



SERVICE DESCRIPTION

Information Technology Systems & Services



MANAGEMENT SCIENCE ASSOCIATES, INC.
RockPointe Business Park
400 MSA Drive
Tarentum, Pennsylvania 15084-2808
TEL 724.265.6500 • FAX 724.265.5738

Table of Contents

1. REMOTE DATA PROTECTION SERVICE SUMMARY.....	1
1.1. DS-CLIENT APPLIANCE	2
1.2. CONTROL PROCESSOR	2
1.2.1. DS-Client Appliance SLA Monitor.....	2
1.3. REMOTE DATA PROTECTIONS DS-CLIENT APPLIANCE.....	3
1.3.1. Customer Network Interface.....	3
1.3.2. Remote Data Protection Client Software	3
1.3.3. Encryption Keys	4
1.3.4. Private Key.....	4
1.3.5. Account Key.....	4
1.4. DS-USER CONSOLE	5
1.5. REMOTE DATA PROTECTION SERVICE SETUP.....	5
2. REMOTE DATA PROTECTION OPERATIONS	6
2.1. BACKUPS	6
2.1.1. Backup Sets	6
2.1.2. Open File Backup.....	7
2.1.3. Backup Schedules.....	7
2.1.4. Monitoring Backups	8
2.1.5. Initial Data Collection.....	8
2.2. RESTORATION	8
2.3. ONLINE RESTORE	9
2.4. PORTABLE REMOTE DATA PROTECTION DISK RESTORE	9
2.5. REMOTE DATA PROTECTION DR SYSTEM RESTORE.....	10
2.6. SUPPORT AND ESCALATION PROCEDURE.....	10
2.7. DISASTER RECOVERY – HIGH PRIORITY	12

1. REMOTE DATA PROTECTION SERVICE SUMMARY

- Remote Data Protection provides an automated and unattended backup process ensuring that data held on PCs, file servers, laptops, and application/database servers is securely backed up and transferred offsite via the DS-Client Appliance.
- Backup data is transferred offsite to one of MSA's secure Data Centers via either a high performance dedicated leased line connection or basic existing internet connectivity. The MSA network can support leased line connection capacities of between xDSL and OC-192.
- Sophisticated data compression technologies, Global Single Instance Storage (sometimes called common file elimination) and delta blocking, maximize data transfer over the telecommunications connection.
- All data is AES encrypted at the customer site prior to transmission offsite and remains encrypted while at the vault.
- Encrypted data is held offsite in an encrypted format on a dedicated (or shared, as the case may be) RAID 5 disk sub-system which is in turn mirrored and backed up.
- Remote Data Protection provides an easy to use interface that simplifies the backup and recovery process and provides detailed information about scheduled operations.
- Centralized configuration of the Remote Data Protection Client software enables a network administrator/IT manager to specify exactly what data is to be backed up, ensuring investment is not wasted by backing up unauthorized or unnecessary information.
- A user definable number of backup versions of files are retained on disk, for immediate online restore.
- Backup data can easily be selected and restored online without the need to locate and identify backup tapes.
- Customers can perform regular online restores allowing them to test the integrity of their data at any time.
- MSA Technical Support is on 24x7 standby to support major data recovery by delivering requested backup data to the customer site.
- In the event of a major customer site disaster a portable storage media device is delivered to the customer site or to a specified disaster recovery site.
- MSA shall provide 24 hour/7 day a week Customer telephone support necessary to respond to mutually agreed upon services.

- Remote Data Protection Service Definition

Remote Data Protection is a unique alternative to traditional backup methods, replacing conventional tape based systems with a fully automated online solution. It provides agentless, centralized and automated backups of PCs, file servers, and application/database servers with secure offsite storage and immediate online restoration.

The system uses a DS-Client Appliance, installed onto the customer network, which hosts the Remote Data Protection Client application software that performs the backup and restore activity.

1.1. DS-Client Appliance

The Remote Data Protection Service is delivered through a suitably configured DS-Client Appliance, installed on the customer's network. The DS-Client Appliance configuration shall be determined by the specific requirements of each customer.

The key criteria in establishing the specification of the DS-Client Appliance are the size and scope of the customer network, the number of customer servers, the mix of applications and operating systems, and the quantity of data to be managed.

1.2. Control Processor

1.2.1. DS-Client Appliance SLA Monitor

MSA has an SLA Monitor for monitoring the DS-Client Appliance for use by customer personnel. It is HTML based and accessed from customer machines running TCP/IP and an appropriate Web browser.

The SLA Monitor graphical user interface (GUI) provides status information about the Remote Data Protection service [and reference information about MSA customer services.] The Remote Data Protection status report displays the current status of all Remote Data Protection backup activity. It includes information such as backup start and completion times, backup results, data backed up, and information on any open files that failed to back up.

The customer services section includes MSA's support guide and knowledge base, and a section on frequently asked questions, as well as corporate facts, site maps, and customer support details.

1.3. Remote Data Protections DS-Client Appliance

The Remote Data Protection DS-Client Appliance is self-contained processing units that assist in the delivery of the Remote Data Protection Service. They connect to the customer Local Area Network (LAN) and run the Remote Data Protection Client Software.

1.3.1. Customer Network Interface

Each DS-Client Appliance is connected directly to the customer 10/100 Ethernet, Gigabit Ethernet or 4/16 Token Ring Local Area Network (LAN) using a Category 5 cable. Remote Data Protection supports TCP/IP, NetBIOS, and IPX protocols

For the TCP/IP protocol the customer is responsible for providing an appropriate IP address. The DS-Client Appliance supports either static or DHCP addresses.

NetBIOS is self-configuring and requires no customer information or configuration actions.

Use of IPX requires the interface to be configured with the appropriate frame type and IPX network number. The customer is responsible for providing this information.

1.3.2. Remote Data Protection Client Software

The Remote Data Protection Client software runs on a DS-Client Appliance. It utilizes standard Microsoft Windows and Novell NetWare, NFS and SSH, or other networking resources (e.g. SQL Server APIs, Oracle APIs, etc.) to connect to the customer systems to be backed up and restored. To backup and restore Exchange and SQL servers, the Remote Data Protection Client Software uses standard Microsoft Application Processing Interfaces (API).

The Remote Data Protection Client Software is configured and operated using a separate DS-User Console software product called DS-User. The DS-User Console must be installed on one or more of the customer's systems (e.g. Windows 2000, 2003, XP, Linux RedHat, or Suse).

Depending on the customer network configuration, MSA may require the customer to set up appropriate permissions on any network resource requiring backup and restore capabilities.

Apart from the DS-User Console, no other Remote Data Protection software is installed on customer systems, making this an agentless solution that is particularly easy to deploy and support.

1.3.3. Encryption Keys

For the security of customer backup data, the Remote Data Protection Client Software within the DS-Client Appliance encrypts every file it sends with an encryption key provided by the customer. The files are stored and remain encrypted on the Remote Data Protection System at all times. The decryption process occurs during the restore operation of the backup data by the Remote Data Protection Client Software. This ensures that all backup data transferred and stored outside the customer location is always encrypted. The Remote Data Protection Client Software uses up to 256 AES encryption algorithm and can be configured with two encryption keys: Private and Account.

1.3.4. Private Key

The private key is the default; used by individual DS-Client Appliance to encrypt data before it is transmitted to the Remote Data Protection System at the MSA Data Center. Backup files that are unique to a DS-Client Appliance are encrypted using the DS-Client Appliance private key and stored in that DS-Client Appliance private library area on the Remote Data Protection System.

1.3.5. Account Key

For customers with more than one DS-Client Appliance, an account encryption key is also defined. The account key is used to encrypt customer files that are common to multiple DS-Client Appliances to the same Remote Data Protection System. These common backup files are encrypted with the account key and stored in the account library area on the Remote Data Protection System. DS-Client Appliance that shares a Remote Data Protection System must be configured with the same account key.

The Remote Data Protection System uses encryption cookies to verify every connection by the DS-Client Appliance. Cookies are a piece of code generated using the encryption key, but not the key itself. The DS-Client Appliance sends its cookie on every connection request, which the Remote Data Protection System compares with the original received during the initial DS-Client Appliance configuration. This verification process ensures

integrity of both private and account keys. After initial configuration the authentication between the DS-Client Appliance and the Remote Data Protection System is transparent.

Both private and account encryption keys can be up to 32 alpha/numeric characters and are configured during Remote Data Protection Client Software installation. Encryption keys are stored in the Registry in encrypted form, (note: and for Linux based DS-Clients in the DS-Client config file in encrypted form) so even if you have full access to the DS-Client Appliance (such as MSA Customer Support) they cannot be read. Intentional or unintentional changes to the encryption keys shall make data stored on the Remote Data Protection System unusable.

It is the responsibility of the customer to supply appropriate values for the private and account encryption keys. These values once entered shall not be required again except in the case of a bare metal restore or a disaster recovery situation where the DS-Client Appliance must be re-configured.

IMPORTANT: The customer is responsible for storing their original encryption keys in a secure location. Loss of the keys shall prevent recovery of the DS-Client Appliance and the customer's backup data. MSA has no knowledge of the customer's encryption keys and no method nor manner to recover them.

1.4. DS-User Console

The DS-User Console is the GUI for the Remote Data Protection Client Software and is operated by the customer network administrator to define backup sets and schedules, monitor backups and perform restores.

The DS-User Console must be installed on one or more of the customers Windows 2000, 2003, XP, or Linux systems.

DS-User Console access is integrated into Windows and Unix networking security. Individual user accounts, or groups of users, can be defined and granted authority to perform different levels of Remote Data Protection Service functions.

1.5. Remote Data Protection Service Setup

The Remote Data Protection software may be setup by the Customer. If the Customer prefers MSA to perform the setup, MSA shall arrange a convenient time to perform the installation and configuration of the DS-Client Appliance. Once the DS-Client Appliance has been installed, MSA shall work with the customer to configure the Remote Data Protection

Client Software. This shall involve configuration of the Remote Data Protection Client Software settings, definition of the customers' encryption keys, installation of the DS-User Console software and demonstration of the Remote Data Protection functionality.

Eight (8) hours of telephone support and/or training for this initial configuration is included within the standard Remote Data Protection Service offering. The customer can purchase additional telephone and/or onsite support at a fixed daily rate.

2. REMOTE DATA PROTECTION OPERATIONS

All Remote Data Protection operations are performed using the DS-User Console. Authority to perform Remote Data Protection operations can be controlled by defining access to authorized users or groups of users, thus preventing backup and restoration of data by unauthorized personnel.

2.1. Backups

Remote Data Protection backups are based on backup sets that define the scope of the backup operation to be performed. Backup sets are executed to perform the specified backup operation and can be executed manually or scheduled automatically.

2.1.1. Backup Sets

A backup set defines the files or databases that are to be backed up. They can include or exclude files or databases by directories or by filtering the file type. This allows the customer administrator to define backup sets that meet precisely the customer's requirements, thus eliminating the backup of unnecessary data.

In addition, these backup sets define the number of retained generations, or versions, of files and databases backed up. This enables the customer to selectively restore any of the previous versions of files that have been backed up. The default number of generations is set during installation.

Multiple backup sets can be defined for the same customer system. This feature enables the customer to define separate backups of different types of data on the same system. Multiple backup sets for the same system can also be actioned independently.

A backup set can only include data from a single customer system; one or more backup sets must be defined for each system to be backed up.

Backup sets are defined in a similar manner for Microsoft Windows, Novell NetWare, and Unix file systems and for backups of Microsoft Exchange and SQL Server. This single interface enables efficient administration of the Remote Data Protection Service.

Authorized administrators can manually execute ad-hoc backups, however, the normal method shall be to schedule automatic execution of the backup sets.

2.1.2. Open File Backup

By default, Remote Data Protection shall attempt to backup files that are opened, but not locked, by other applications on the customer system. The customer administrator can further configure this functionality, either globally or by individual backup set, to define the method for handling open files and the number of backup re-tries to perform. The DS-User Console provides comprehensive online help information for defining these options.

Files that are completely locked by another application, such as Microsoft Outlook PST files, shall not be backed up, but the DS-Client Appliance Client Software can work with any third party Open File Manager product (e.g. File Access Manager from VisionWorks Solutions Inc) to back up these locked files. The Message Level Restore (MLR) plug-in shall back up locked PST files.

All open files that fail to backup are reported in the activity log on the DS-User Console and in the Remote Data Protection status report provided by the DS-Client Appliance web portal interface.

2.1.3. Backup Schedules

Remote Data Protection has an extensive calendar based scheduler for automatically executing backup sets. Schedules can be defined to execute backups daily, weekly, monthly, or on a randomly defined frequency.

Multiple schedules can be defined and multiple backup sets can be associated with a schedule. Where multiple backup sets are associated to a schedule, the customer administrator can define the number of concurrent backup sets to be executed and the priority in which they should be executed.

The DS-User Console provides a graphical view of the backup schedules. This allows the customer network administrator to

quickly view the status of the backups and identify any conflicting or overlapping schedules.

2.1.4. Monitoring Backups

In addition to the DS-User Console, a web based interface from the DS-Client Appliance presents daily management reports on the status of the Remote Data Protection Service. This web interface includes a summary of scheduled backups, highlights of any errors that may have occurred, and statistical information detailing the quantity of data backed up.

The DS-User Console provides extensive monitoring and reporting capabilities for customer administrators. This includes detailed logs of backup activity, details of all files backed up, error reports, and audit trails for all backup and restore activity.

2.1.5. Initial Data Collection

The primary method of backup is over the Internet between the DS-Client Appliance and the Remote Data Protection System at MSA's Data Center. However, in situations where the initial backup volume is such that a network transfer is impractical, MSA shall collect and transport it to the Data Center.

Where it is appropriate for MSA to manually transport the initial backup data, the process shall involve removable/portable hard-disk location on the customer premises and connecting it to the software within the DS-Client Appliance, via a private LAN connection. Initial backups are performed to this removable/portable hard-disk location until an agreed time when the removable/portable hard-disk device is disconnected from the LAN and transported back to the Data Center. Once at the Data Center, the data residing on the portable hard-disk device is imported into the Remote Data Protection System and incremental backups between the Remote Data Protection System and the DS-Client Appliance can occur on a regular basis (either scheduled or on-demand).

2.2. Restoration

The DS-User Console allows the authorized customer network administrator to quickly and easily select and restore data. Data can be restored to a remote system, for example, the administrator could use their desktop machine to restore data to a remote server.

There are several different methods in which data can be restored. The first is online where data is restored across the Internet. The second is where the restore data is delivered via a portable Remote Data Protection disk. The third is to restore a copy of the latest version of a file from a local storage location.

MSA divides restore operations into three categories that represent the scale of the recovery.

The following table maps these restore categories to the three methods of data restoration.

Restore category	Example	Volume of customer data	Restore method	Time to Restore (hours)
1	Moderate Data Loss Single/small number of files; small/medium server	1 MB - 20 GB	Online Restore	0 - 12
2	Major Data Loss Major database server or multiple servers	20 GB - 100 GB	Portable Disk Restore	6 - 12
3	Disaster Recovery Multiple server loss or complete site	100 GB +	DR System Restore	8 - 24

2.3. Online Restore

The primary method of data restoration is online. The DS-User Console provides a Restore Wizard that guides the customer administrator through the process of selecting and restoring data. The Restore Wizard allows the administrator to search and select files for restore, select the version of the files and choose the target destination for delivery. Customers can be given a granular permission to restore their own data.

Having selected the data to be restored, the Remote Data Protection Client Software delivers it across the Internet from the Remote Data Protection System at the MSA Data Center. The Remote Data Protection Client Software then delivers the data to the specified system on the customer network. As part of the operation all associated security permissions for the data are also restored.

2.4. Portable Remote Data Protection Disk Restore

For larger quantities of data, the customer administrator can invoke the Disaster Recovery Wizard to request that a copy of the backup data be copied to a portable Remote Data Protection disk.

The Disaster Recovery Wizard provides the same level of restore granularity as the Restore Wizard, but rather than restoring the data across the network it is copied to a portable Remote Data Protection disk, which is then transported to the customer site. The customer network administrator can then use the DS-User Console to restore the requested data directly from the DS-Client Appliance to the system being restored.

The only data that can be restored from the portable Remote Data Protection disk is that which was specified when initially requested. If additional backup data is required then this can be restored either online or by a new request for a portable Remote Data Protection disk being initiated.

2.5. Remote Data Protection DR System Restore

The third restore option is to request a portable Remote Data Protection System. This could be used as an alternative to the portable Remote Data Protection disk or in a major disaster situation where complete backup data is required.

MSA shall deliver the portable Remote Data Protection DR System to either the customer's site or an alternate disaster recovery location. The portable Remote Data Protection DR System is then connected to the customer's or a replacement DS-Client Appliance via a private LAN connection. Data can then be restored in the same way as for an online restore but with the performance benefit of the portable Remote Data Protection DR System being on an internal DS-Client Appliance LAN.

IMPORTANT: The customer's DS-Client Appliance Client Software and encryption key(s) must be made available for data to be successfully restored.

2.6. Support and Escalation Procedure

<p><u>Priority 3 (Low)</u></p> <p>Classification: General inquiry or problem which has no operational impact on the customer system.</p> <p>Call Logging: 08:00 to 18:00 hrs weekdays</p> <p>Time to Resolve: 48-72 hours</p>	<p><u>Typical Event:</u></p> <ul style="list-style-type: none"> ▪ Billing or documentation query ▪ Request to move or re-deploy services ▪ General product/functionality inquiry ▪ Report generation issues ▪ General advice and guidance ▪ Product/service enhancements <p>Logged calls shall be serviced on a first-come-first served basis and typically resolved within one day.</p>
<p><u>Priority 2 (Medium)</u></p> <p>Classification: Customer or MSA have identified a possible error or fault with the installed MSA service but which has no critical effect on any other part of the service.</p> <p>Call Logging: 24hr x 7 day x 365 days</p> <p>Time to Resolve: 24-48 hours</p>	<p><u>Typical Event:</u></p> <ul style="list-style-type: none"> ▪ Previously installed and working Remote Data Protection software now not functioning correctly ▪ Problem backing up a single customer system <p>If logged during business day (08:00 – 18:00 hrs. Monday to Friday) and an immediate resolution is not available the call shall receive attention during the next business day.</p>
<p><u>Priority 1 (High)</u></p> <p>Classification: Customer or MSA have identified a possible error or fault with the installed MSA service which is affecting multiple customer clients or causing severe impact to system operations.</p> <p>Call Logging: 24hr x 7 day x 365 days</p> <p>Time to Resolve: 0-24 hours</p>	<p><u>Typical Event:</u></p> <ul style="list-style-type: none"> ▪ Escalation of Priority 2 call ▪ MSA remotely monitored fault on leased line ▪ Customer unable to restore data ▪ Customer experiencing MSA related problems backing up from multiple systems <p>Call referred immediately to the MSA Project Manager who shall become the primary point of contact and coordinate recovery actions.</p> <p>If problem requires onsite technical support this shall be scheduled with Customer.</p> <p>Every 3 hours MSA management shall review the situation and the MSA Project Manager shall provide a status report to the Customer.</p>

Some calls may require further investigation and even internal escalation by technical specialists. Although MSA shall aim to resolve an open call in the shortest possible timeframe, this may, in some cases depend on the availability of diagnostic information from the Customer. In this case MSA shall monitor events at every stage throughout the diagnostic process and keep the Customer informed of progress.

In many cases MSA’s operations staff, through their service monitoring systems, shall be aware of problems before they are logged by Customer. In these cases the operations staff shall call the assigned Customer authorized representative to arrange the necessary remedial action.

Any investigative work carried out by MSA personnel on a fault that is found not to be the responsibility of MSA shall incur charges, with a minimum billable charge of \$250. Should travel and accommodation be involved, this shall also be charged at cost to Customer.

2.7. Disaster Recovery – High Priority

<p><u>Disaster Recovery (High)</u></p> <p>Classification: Customer invokes an onsite disaster recovery.</p> <p>Call Logging: 24hr x 7 day x 365 days</p> <p>Time to Resolve: Problem determination shall start immediately and a recovery plan shall be proposed to Customer depending on the exact nature, location and scale of the problem. Problem resolution activity shall be maintained on a 24 hour basis until the problem is resolved.</p>	<p><u>Typical Event:</u></p> <ul style="list-style-type: none"> ▪ Major data loss ▪ Loss of entire customer site ▪ Scheduled disaster recovery test <p>Call referred immediately to the Customer representative who shall become the primary point of contact and coordinate the following actions:</p> <ul style="list-style-type: none"> ▪ Notify all relevant members of the MSA management ▪ Review of any previous call history ▪ Interrogation of database and remote diagnostic support systems ▪ Implement repair/replacement/Technical Support Staff procedure ▪ Arrange arrival onsite of MSA Technical Support, if applicable ▪ Feedback problem status updates to Customer on a regular basis ▪ Contact Customer to confirm successful resolution <p>If a problem requires an onsite technical visit, this shall be scheduled with the Customer.</p>
--	---