choose between Simple and Advanced Mode. Simple Mode is suitable for most Users. Advanced Mode displays additional information when the system encounters an error and displays GUIDs (ID numbers used to identify objects, such as Jobs, Devices, etc.) and allows system administrators to assign roles and privileges to users and user groups. For advanced access control tasks, such as assigning roles and privileges directly to users or user groups, you must be logged on in Advanced Mode. The instructions below specify the times when Advanced Mode is required.

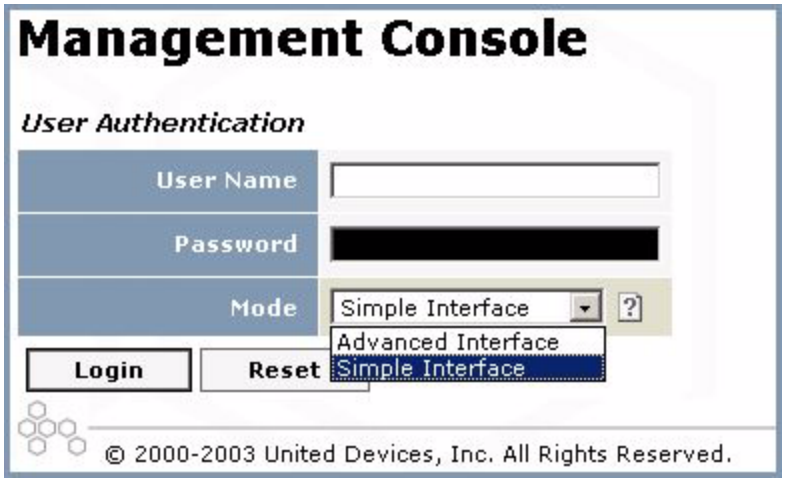


Figure 14. MP Console Logon Screen

View a List of All Users

You can view a list of the existing Users in the system through the MP Console from the Users screen. The screen lists the current Users, the User's state, and the date the User profile was last updated. From this list, you can link to more detailed views of individual User profiles.

Where to Start

1. Log on to the MP Console.
2. Click Start > Platform > Security > Users. The system displays the Users screen.

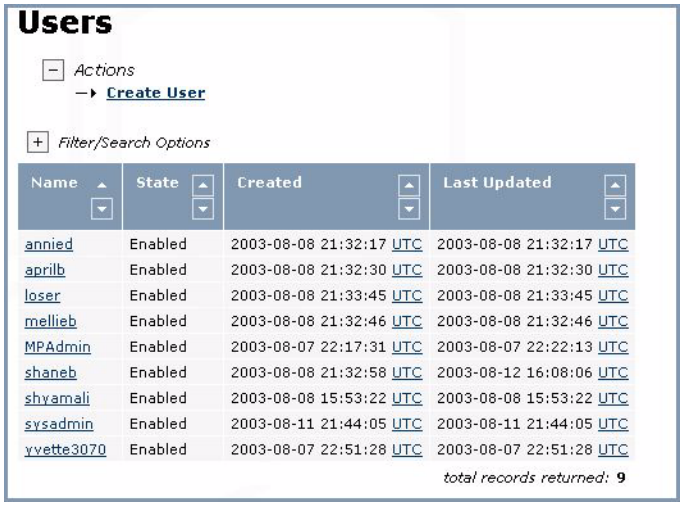


Figure 15. Users Screen

Using the Screen

- Click a User name to navigate to a detailed view of the User's profile.
- Use the arrows to sort the list by name, state, created date or last modified date.

View Detailed User Information

To see information about a User, such as Role assignments, telephone number, and email address, you can use the User screen in the MP Console. The User screen also contains links to screens where you can manage Role assignments, view statistics about Jobs created by the User, and more.

Where to Start

1. Log on to the MP Console.
2. Click Start > Platform > Security > Users. The system displays the Users screen.

3. Click the name of the User you want to view. The system displays the User details screen.

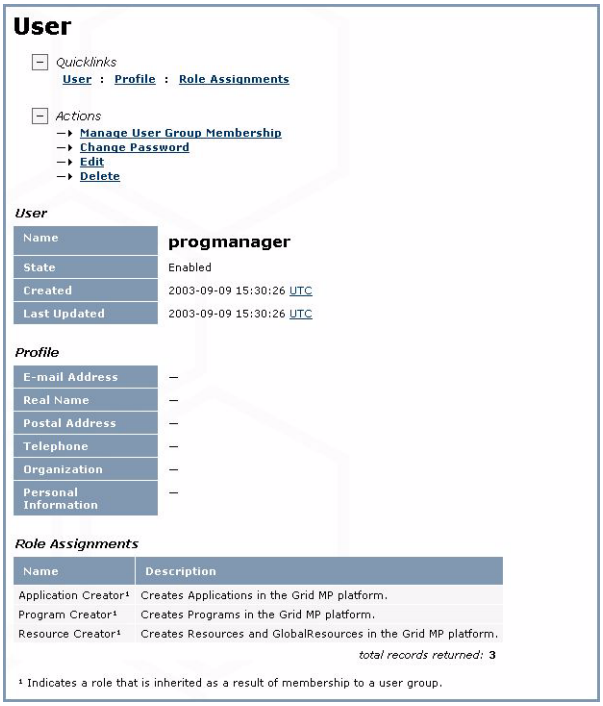


Figure 16. User Screen

Using the Screen

- From the User details screen, you link to screens you can use to change a User password, edit the User record, or add the User to User Groups, or delete the User.
- The User's current Role assignments display at the bottom of the page.

Create a New User

When you first install the Grid MP platform, one default User exists in the system: MPAdmin. You must create additional Users and assign them to User Groups for people to be able to log on to the MP Console.

Where to Start

1. Log on to the MP Console.
2. Click Start > Platform > Security > Users. The system displays the Users screen.
3. Click **Create User** in the Actions list. The system displays the Create User screen.

4. Provide a User name and password for the new account. You may also provide personal and contact information for the User.
5. Click **Create**.

Using the Screen

- You must provide a user name and password to create a User profile. All other attributes are optional.
- Click **Reset** to clear all the fields.
- Click **Cancel** to return to the Users screen.

Change User Password

You may need to change passwords when Users forget passwords or at other times to maintain security.

CAUTION Do not change the password for the default MPAdmin User account. Doing so will prevent the Service Manager from working correctly.

Where to Start

1. Log on to the MP Console.
2. Click Start > Platform > Security > Users. The system displays the Users screen.
3. Click the name of the User for which you want to change a password. The system displays the User details screen.
4. Click **Change Password** to display a form for changing passwords.

Figure 17. Change Password Screen

Using the Screen

- Type the new password and retype it for validation.
- Click **Change** to change the password
- Passwords must be at least six characters in length and contain both letters and numbers.
- Click **Reset** to clear the fields.
- Click **Cancel** or the User name to return to the User details screen.

Disable User Account

There may be times when you do not want to delete a User profile, but you do not want the User to access the MP Console. You can temporarily disable a User account by changing the User's state.

Where to Start

1. Log on to the MP Console.
2. Click Start > Platform > Security > Users. The system displays the Users screen.
3. Click the name of the User account you want to disable. The system displays the User details screen.
4. Click **Edit**. The system displays an editable User details form.

Using the Screen

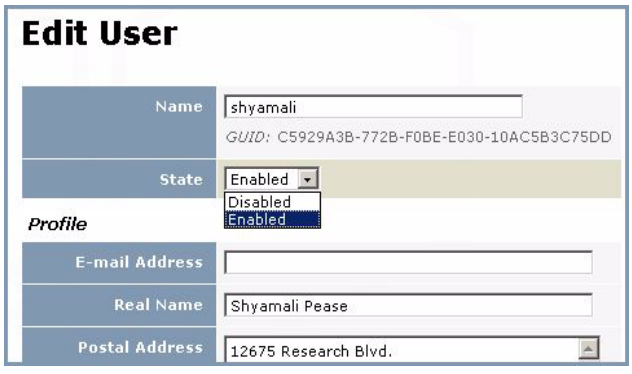


Figure 18. Edit User Screen - Disable User

- Change the state from Enabled to Disabled.
- Click **Update** to save your changes.

- Once you disable an account, the User will not be able to log on to the MP Console until you enable the account.
- Click **Reset** to return the form to its last modified state.
- Click **Cancel** to return to the User details screen.

Edit User Information

Due to organizational changes or other factors, you may need to edit a User profile to change the contact and other personal information for the User. Users can edit their own personal information, but only MP Administrators can edit the User name or status.

Where to Start

1. Log on to the MP Console.
2. Click Start > Platform > Security > Users. The system displays the Users screen.
3. Click the name of the User account you want to edit. The system displays the User details screen.
4. Click **Edit**. The system displays an editable User details form.

Using the Screen

- Change the personal or contact information and click **Update** to save your changes.
- If you disable an account, the User will not be able to log on to the MP Console until you enable the account.
- Click **Reset** to return the form to its last modified state.
- Click **Cancel** to return to the User details screen.

Delete User

If a User no longer needs access to the Grid MP platform, you can delete the User account. Deleting a User deletes Jobs and Data created by the User.

CAUTION If you delete the User account used for registering MP Agents, you will not be able to register new MP Agents until you create a new User account and change the init.ud parameters to reflect the change. For more information, see Chapter 6, "Installing the MP Agent," in the *Installation Guide*.

Where to Start

1. Log on to the MP Console.
2. Click Start > Platform > Security > Users. The system displays the Users screen.
3. Click the name of the User account you want to delete. The system displays the Delete User screen.
4. Click **Delete** to remove the User from the database. The system prompts you to confirm the action. Click **OK** to confirm.

Using the Screen

- Once you delete the User account, the User will not be able to access the Grid MP platform.
- You cannot undo a delete action.
- From the Delete User screen, click the username or **Cancel** to return to the User details screen.
- From the Delete confirmation prompt pop-up window, click **Cancel** to return to the Delete User screen.

MP Console User Group Actions

The following sections describe commonly performed User-group-related tasks you can perform in the MP Console. Each task section explains how to navigate through the necessary screens to perform the task and provides tips for using the screen or screens involved. For detailed MP Console field and screen element descriptions, see the online help by clicking **Help** from any page in the MP Console.

View a List of All User Groups

You can view a list of the existing User Groups in the system through the MP Console from the User Groups screen. The screen lists the current User Groups, each group's state, the number of Users in the group, and the date the User Group's profile was created and last updated. From this list, you can link to more detailed views of individual User Groups.

Where to Start

1. Log on to the MP Console.
2. Click Start > Platform > Security > User Groups. The system displays the User Groups screen.

Using the Screen

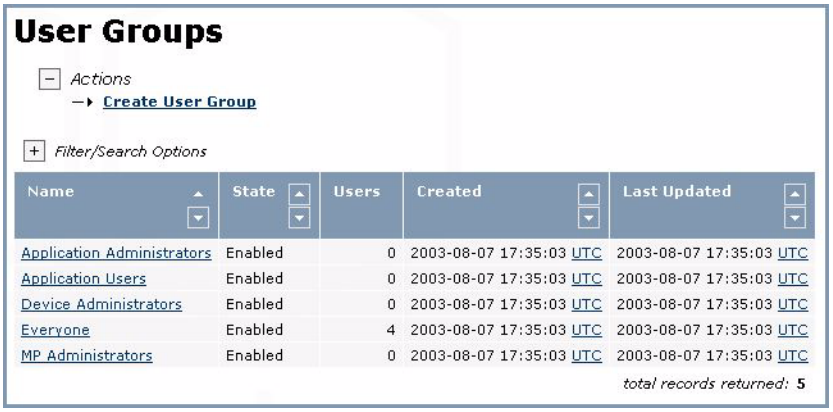


Figure 19. User Groups Screen

- Click a User Group name to navigate to a detailed view of the User Group's profile.
- Use the arrows to sort the list by name, status, number of Users, created date, or last modified date.

View Detailed User Group Information

To see information about a User Group, such as Role assignments and a description of the group, you can use the User Group screen in the MP Console. The User Group screen also contains links to screens where you can manage Role assignments, view statistics about Jobs created by the User Group, and more.

Where to Start

1. Log on to the MP Console.
2. Click Start > Platform > Security > User Groups. The system displays the User Groups screen.
3. Click the name of the User Group you want to view. The system displays the User Group details screen.

Using the Screen

- Role assignments listed are the default Roles Users assigned to the group will inherit.

Create a New User Group

When you first install the Grid MP platform, five preconfigured User Groups exist in the system. For more information about the preconfigured User Groups, see "User Groups," on page 82. To create new User Groups, use the Create User Group screen.

Where to Start

1. Log on to the MP Console.
2. Click Start > Platform > Security > User Groups. The system displays the User Groups screen.
3. Click **Create User Group** in the Actions list. The system displays the Create User Group screen.
4. Provide a name for the new User Group. You may also provide a description and change the User Group state.
5. Click **Create**.

Using the Screen

- You must provide a User Group name to create a User Group profile. All other attributes are optional.
- Click **Reset** to clear all the fields.
- Click **Cancel** to return to the User Groups screen.
- To assign Roles and Privileges to a User Group, you must log on to the MP Console in Advanced Mode. Contact United Devices Professional Services for assistance. For more information, see "MP Console Role and Privilege Actions" on page 102

Disable User Group

There may be times when you do not want to delete a User Group profile, but you do not want the User Group to access the MP Console. You can temporarily disable a User Group account by changing the User Group state.

NOTE	Disabling a User Group does not disable complete access to the MP Console, it just inhibits the use of Privileges/Roles that resulted from membership to that group.

Where to Start

1. Log on to the MP Console.
2. Click Start > Platform > Security > User Groups. The system displays the User Groups screen.
3. Click the name of the User Group account you want to disable. The system displays the User Group details screen.
4. Click **Edit**. The system displays an editable User Group details form.
5. Change the state from Enabled to Disabled.
6. Click **Update** to save your changes.

Using the Screen

- Users will not have access to Roles and Privileges they inherit from the disabled User Groups, but they will still have access to all other Roles and Privileges on their User account or from other User Groups.
- Click **Reset** to return the form to its last modified state.
- Click **Cancel** to return to the User Group details screen.

Delete User Group

If a User Group no longer needs access to the Grid MP platform, you can delete the User Group account.

Where to Start

1. Log on to the MP Console.
2. Click Start > Platform > Security > User Groups. The system displays the User Groups screen.

3. Click the name of the User Group account you want to delete. The system displays the Delete User Group screen.
4. Click **Delete** to remove the User Group from the database. The system prompts you to confirm the action. Click **OK** to confirm.

Using the Screen

- Once you delete the User Group account, Users belonging to the User Group will not be able to perform actions in the Grid MP platform, unless they belong to other User Groups or have Roles and Privileges directly assigned to their User account.
- You cannot undo a delete action.
- From the Delete User Group screen, click the User Group name or **Cancel** to return to the User Group details screen.
- From the Delete confirmation prompt pop-up window, click **Cancel** to return to the Delete User Group screen.

Add User to User Group

Users you add to a User Group automatically inherit any Roles assigned to the group.

Where to Start

1. Log on to the MP Console.
2. Click Start > Platform > Security > User Groups. The system displays the User Groups screen.
3. Click the name of the User Group to which you want to add Users. The system displays the User Group details screen.
4. Click **Manage User Membership**. The system displays the Manage User Membership for User Group screen. The screen contains a list of any Users previously added to the group
5. Click Add Users to User Group. The system displays a screen containing a list of Users on the system.
6. Select the check box(es) corresponding to the User(s) you want to add.
7. Click **Add** to add the Users.

Using the Screen

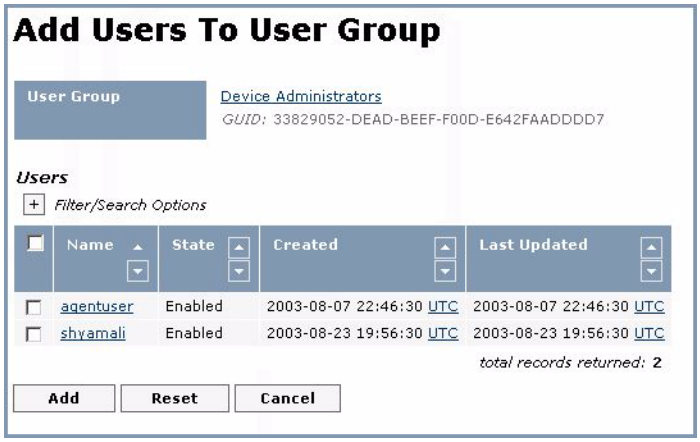


Figure 20. Add Users to User Group Screen

- Users can belong to more than one User Group.
- You can use the Add Users to User Group screen as described above to add multiple Users to one group. If you want to add one User to multiple groups, it is more efficient to use the Add User to User Groups screen. To access that screen:
  a. Click Start > Platform > Security > Users.
  b. Select the User you want to add to multiple groups.
  c. Select Manage User Group Membership from the User details screen.
  d. Click Add User to User Groups from the Manage User Group Membership screen.
- To clear a checked box, click the box a second time.
- Click **Reset** to return the check boxes to the last modified state.
- Click **Cancel** to return to the User Group details screen.

Remove User from User Group

Due to organizational changes, you may need to move Users from one User Group to another or to simply remove Users from a User Group. You can use the Remove Users from User Group screen to accomplish this task.

Where to Start

1. Log on to the MP Console.
2. Click Start > Platform > Security > User Groups. The system displays the User Groups screen.

3. Click the name of the User Group to which you want to add Users. The system displays the User Group details screen.
4. Click **Manage User Membership**. The system displays the Manage User Membership for User Group screen. The screen contains a list of any Users previously added to the group.
5. Click Remove Users from User Group. The system displays a list of any Users previously added to the group.
6. Select the check box(es) corresponding to the User(s) you want to remove.
7. Click **Remove** to remove the Users.

Using the Screen

- Users can belong to more than one User Group. Removing a User from one User Group does not automatically disable their access to the system. See "Disable User Account" on page 94 for help disabling User access to the system.
- You can use the Remove Users from User Group screen as described above to remove multiple Users from one group. If you want to remove one User from multiple groups, it is more efficient to use the Remove User from User Groups screen. To access that screen:
  a. Click Start > Platform > Security > Users.
  b. Select the User you want to add to multiple groups.
  c. Select Manage User Group Membership from the User details screen.
  d. Click Remove User from User Groups from the Manage User Group Membership screen.
- To clear a checked box, click the box a second time.
- Click **Reset** to return the check boxes to the last modified state.
- Click **Cancel** to return to the User Group details screen.

MP Console Role and Privilege Actions

Assign Roles to a User

You can assign Users to a User Group to automatically grant them all the Roles and Privileges associated with the group. You can also assign a Role or Roles directly to the User for them to have access to functionality and data.

Where to Start

1. Log on to the MP Console in Advanced Mode.
2. Click Start > Platform > Security > Users. The system displays the Users screen.
3. Click the name of the User to which you want to assign a role in the Users list. The system displays the User details screen.
4. Click **Manage Role Assignments**. The system displays the Manage Role Assignments for User screen.

Using the Screen

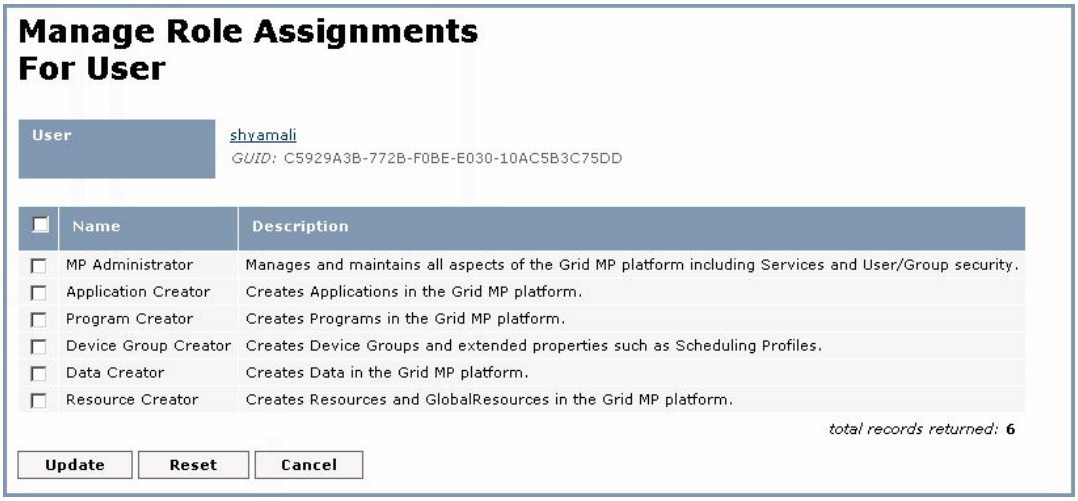


Figure 21. Manage Role Assignments Screen

- Select the check box(es) corresponding to the Role(s) you want to assign.
- Click **Update** to assign the Roles.
- If you assign more than one Role to a User, the User has all of the Privileges of all of the Roles.
- Selecting the check box in the table header selects all Roles.
- To clear a checked box, click the box a second time.
- Click **Reset** to return the check boxes to the last modified state.
- Click **Cancel** to return to the User details screen.

Assign Roles to a User Group

Once you create a User Group and add Users to it, you should assign Roles to the group to make it truly useful. You can create a User Group with Role assignments and then assign Users to it who are likely to perform the same functions. The Users automatically inherit the Roles you assigned to the group.

NOTE Editing existing User Group Privileges affects all Users in the group and any new Users added to the group. Reverting changes is not trivial and includes changing the User Privileges assigned to the group, as well as individual Privileges for all objects created while Privileges are in flux.

Where to Start

1. Log on to the MP Console.
2. Click Start > Platform > Security > User Groups. The system displays the User Groups screen.
3. Click the name of the User Group to which you want to assign a Role in the User Groups list. The system displays the User Group details screen.
4. Click **Manage Role Assignments**. The system displays the Manage Role Assignments for User Group screen.
5. Select the check box(es) corresponding to the Role(s) you want to assign.
6. Click **Update** to assign the Roles.

Using the Screen

- Selecting the check box in the table header selects all roles.
- To clear a checked box, click the box a second time.
- Click **Reset** to return the check boxes to the last modified state.
- Click **Cancel** to return to the User Group details screen.

Grant and Revoke Privileges

Users have access to data they entered themselves, such as Jobs they create, but they can also grant access to their own data to other Users.

From the object detail screens in the MP Console, you can access the Manage Privileges screens for the following objects:

- Applications
- Programs
- Jobs
- Device Groups
- Data Sets

Where to Start

1. Log on to the MP Console in Advanced Mode.
2. From the Application, Program, Job, Device Group, or Data Set details screen, click one of the **Manage Privilege** screens. The system displays the Manage Privileges screen.

NOTE	You can grant or revoke Privileges for Users or User Groups. The following instructions walk you through granting User Privileges. See the MP Console online help for help revoking Privileges.

3. Click **Grant Users** to navigate to a form you can use to add Privileges for the specified object to one or more Users. The form displays a list of Users in the system.

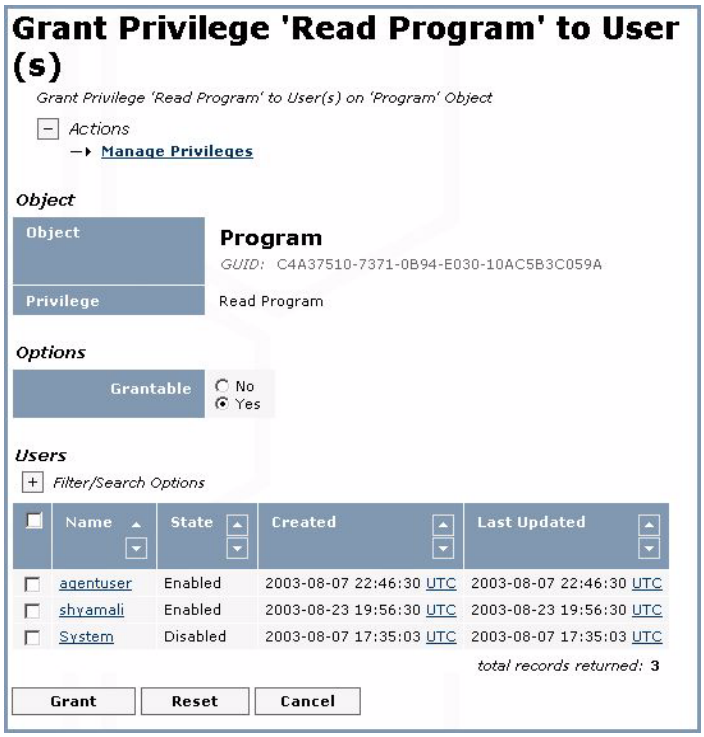


Figure 22. Grant Privileges Screen

Using the Screen

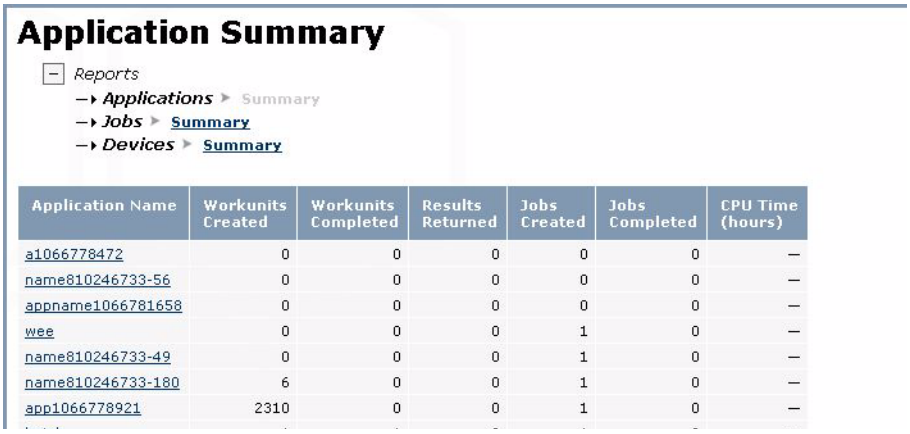
- Select the check box(es) corresponding to User(s) you want to grant the Privilege.
- Click **Grant** to save your changes
- Click a user name to navigate to the User details screen.
- To allow the User or Users to grant the Privilege to others, select Yes for the Grantable option.
- Click **Reset** to return the check boxes to the last modified state.
- Click **Cancel** to return to the Manage Privileges screen.

Chapter 7: MP Console Reports

The MP Console contains three reports to assist System Administrators in monitoring system utilization. The Application, Job, and Device Summary reports provide daily snapshots of the most important usage information in the Grid MP platform. A crontab automatically creates the reports based on the prior days data and past reports are stored in XML files.

NOTE The MP Console reports are only available for DB2 configurations at this time.

Application Summary Report



Application Name	Workunits Created	Workunits Completed	Results Returned	Jobs Created	Jobs Completed	CPU Time (hours)
a1066778472	0	0	0	0	0	–
name810246733-56	0	0	0	0	0	–
appname1066781658	0	0	0	0	0	–
wee	0	0	0	1	0	–
name810246733-49	0	0	0	1	0	–
name810246733-180	6	0	0	1	0	–
app1066778921	2310	0	0	1	0	–

Figure 23. Application Summary Report

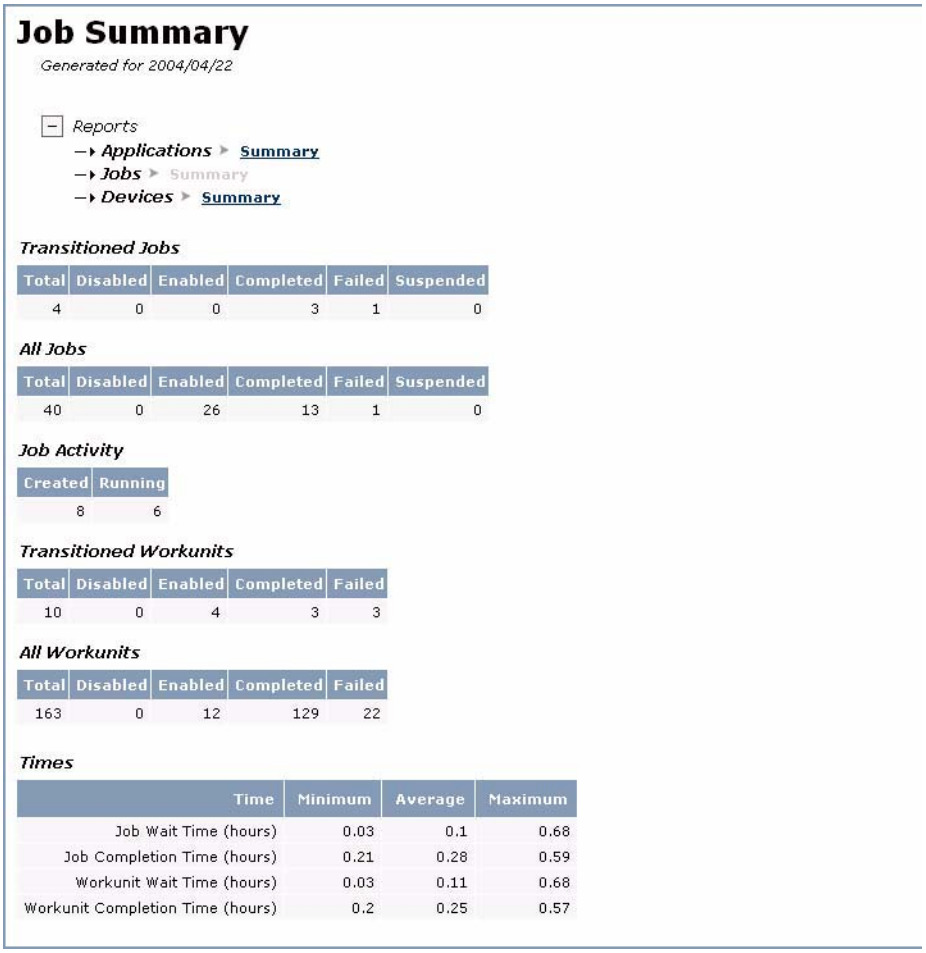
The Application Summary report contains the following information about Applications in the Grid MP platform during the report period:

- Application Name—The name of the Application

NOTE The Application Summary Report includes all Applications that existed at any point during the report period, even if the Application was deleted prior to the end of the report period.

- Workunits Created/Completed—Two columns display the number of Workunits created for Jobs instantiating the Application, and the number of Workunits completed.
- Results—The number of Results.
- Jobs Created/Completed—Two columns display the number of Jobs created for each Application, and the number of Jobs completed.
- CPU Hours—The amount of CPU time that has been devoted to each Application by Devices on the Grid MP platform.

Job Summary Report



Job Summary

Generated for 2004/04/22

Reports
Applications ▸ Summary
Jobs ▸ Summary
Devices ▸ Summary

Transitioned Jobs

Total	Disabled	Enabled	Completed	Failed	Suspended
4	0	0	3	1	0

All Jobs

Total	Disabled	Enabled	Completed	Failed	Suspended
40	0	26	13	1	0

Job Activity

Created	Running
8	6

Transitioned Workunits

Total	Disabled	Enabled	Completed	Failed
10	0	4	3	3

All Workunits

Total	Disabled	Enabled	Completed	Failed
163	0	12	129	22

Times

Time	Minimum	Average	Maximum
Job Wait Time (hours)	0.03	0.1	0.68
Job Completion Time (hours)	0.21	0.28	0.59
Workunit Wait Time (hours)	0.03	0.11	0.68
Workunit Completion Time (hours)	0.2	0.25	0.57

Figure 24. Job Summary Report

The Job Summary report contains information about Jobs and Workunits in the Grid MP platform during the report period.

Transitioned Jobs/All Jobs

The Transitioned Jobs section displays the number of Jobs in each state for all Jobs that had a different state at the end of the report period than they had at the beginning of the report period. The All Jobs section displays the number of Jobs in each state for all Jobs in the Grid MP platform at the end of the report period.

NOTE If a Job was deleted during the report period, it will not be counted in the All Jobs section. If it underwent a change of state prior to the deletion, it will be counted in the Transitioned Jobs section.

The state information is the last known state for the report period. Reports are based on past information, and Jobs may have changed state since the report ran.

At the time of the report, Jobs were in one of the following states:

- Total
  - Transitioned Jobs—The total number of Jobs that underwent a change of state during the report period.
  - All Jobs—The total number of Jobs in the Grid MP platform for the report period.
- Disabled—Jobs in this state were not enabled yet and were not able to run. Enabled—Jobs in this state were ready to run.
- Completed—Jobs in this state met the requirement for the minimum number of Results.
- Failed—Jobs in this state contained a Job Step that failed due to a Workunit reaching the maximum number of Errors allowed.
- Suspended—Jobs in this state were suspended and not able to run.

Job Activity

The reports displays the number of Jobs in each of the following states for the Report date:

- Created—Jobs in this state were created during the report period.
- Running—Jobs in this state were running Workunits on a Device during the report period.

Transitioned Workunits/All Workunits

The Transitioned Workunits section displays the number of Workunits in each state for the Workunits that underwent a change of state during the report period. The All Workunits section displays the number of Workunits in each state for all Workunits in the Grid MP platform at the end of the report period.

NOTE If a Workunit was deleted during the report period, it will not be counted in the All Workunits section. If it underwent a change of state prior to the deletion, it will be counted in the Transitioned Workunits section.

At the time of the report, Workunits were in one of the following states:

- Total
  - Transitioned Workunits—The total number of Workunits that underwent a change of state during the report period.
  - All Workunits—The total number of Workunits in the Grid MP platform for the report period.
- Disabled—Workunits in this state were disabled and could not run.
- Enabled—Workunits in this state were enabled and ready to run.
- Completed—Workunits in this state met the required number of Results, and will no longer be run.
- Failed—Workunits in this state generated the maximum number of Errors, and will no longer be run.

Wait/Completion Time

The Minimum, Average, and Maximum number of seconds for each of the following:

- Job Wait Time—The number of seconds from the time the Job was created to the time the first Workunit was dispatched to a Device.
- Job Completion Time—The number of seconds from the time the Job was created to the last time the record was modified while in the completed state.
- Workunit Wait Time—The number of seconds from the time the Workunit was created to the time the Workunit was dispatched to a Device.

- Workunit Completion Time—The number of seconds from the time the Workunit was created to the last time the record was modified while in the completed state.

NOTE	Editing a Job or Workunit record after it completes, can cause the Job Completion Time or Workunit Completion Time to be incorrect

Device Summary Report

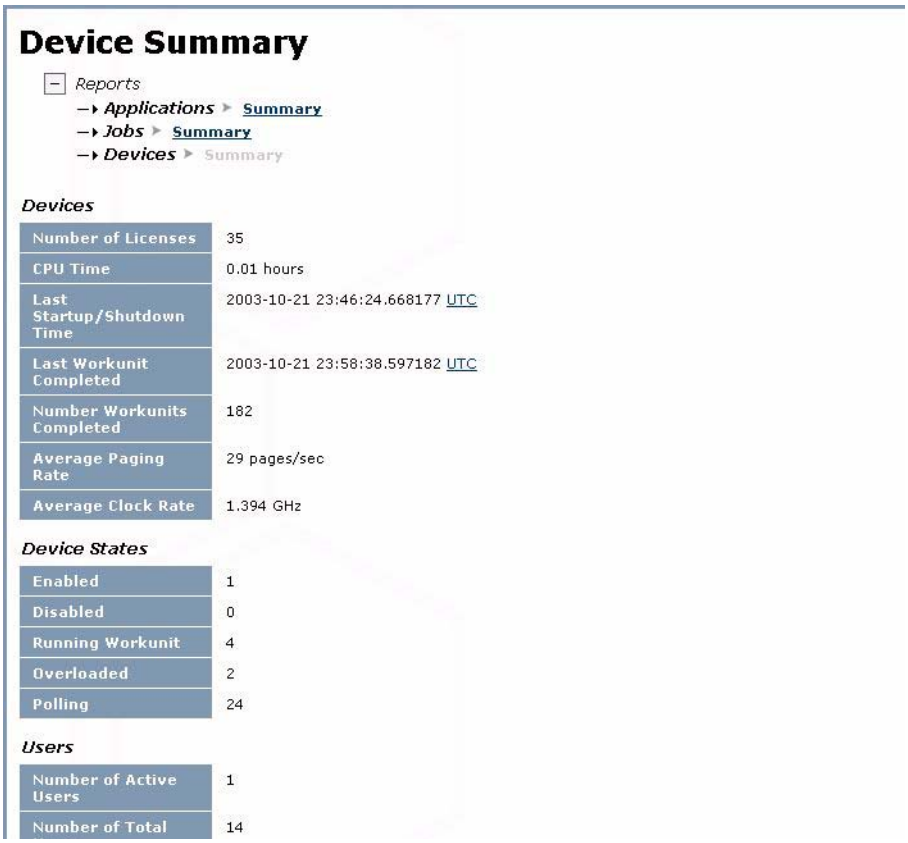


Figure 25. Device Summary Report

The Device Summary report contains the following information about Devices in the Grid MP platform during the report period:

Devices

- Number of Licenses—The number of MP Agents currently licensed to log on to the Grid MP platform.

- Number of Unique Devices Returning Results— The number of unique devices that participated in all Jobs on the given report date.
- CPU Time—The number of CPU seconds the system took to create the Results returned during the report period.
- Last Workunit Completed—The timestamp of the most recent completion of a Workunit during the report period.
- Number Workunits Completed—The total number of Workunits that have met the required number of Results, and will no longer be run.
- Average Paging Rate—The average disk paging rate (in pages/sec) for all Devices connected to the Grid MP platform during the report period.
- Average Clock Rate—The average approximate processor speed (in gigahertz) of Devices running Workunits during the report period.

Device States

The report displays the number of Devices in each of the following states for the given report period:

- Enabled—Devices in this state were able to receive Workunits during the report period.
- Disabled—Devices in this state were not able to receive Workunits during the report period.
- Running Workunit—Devices in this state were running Workunits during the report period.
- Overloaded—Devices in this state reported that they were suspending a Workunit due to exceeding a device threshold.
- Polling—Devices in this state communicated with the Poll Service during the report period.

Appendix A: Troubleshooting

This appendix describes atypical symptoms or events that may occur and provides guidance for resolving those issues. For all other issues, please contact United Devices Professional Services.

A utility named ud_logbundle is installed during the Grid MP platform installation in the server /usr/local/UD/utils directory. This utility is used to automatically bundle Grid MP platform log information from select server system logs. The resulting file can subsequently be sent to UD Professional Services for analysis and troubleshooting. Command line arguments can be passed to this utility to specify a range of dates and times for which relevant log information will be extracted from the Grid MP platform.

Unable to Display the MP Console Login Page

If a User cannot display the MP Console logon screen, one of the following situations might have occurred:

- The browser or browser version is unsupported.

  Use a supported browser. For more information, see the "Prerequisites and Requirements" section in Chapter 1 of the *Installation Guide*.

- The browser does not accept cookies.

  Change browser settings to accept cookies.

- The browser is not Javascript-enabled.

  Change browser settings to enable Javascript.

- The correct URL and port for the MP Console does not match the URL and port you are using.

  Check installation notes and ud.conf settings with help from United Devices Professional Services.

- The MGSI RPC Service and/or the MP Console is not running.

Check the status of the MGSI RPC Service and MP Console Service from the command line as described in “Managing Services from the Command Line” on page 30. If the services are not running, restart them.

User Cannot Log on to the MP Console

- The username or password is incorrect.
  a. Log on to the MP Console as an MPAdmin User. MPAdmin is the default system administration User. You or other system administrators may have created other system administration User accounts after installation. Use the most appropriate account.
  b. Check that the User has a User account.
  c. Check the status of the User account. If it is disabled, this may be for an administrative reason. If not, you can enable the password by reversing the instructions in “Disable User Account” on page 94.
  d. If the User has an account and it is enabled, you can give the User a new password and instruct them to change the password after logging on.

- The MP Console reports an error

  You may see one of the following errors when attempting to log on to the MP Console:

  – Grid MP platform Database is offline—This message could mean that the Database is down for maintenance or due to an error. Check /var/log/ud.log and /var/log/messages for more information and contact your DBA or United Devices Professional Services for assistance.
  – Grid MP platform currently under heavy load—This message could mean that the services cannot connect to the database or that other problems are occurring. Check /var/log/ud.log and /var/log/messages for more information.
  – MGSI RPC Service is offline—If one of the services is offline, attempt to restart services.

500 Error when trying to Log on to the MP Console

This is an Apache Server error and must be investigated by executing the following command on the Apache server:

```
grep httpd_prefork /var/log/ud.log
```

to see what the cause of the error condition is.

Services cannot connect to the Database

When troubleshooting, if you come across errors such as the following in the ud.log, it means the services cannot connect to the database:

```
run_batch[17050]: FATAL: Unable to open connection to
   database: ERR_DB_ODBC
```

- It is possible that the configuration parameters for the services are incorrect

  Log in to the system hosting the service(s) as root and check the following parameters in the `/usr/local/UD/conf/ud.conf` file:

  - UD_DB_NAME
  - UD_DB_PASSWORD
  - UD_DB_USER

  If the value of any preceding parameter is incorrect, change the parameter and restart the service. For more information about changing parameters, see"Changing MP Configuration Parameters" on page 19.

- The database may be down for maintenance or due to a database failure. Contact your DBA or United Devices Professional Services for assistance.

System Administrator Lost Password

If there are other system administrators with their own accounts, request that one of them log on and reset the lost password. If you are the only system MP administrator, log on as the default administrator MPAdmin and reset your password. If you have lost the password for the default administrator account, and you are the only administrator, contact Professional Services. Professional Services can supply you with a database command to reset the password.

CAUTION Do not change the password for the default MPAdmin User account. Doing so will prevent the Service Manager from working correctly.

MP Services Are Not Running

Check the Services screen in the MP Console to determine which services have stopped.

- Multiple services are stopped or in error.

  Restart services manually through MP Console. This can take a few minutes to complete. If services do not restart, contact Professional Services.

- If only the Dispatch Service is down, and restarting from the MP Console does not resume normal operations, it may be a license issue:

  a. Check to ensure that the server license file (ud_server_license.sig) is in /usr/local/UD/conf/.

  b. Ensure that the license file is world readable.

  ```
  chmod a+r ud_server_license.sig
  ```

  c. Use grep to search the /var/log/ud.log file for license information with the following command on the Dispatch Service machine:

  ```
  grep -4 'verify_signature_file' /var/log/ud.log
  ```

  d. If the search does not return verification information, you can also check /var/log/ud.log for license related errors. If the license is invalid or expired, you should see one of the following errors:

  "Your license has expired. Please contact United Devices for relicensing information."

  "Your Grid MP license file could not be verified. Ensure that /usr/local/UD/conf/ud_server_license.sig is a valid license, or contact United Devices for licensing information."

  If you receive either error, contact United Devices to obtain a valid server license file.

The System Is Not Operating Correctly

When the system is not performing as well as usual, or you start to encounter other unexpected system behavior, perform the following steps in order:

1. Increase the logging levels for each service to **`INFO`**, **`DEBUG`**, or **`TRACE`** and restart the services. Log levels are controlled by ud.conf parameters. For information on which parameters to update and what each level represents, see "Log Location" on page 33.

   CAUTION Changing the log levels can affect performance. In some usage scenarios, higher log levels can cause logs to fill up available disk space. Monitoring remaining disk space in /var is recommended.

2. Check server health; this includes monitoring disk space on partitions, network connectivity, and CPU boundedness. Professional Services can assist you in setting up server monitoring solutions, or integrating with existing solutions.
3. Contact Professional Services. It is possible Professional Services will ask you to run ud_logbundle.

I Need to Migrate to Another Set of Hardware

Contact Professional Services to coordinate the migration.

I Need to Reorganize the Currently Deployed Services

If you have just installed the services, but have not logged in or used the Grid MP platform, and decide you need to reorganize the service configuration, see the Troubleshooting appendix in the *Installation Guide* for help uninstalling. If you have a working deployment and you want to move services, contact Professional Services for assistance.

Agents Cannot Receive Workunits/Synchronization

If an MP Agent can register against the Realm Service but fails to receive Workunits from the Dispatch Service, you may want use the decryptlog utility to view the cslg.ud file in the mpagent directory. See "Monitoring Agents," on page 46 for help using the decryptlog utility.

If the cslg.ud file contains entries such as the following, it may be an indication that service machine clocks are not synchronized.

```
ERROR: ConstructResponse: client supplied an invalid
   authentication token

ERROR: Fault: Realm token has been revoked

ERROR: Realm authentication token marked as invalid
```

The Grid MP installer includes the ntp daemon, however it may not be running or may not be able to acquire time synchronization peers properly due to firewall or network restrictions.

Run the following commands on each component machine to ensure ntpd is working.

1. To verify that ntpd is active:

   /sbin/service ntpd status

2. To verify that ntpd is able to acquire peers:

   /usr/sbin/ntpdc -c peers

The output should contain multiple hosts and the magnitude of the "offset" columns should all be less than 1.0. For example, the following output is displays two service machines with an acceptable time offset:

```
remote             local      st poll reach  delay
   offset    disp
=service1.host.com 172.16.1.34      2 1024  377 0.00050
   0.000580 0.01482
*service2.host.com     172.16.1.34      2 1024  377 0.00044 -
   0.002166 0.01483
```

If ntpd is not active, or not working, contact your system administrator or Professional Services for assistance. Ensure that all machines are in the same timezone and use NTP to synchronize all clocks. Restart your services. Your MP Agent should no longer obtain realm tokens that are detected as being invalid by the Dispatch Service.

Slow response time for Jobs

If a User reports very slow response time for Jobs:

- Check that the Job is running.
- If the Job is running, check the Errors and Results for the Jobs.
- Check the factors that affect the scheduling of Jobs, such as Device thresholds or maximum Workunit timeouts. Suggest that the User increase the Job priority, reduce the minimum number of Results required for a Job to complete, and that the User request that Device managers increase the User's priority level on Device Groups. See "Scheduling" on page 59 for a list of all of the properties that can affect Jobs.
- Check the Runnable flag for the Job and Job Step. For a Job to be flagged as runnable, the Job Step(s) state must be ENABLED_OPEN or ENABLED_CLOSED; the Job state is ENABLED; the Program.state must be ENABLED, CLOSED, or PENDING_DELETE; the application state is ENABLED, CLOSED, or PENDING_DELETE; and if the current time is within the Job start and end times.
- If the Job or Job Step is not flagged as runnable, check the state of the Job, Job Step, Program, and Application. Check that the current time is within the Job start and end times.
- It is also possible that service machine clocks are not synchronized. For more information, see "Agents Cannot Receive Workunits/Synchronization," on page 117.

User Cannot Upload Files

- If a User receives an error when attempting to upload a Program Module executable or MP Agent module, the machine running the File Service may have insufficient memory. Ensure that the machine has at least 1GB of RAM.
- The File Service may be down. Check service status.
- For very large Data file uploads, the MGSI may be more appropriate than theMP Console for uploads. Contact Professional Services for assistance.

Uploading a New License File

The license file provided by Professional Services specifies the number of MP Agents you have purchased. A license is needed for each CPU on multiprocessor machines.

You can install MP Agents on more machines than the number of licenses you have. Workunits are dispatched on a first-come-first-served basis and once the number of licensed MP Agents has been exhausted, all other Devices will be backed-off until a license becomes available. MP Agents that do not have a license can still communicate (such as registering, polling, and receiving Device commands) with the services, but they cannot receive Workunits until a license becomes available.

If a Device is deleted, its license is immediately reclaimed. If the Device is removed, as in a laptop, the license is reclaimed when the Device state transitions to “dormant”, or the Workunit is timed out by the database, or any other User-prompted action which deletes the Workunit on the Device.

To upload a new license from Professional Services,

1. Stop all services:

   ```
   /sbin/service mpservices stop
   ```

2. Copy the license file to /usr/local/UD/conf/ to the machine hosting the Dispatch service:

   ```
   cp directory/ud_server_license.sig /usr/local/UD/conf/
   ```

3. Ensure that the license file is world readable:

   ```
   chmod a+r ud_server_license.sig
   ```

4. Start all services:

   ```
   /sbin/service mpservices stop
   ```

Disabling SSL For File Transfers

Disabling the SSL is recommended for deployments where:

- Switched networking or other network topology where network snooping of file data is not a concern.
- Network performance of file transfers is being impacted heavily by SSL encryption overhead.
- Use of SSL is not possible or permitted due to networking or compatibility restrictions.

Use the following steps to disable the SSL:

1. Edit /usr/local/UD/conf/ud.conf and set the `UD_WEB_FILESVR_ALLOW_INSECURE` to `1`.
2. Edit /usr/local/UD/conf/svcmgrconf.xml and change the URI for the File Service that says:

   `https://xxxxxxxxxx:28443/mgsi/filesvr.cgi` to `http://xxxxxxxxx:28080/mgsi/filesvr.cgi`

   where xxxxxxxxxx is the IP address or the host name of the machine.
3. Restart the File Service:

   `/sbin/service mpwebsvc restart`

Installing custom SSL Certificates

If you want to use your own custom SSL certificate, you need to replace the self-signed certificate provided by United Devices with the certificate generated by you. For multi-box setups, you will need to perform these steps on each machine except the one hosting the database.

Use the following steps to install the custom SSL certificates:

1. Copy the certificate file to /usr/local/UD/inetpub/etc/ssl/crt and rename it as mpservice.crt.
2. Copy the file containing the key to /usr/local/UD/inetpub/etc/ssl/key and rename it as mpservice.key.
3. Restart the MP Services:

   `/sbin/service mpwebsvc restart`

NOTE	If errors occur during restart, check /var/log/ud.log for error messages.

Appendix B: Managing the Database

This appendix provides very basic database commands and recommendations for usage with the Grid MP plaform.We strongly recommend that you review these commands with your DBA to ensure they are the most appropriate actions for your environment.

NOTE	United Devices recommends using the MP Console or MGSI to access database information. Otherwise, your database could be corrupted.

Introduction to DB2 commands

This section introduces the basics of running and using DB2 commands.To run DB2 commands, you must first run the DB2 profile.

```
. /instance_owner_home_dir/SQLLIB/db2profile
```

NOTE	The *instance_owner_home_dir* is the name of the home directory for the owner of the db2 instance user account. In many cases this will be /home/db2inst1.

The examples in this document use the DB2 command environment.To start the DB2 command environment, type `db2` without arguments from a Linux shell:

```
$ db2

db2>
```

The DB2 command environment prompt replaces the command-line prompt. In the environment, you can run only DB2 commands.To exit the DB2 command environment, type **`quit`**, which returns you to the Linux shell.

The DB2 database provides online help, which displays either command summaries or error message descriptions. The following example shows the syntax of the online help facility.

```
? { command | errorMessageNumber }
```

The following command displays the restore command summary:

```
db2> ? restore
```

Regular maintenance – DB2

The following sections describe regular maintenance procedures.

Runstats

In Grid MP platform installations, the installer automatically installs a crontab entry under the db2 instance user account on the MP Console service machine that executes a runstats.sh script daily. This script located in /usr/local/UD/db/periodic/ will ensure that table statistics are updated on a regular basis to maintain optimal database performance.

Backup database for disaster recovery

United Devices highly recommends that you perform regular backups of your database. The following commands describe two ways to do backups. Consult with your DBA or United Devices Professional Services for help designing a backup and restore strategy.

You can run the following command when there are no connections to the database:

```
db2> backup database dbName TO dir/dev [ {,dir/dev} ... ]
```

When there are active connections to the database and database is in log recovery mode, you can run the following commands:

1. Set the DB2 configuration parameter to RECOVERY:

```
db2> update database manager configuration for dbname using
   logretain recovery;

db2> db2stop;

db2> db2start
```

NOTE Before stopping and starting the database, be sure to shut down the MP Services. See "Managing Services from the Command Line," on page 30 for instructions.

2. Run the backup database command:

```
backup database dbName ONLINE TO dir/dev [ {,dir/dev} ... ]
```

Restoring a DB2 database

To restore a database from offline backup files, enter a `restore` command that uses the syntax in the following example:

```
RESTORE DATABASE dbName: FROM dir/dev
   [ {,dir/dev} [TAKEN AT dateTime] [TO targetDirectory]
   [REPLACE EXISTING] [WITHOUT ROLLING FORWARD]
```

To restore a database from online backup files, enter a **restore** command and a **rollforward** command. The following example shows the syntax of the restore command:

```
RESTORE DATABASE dbName: FROM dir/dev
   [ {,dir/dev} [TAKEN AT dateTime] [TO targetDirectory]
   [REPLACE EXISTING]
```

The following example shows the syntax of the `rollforward` command:

```
ROLLFORWARD DATABASE dbName
   [TO {UTC | END OF LOGS [AND {COMPLETE | STOP}]
```

The following example shows a point-in-time restore using online backups and logs:

```
db2> restore database UDDB from /scsi/backups/online
   taken at 20011206163839 to /db/UDDB
   replace existing

db2> rollforward database UDDB to end of logs and complete
```

The following example shows a restore using offline backup:

```
db2> restore database UDDB from /scsi/backups/offline
   taken at 20011206163839 to /db/UDDB
   replace existing without rolling forward
```

Introduction to Oracle commands

This section introduces the basics of running and using Oracle commands.

To run Oracle commands you use the SQL*Plus interface. To run SQL*Plus you must set your environment variables, set your PATH for Oracle and have an Oracle user account/password.

To set your environment variable and PATH for Oracle, type the following:

```
export ORACLE_BASE=Oracle base directory
export ORACLE_HOME=Oracle base directory/product/9.2
export ORACLE_SID=uddb
export PATH
PATH=$PATH:$ORACLE_HOME/bin
```

NOTE In the above example, those items in italics should be replaced with your Oracle environment specific settings.

To start the SQL*Plus command environment, type `sqlplus` without arguments from a Unix shell or Windows command line:

```
$ sqlplus
```

SQL*Plus will then prompt you for your username and password.

Once the SQL*Plus prompt replaces the command-line prompt, you are in the SQL*Plus environment and you can run only SQL*Plus commands. To exit the SQL*Plus command environment, type **`exit`**, which returns you to the Unix shell or Windows command line.

Use the SQL*Plus environment to run sql queries, to start up and shut down your database, and to monitor and manage your database. For more information on SQL*Plus, review the SQL*Plus Quick Reference guide book from Oracle.

Regular maintenance - Oracle

The following sections describe the regular maintenance procedures of updating database statistics and backing up the database.

Database statistics

In Grid MP platform installations, the installer automatically installs a crontab entry under the root user account on the MP Console service machine that executes a runstats.pl script daily. This script located in /usr/local/UD/db/periodic ensures that table statistics are updated on a regular basis to maintain optimal database performance.

Physical Backups for disaster recovery

This installation by default is in NOARCHIVELOG mode, meaning that Oracle overwrites redo records without archiving them first. In NOARCHIVELOG mode, the whole database backup is recommended.

CAUTION If the database is in NOARCHIVELOG mode, never perform a whole database backup after an instance fails or is aborted. This backup is inconsistent and requires recovery to be made consistent, so unless the needed redo exists in the online redo logs and these logs are intact, the backup is unusable.

To make consistent whole-database backups

You must first guarantee that a database's datafiles are consistent by shutting down the database with the NORMAL, IMMEDIATE, or TRANSACTIONAL options before making a whole database backup. You can then run the following commands to take a cold database backup:

1. Get all files associated with the database and shutdown the database. Then run the following SQL*Plus commands:

```
sql> select name from v$controlfile
union
select  name from v$datafile
union
select  member from v$logfile;
sql> shutdown;
```

2. Get all configuration and password files:

```
ls $ORACLE_HOME/dbs/*
```

3. Get network files:

```
ls /var/opt/oracle/tnsname.ora
ls $ORACLE_HOME/network/admin/*.ora
```

Restoring an Oracle database

When a media failure occurs that damages datafiles, restore backups of the affected datafiles using operating system commands and then perform recovery with the SQL*Plus RECOVER command. You can either restore only some datafiles and perform recovery of the tablespaces containing the restored datafiles, or restore and recover the entire database. Keep careful records of your backups so that you know the original locations of the datafiles as well as the locations of the backups.

To begin media recovery operations when your database is running in `ARCHIVELOG` mode, use the SQL*Plus `RECOVER` command. The two basic types of media recovery are:

- Complete recovery

  In complete recovery, all redo generated on the database is applied.

- Incomplete recovery

  In incomplete recovery, not all the existing redo is applied. Incomplete recovery is only valid for restore and recovery of the entire database. A special procedure for performing incomplete recovery of an individual tablespace is called **tablespace point-in-time recovery (TSPITR)**.

Oracle's Restore and Recovery Methodology

The basic user-managed restore and recovery strategy is as follows:

1. Determine what you need to restore and recover.
2. Restore backups of files permanently damaged by media failure by using an operating system utility. If you cannot restore a datafile to its original location, then relocate the restored datafile and change the location in the control file.
3. Restore necessary archived redo log files with an operating system utility.
4. Recover the files by using the SQL*Plus `RECOVER` command.

NOTE Review the Oracle 9*i* User-Managed Backup and Recovery Guide for more in-depth instruction.

Appendix C: External Authentication Plug-ins for MGSI

This appendix is meant for advanced users who what to make the Grid MP platform authenticate against an external password system. This appendix contains information about the authentication plug-in and includes details about the Kerberos authentication plug-in.

Overview

Many corporations want to standardize on centralized single-sign-on (SSO) technologies in order to reduce the number of IT support requests for changing forgotten passwords. There are many solutions available for providing unified account management including:

- Microsoft ActiveDirectory (compatible with LDAP, Kerberos, and NTLM)
- Netegrity SiteMinder/IdentityMinder
- Novell NDS (compatible with LDAP)
- LDAP
- Kerberos
- NIS/YP

Additional types of authentication systems aim to provide more convenient or just higher level of security:

- X509 or SSL client-side certificate security
- RSA SecurID two-factor authentication
- thumbprint or other biometric authentication systems

Because of the variety of authentication schemes possible, an extensible plug-in architecture is implemented within the RPC CGI binary in order to reduce the complexity of adding support for each new authentication method in the future. This

method also allows for the possibility of implementing support for new authentication methods at the customer site by United Devices Professional Services.

Implementation

When the MGSI `login()` or `login2()` functions are invoked by SOAP or XML-RPC, the RPC CGI binary checks the /usr/local/UD/conf/ud.conf file for the existence of the `UD_MGSI_AUTH_ENGINE_PLUGIN` variable. If it is defined, then the named file is executed by the RPC CGI binary for the login attempt. If it is not defined, then the RPC binary reverts to normal behavior of checking the username and password against the Grid MP database.

When the RPC CGI binary (`rpc_xmlrpc.cgi` or `rpc_soap.cgi`) executes the authentication engine plug-in, it automatically supplies the two environment variables namely, `UD_MGSI_AUTH_ENGINE_USERNAME` and `UD_MGSI_AUTH_ENGINE_PASSWORD` to be the values of the two parameters that were originally passed to the MGSI `login()` function.

Plug-In Exit Scenarios

After the RPC CGI binary executes the authentication engine plug-in, it waits for the child process to exit or be signaled. If the plug-in exits with a non-zero exit code or terminates with a signal, an error condition is assumed and the MGSI `login()` function returns an exception to the caller. Successful exit of the plug-in is, therefore, indicated with exit code of zero, and optionally one or more special "notification lines" by means of STDOUT (see “Notification Messages” on page 129). If the exit code of the process is non-zero, the user is rejected.

The most common exit scenarios for the plug-in are listed below:

- Plug-in exits with non-zero. Exception is returned to caller and login is denied.
- Plug-in terminates with a signal. Exception is returned to caller and login is denied.
- Plug-in exits with any code, and supplies `exception=`*value*. Exception is returned to caller with the specified text and login is denied.
- Plug-in exits with zero. Originally supplied username is queried in database for the specific user and access is granted.
- Plug-in exits with zero, and supplies `username=`*value* to specify the actual user record. Access is granted.

- Plug-in exits with zero, and supplies `passhash=`*value* to indicate that the database record corresponding to the originally supplied username should be compared with the `passhash` value. Access is granted if they match.

- Plug-in exits with zero, and supplies `username=`*value* and `passhash=`*value*. Access is granted if the specified user record exists and the corresponding password field matches the `passhash` value.

- Plug-in exits with zero, and supplies `passthru=`*value*. Access is granted if the originally specified user record exists and the corresponding password field matches the SHA1 or MD5 of the originally specified password.

Notification Messages

The authentication script should return the `exception`, `debug`, and `passthru` messages depending on the username and password. All the notification lines have the format of "word=value" and must be printed to STDOUT followed by a newline.

The following table summarizes the accepted notification lines:

Table 7: Notification Lines

notification line	description
`exception=`*value*	The specified *value* is used as additional text within a custom exception that is returned to the caller. The presence of this notification line causes the login to fail, regardless of any other notification lines. When this line is specified, the exit code of the process is ignored.
`debug=`*value*	The specified *value* is used to write a debugging message to the syslog by means of the /var/log/ud.log file at the debug verbosity level.
`passthru=`*value*	The actual *value* specified after the equals sign is ignored. This notification line indicates that the plug-in chooses not to authenticate the specified user, but at the same time is also unwilling to refuse the user access. The RPC CGI should perform the standard username/password checks against the Grid MP database using the originally supplied username and password (this is similar to the `UD_MGSI_AUTH_ENGINE_PLUGIN` being disabled in the ud.conf file). Specifying this notification line causes the `username=`*value* and `passhash=`*value* lines to be ignored, if they are specified.
`username=`*value*	Indicates that the supplied username and password were accepted by the plug-in, but the corresponding Grid MP username should be the specified *value* instead. If no record exists in the Grid MP database for the *value* username, an exception is returned to the caller and the login fails.

Table 7: Notification Lines

notification line	description
`passhash=value`	This notification line indicates that the username was accepted by the plug-in. However, the RPC CGI binary needs to perform an additional case-insensitive equality comparison of the specified *value* with the password field from the Grid MP database, for the given user. No implied SHA1 or MD5 hashing operations are done against the specified value, so the plug-in should perform such hashing first if it is necessary for the comparison to succeed. If the username=*value* notification line is also specified then that username is used as the User record to retrieve. Possible uses for this notification line are schemes such as RSA SecurID two-factor authentication. The authentication plug-in splits the password into the two parts, validating that the numeric prefix portion of the password matches the expected SecurID value, and then returning the hash of the second portion of the password so that it can be verified against the Grid MP database.

Example authentication plug-in (Kerberos)

The authkerberos.sh script is the Kerberos authentication plug-in that allows external password checking against a Kerberos realm. The script simplifies password management by providing users the ability to use the same passwords as their user accounts in a Kerberos realm.

About the authkerberos.sh script

The authkerberos.sh script is a simple authentication plug-in written in shell script. When a user logs in and the Kerberos authentication rejects the password, the password will also be validated against the password stored in the MP Database by default. If you want to disallow this fallback password check and rely exclusively on the Kerberos realm for all password authentications, you may edit the authkerberos.sh script and change the `ALLOW_FALLBACK_PASSTHRU` line, which controls that behavior.

Example 1. authkerberos.sh script file

```
# Set this to 0 to disable fallback authentication against the
Grid MP password database if the Kerberos login attempt fails.
ALLOW_FALLBACK_PASSTHRU=0

# Check that the environment variables were set already.
if [ -z "$UD_MGSI_AUTH_ENGINE_USERNAME" ]; then
  echo "exception=Username not set."
  exit 1
fi
```

```
if [ -z "$UD_MGSI_AUTH_ENGINE_PASSWORD" ]; then
  echo "exception=Password not set."
  exit 1
fi

# Certain usernames should always validate against the database
# directly for performance reasons, and to avoid triggering
wasteful
# network accesses and Kerberos authentication errors.
LCUSERNAME=`echo "$UD_MGSI_AUTH_ENGINE_USERNAME" | tr A-Z a-z`
if [ "$LCUSERNAME" = 'mpadmin' ]; then
  echo "passthru=1"
  exit 0
fi

# Try logging into Kerberos with the password.
ERRTEXT=`echo "$UD_MGSI_AUTH_ENGINE_PASSWORD" | kinit
"$UD_MGSI_AUTH_ENGINE_USERNAME" 2>&1`
if [ $? -ne 0 ]; then
  if [ -z "$ALLOW_FALLBACK_PASSTHRU" -o
"$ALLOW_FALLBACK_PASSTHRU" -eq 0 ]; then
    # Kerberos login failed, so authoritatively decline the
login attempt.
    echo "exception=$ERRTEXT" | head -1
    exit 1
  else
    # Kerberos login failed, but allow standard Grid MP password
    # checks to be attempted.
    echo "debug=$ERRTEXT" | head -1
    echo "passthru=1"
    exit 0
  fi
fi

# Login was successful, so just discard the ticket and exit.
kdestroy 2>&1 >/dev/null
exit 0
```

Installing the authkerberos.sh script

Before attempting to install the authkerberos.sh script:

- Ensure that the script already exists at the following location: /usr/local/UD/inetpub/sw/bin/authkerberos.sh .

NOTE	The script is automatically installed by the Grid MP Installer. If the script does not exist in the mentioned directory, contact Professional Services.

- Configure your /etc/krb5.conf file with the settings that are appropriate for your Kerberos realm. Contact your network administrator, if needed.

  NOTE The /etc/krb5.conf file contains many case-sensitive values, therefore exercise prudence while editing the file to avoid mistakes.

- Verify that you are able to authenticate against the Kerberos realm by typing "kinit" and entering your password.

Perform the following steps to install the authkerberos.sh script:

1. Copy the authkerberos.sh script to a directory, such as /usr/local/UD/inetpub/sw/bin/.
2. Ensure that the above script file is marked so that it is executable. If needed, use the following command:

   `chmod +x /usr/local/UD/inetpub/sw/bin/authkerberos.sh`
3. Edit the /usr/local/UD/conf/ud.conf file and set `UD_MGSI_AUTH_ENGINE_PLUGIN` to be the fully-qualified filename of the script from above. For example

   `/usr/local/UD/inetpub/sw/bin/authkerberos.sh`

To enable Kerberos authentication against a Windows 2000 ActiveDirectory domain, ensure that your /etc/krb5.conf file lists "des-cbc-crc" for the encryption types, otherwise connections will be rejected. Example 2 shows a functioning /etc/krb5.conf file needed by Linux to authenticate against a Windows 2000 ActiveDirectory domain.

Example 2. /etc/krb5.conf file

```
[libdefaults]
        default_realm = UD.COM
        default_tkt_enctypes = des-cbc-crc des-cbc-crc
        default_tgs_enctypes = des-cbc-crc des-cbc-crc

[realms]
        UD.COM = {
                kdc = cwpads02.ud.com:88
                kdc = cwpads03.ud.com:88
                }

[domain_realm]
        ud.com = UD.COM
        .ud.com = UD.COM
```

NOTE Contact your network domain administrator to obtain the KDC addresses.

Accessing MP Console

Users may now log on to the MP Console or to MGSI using a password that is validated against the Kerberos realm. The MP Administrator must create a Grid MP User account in advance for any Kerberos user wanting to log in. The username for the Grid MP User account must match (case insensitively) the username in the Kerberos realm that will be used. The password given to the Grid MP User account can either be set to a random string, or it can be set to a backup password that will be used as failover.

The MPAdmin account is treated specially and is always checked against the Grid MP Database only. This check is performed to ensure MP Console availability and to ensure that a network outage to the Kerberos server does not prevent the administrator from being able to log into the system.

Index

O

P

R

S

T

U

W

System Administrator's Guide Feedback Form

Please give us your feedback about the *System Administrator's Guide*. Print this form, write your comments on it, and fax it to us at (512) 331-6235. Thank you for your feedback.

1. What operating system do you use?

   _____

2. What is your job title?

   _____

3. Please select the document for which you are providing feedback.

   _____ *Application Developer's Guide* _____ *Installation Guide*

   _____ *Application User's Quick Guide* _____ *System Administrator's Guide*

4. Have you used this document to look for explanations about Grid MP™ platform concepts and technology?
   ____Yes ____No

5. Have you used this document to perform a particular task?
   ____Yes ____No

   If yes, were the step-by-step procedures useful and accurate?
   ____Yes ____No

   If the step-by-step procedures were not useful and accurate, what problem(s) did you have with them?

   _____
   _____
   _____
   _____
   _____
   _____
   _____
   _____
   _____
   _____
   _____
   _____
   _____
   _____
   _____

6. Did you use the Table of Contents and/or the Index in this document?

   ____Table of Contents ____Index

   Were you able to find the information you were looking for?
   ____Yes ____No

   If you were looking for information that you could not find, please describe.

   _____
   _____
   _____
   _____
   _____
   _____
   _____
   _____

   Was the textual layout and design of this document useful and easy to navigate?
   ____Yes ____No

7. This document was delivered as an Adobe® .PDF file. Was this format useful?
   ____Yes ____No

   Did you print this document and consult the hardcopy?
   ____Yes ____No

8. Do you have general or specific comments about this document or suggestions about ways in which this document can be improved?

   _____
   _____
   _____
   _____
   _____
   _____
   _____
   _____
   _____
   _____
   _____
   _____
   _____
   _____
   _____