Macrium Site Manager 8

Macrium Site Manager User Guide

Version: 2

Date: 15 June 2022

Macrium Site Manager User Guide

Search

This guide describes the capabilities of Macrium Site Manager 8, and provides information on how to use it to configure and use Site Manager.

There are a number of sections to this guide, covering all areas from installation and use through to troubleshooting and integration with other products. The sections available are:

- Introduction to Site Manager - general overview of Site Manager, showing the basic concepts and elements involved
- Interface Overview - introduces the basics of accessing and getting started with Site Manager
- Installation and Update - how to install Site Manager and how to keep it up to date, including system requirements
- Licensing - how the licensing model works, what licensing is required and how to update licenses
- Configuration and Security - an overview of how security and networking is managed in Site Manager and the different configuration options available
- Scheduling Centrally Managed Backups - how to set up or modify a set of scheduled network backups in Site Manager
- Monitoring and Management Tools - how to use Site Manager to monitor scheduled backups and be notified about important events
- Managing and Restoring Backups - how to access backup files or restore computers from backup
- Troubleshooting and Advanced Guides - a set of troubleshooting guides covering common areas and problems encountered with Site Manager

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Introduction to Site Manager

Overview

Site Manager enables backup, restore and monitoring of multiple networked computers running Macrium Reflect technology. The Site Manager server is installed as a Windows service on a server computer and may be accessed using a web browser user interface. Supported browsers are Google Chrome, Firefox, Microsoft Edge and IE 11.

A **Macrium Agent** is installed on each remote computer which then communicates via TCP/IP to a single installed instance of the **Macrium Site Manager Server.** This service also exposes an HTTP/HTTPS server service on a configurable port which enables web browser sessions to manage the **Macrium Agent** installed computers.

The Site Manager Server service can be installed on any single networked PC or Server. Both Domain and Workgroup networks are supported.

Requirements and Installation

The **Macrium Site Manager** server can be installed on all Windows operating system from Windows 7 and later, 32 or 64 bit.

The Agent which runs on managed computers can be installed on any Windows operating system from Windows XP Service Pack 3 onwards.

A detailed installation guide for the server is available here. Agent computers can be installed through the server either automatically or through manual install. More details on this process are available here.

Site Manager 8 - New Features

Site Manager 8 is now available - this release contains a lot of new features and improvements, with some of the highlights shown below

- Upgrade To Macrium Reflect 8 Backup Engine
- New Computer Management Tools
    - Redesigned Computers Page
    - Groups and Tags
    - Backup by Tag
- Intra-daily Backups
    - Intra-daily Scheduling
    - Streamlined Logs
- Improved Restore/Recovery Tools
    - Universal Rescue Media

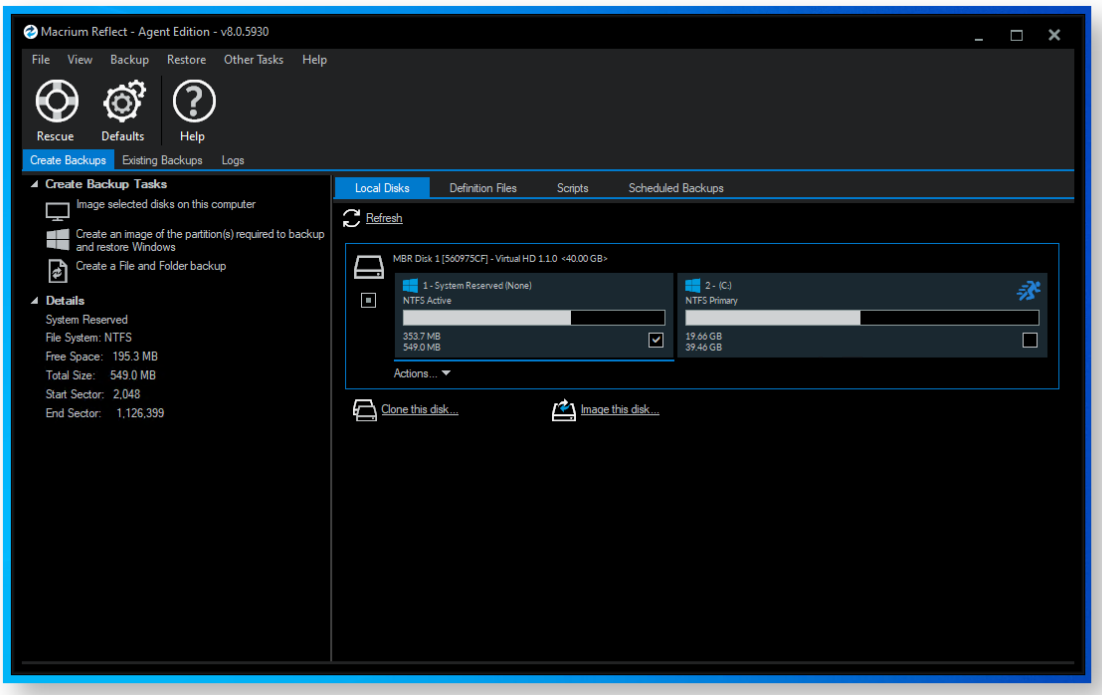
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

- USB Creation Tool
- Improved Active Directory Integration
- Sync Repositories to Amazon S3
- Daily Data Export

There are many other bug fixes and improvements, a full list is shown in the Release Notes

Upgrade To Macrium Reflect 8 Backup Engine

At it's core, Site Manager 8 uses Macrium Reflect 8 technology to provide image and file based backups. This release brings in all the improvements and new features available in Reflect 8



A full list of the new features of Reflect 8 can be found in the Reflect 8 Knowledgebase - New in Version 8.0

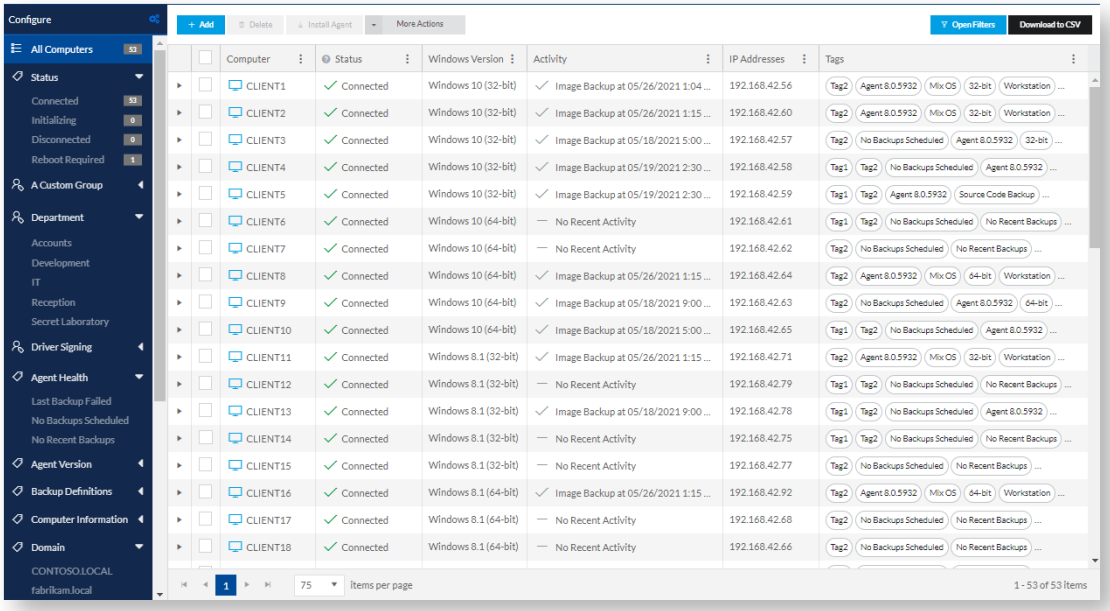
New Computer Management Tools

Redesigned Computers Page

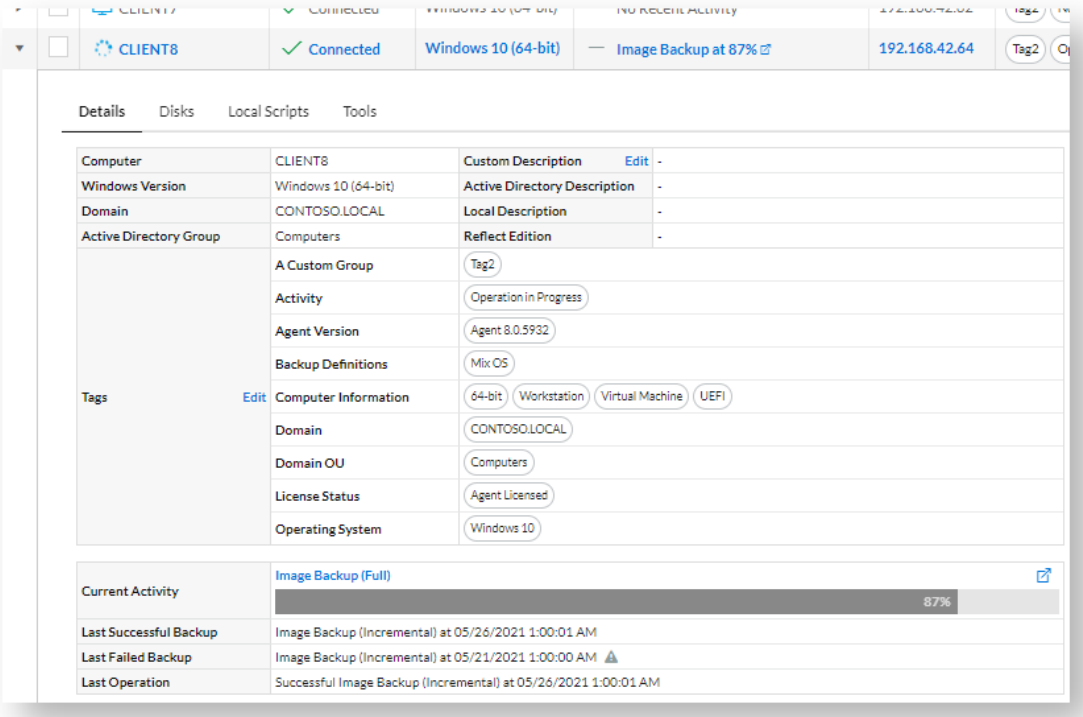
The Computers page itself has undergone a full redesign, improving performance, readability and function.

Additional information has been provided for each computer to help locate and identify problems in backup scheduling.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



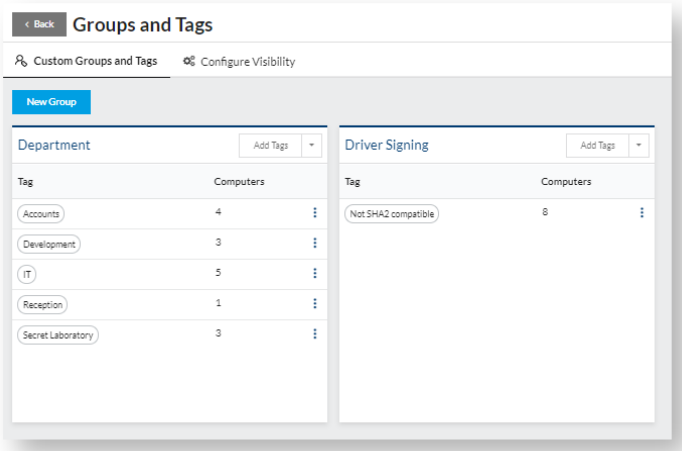
More detail has been added to individual computer rows when expanded, to make it easier to identify computers, configuration and backup problems.

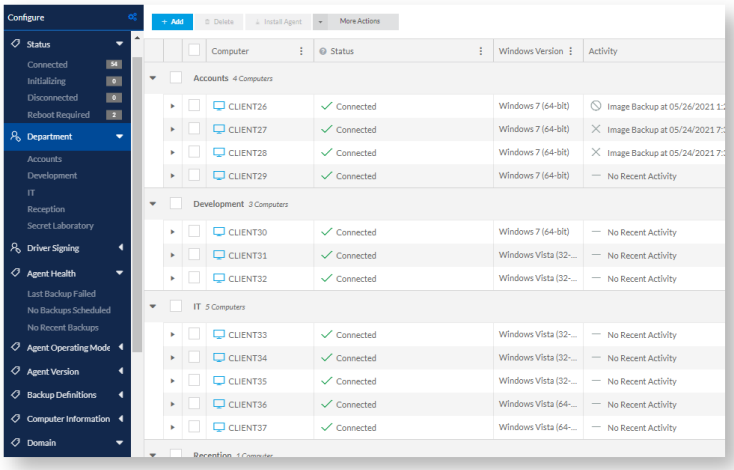


Groups and Tags

Computers can now be tagged and sorted into groups, giving the ability to break the computers page down into groups and dynamically filter it

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

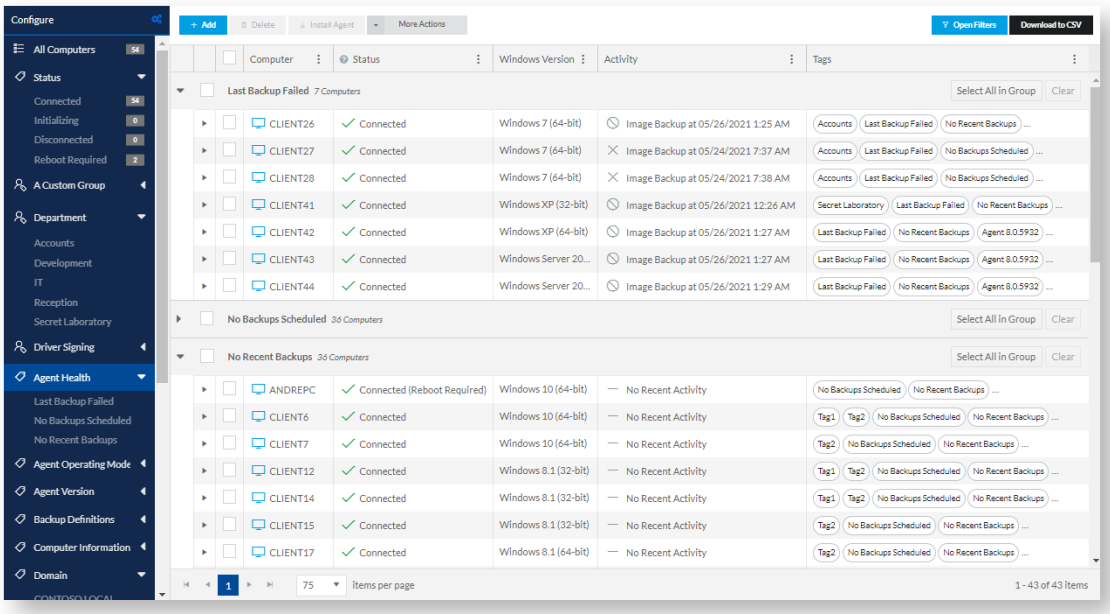




Tags are also created automatically for some data including:

- Computer Status, OS and Agent version
- Backup Definition membership
- Active Directory information
- Last backup failures

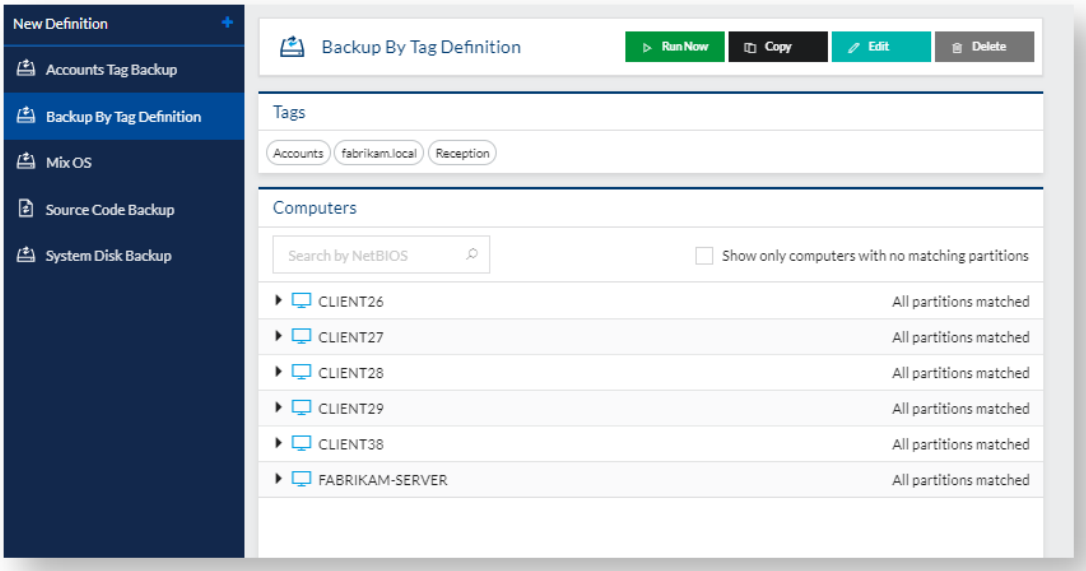
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



See Groups and Tags for detailed information.

Backup by Tag

Backup Definitions can now be based on tags - these backup definitions will update automatically as computers are tagged or lose tags



This makes managing large groups of computers easier - just add a tag to the computer and it will automatically be pulled into backup scheduling. This includes tags based on Active Directory domain group information, allowing changes in AD to automatically update backup schedules.

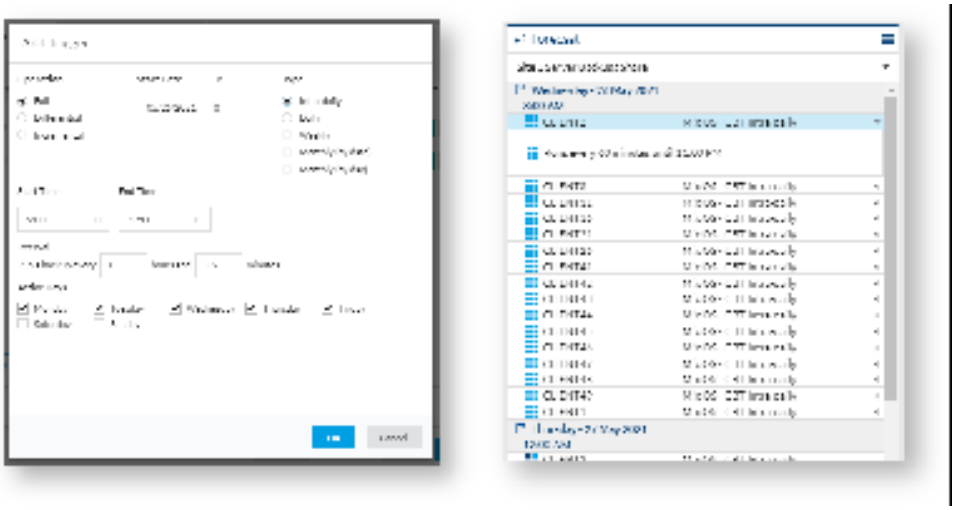
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Intra-daily Backups

Reflect 8 introduced Intra-daily backups (see Reflect 8 Knowledgebase for more information), with additional tools to reduce the amount of messaging and logs around successful backups. Site Manager 8 contains the same tools and technology.

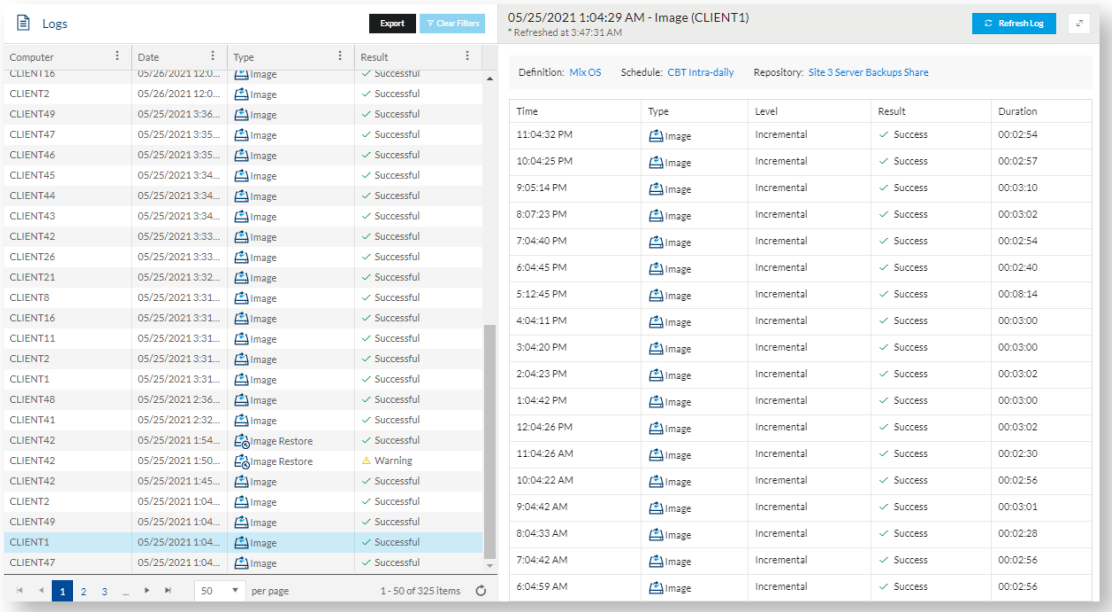
Intra-daily Scheduling

Scheduled backups can now run as frequently as every 15 minutes in a time window.



Streamlined Logs

As frequent intra-daily backups could cause a large number of notifications, logs and UI messages, a 'stealth mode' option has been added - it can be enabled on a per-schedule basis, and when it's in use, intra-daily backups that succeed don't report full backup logs. For these backups, the log view will show a daily summary table of intra-daily backups for each Agent.

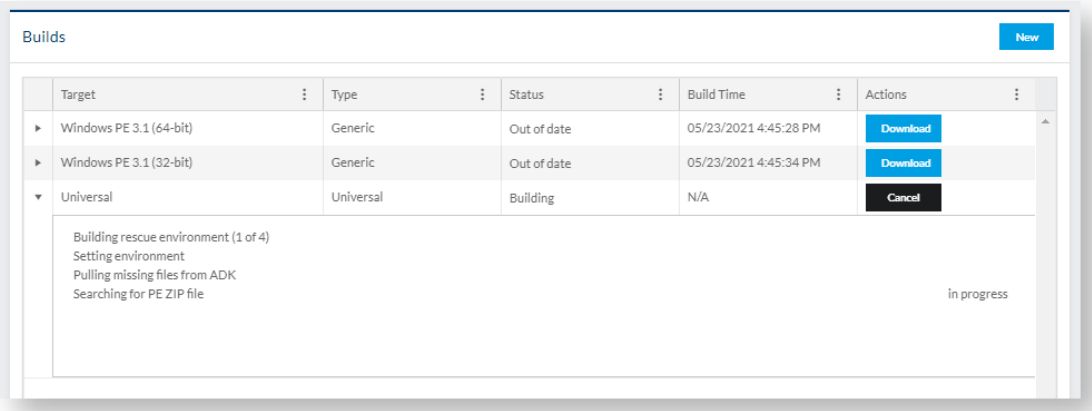


Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

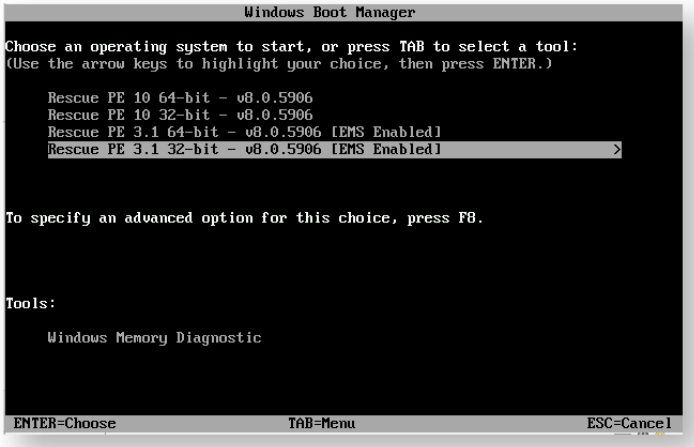
Improved Restore/Recovery Tools

Universal Rescue Media

Site Manager 7 has the ability to create Rescue Media - either for specific Agents or for a version of PE. This has been extended in Site Manager 8 with universal Rescue Media - this is a build of Rescue Media which contains all 4 PE versions and architecture combinations available in Site Manager, along with all drivers and static IP information for every Agent in Site Manager.



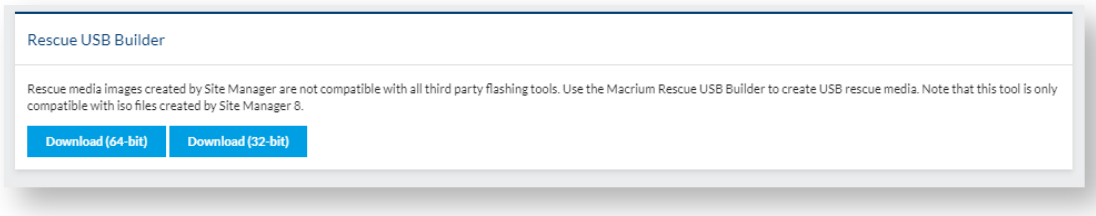
On booting from a universal Rescue Media ISO image, DVD or USB stick, the different PE environments are available in a boot menu



USB Creation Tool

Site Manager produces ISO DVD image files for Rescue Media as the web interface means that it can't access any DVD drives or USB sticks attached to the computer. This has meant that it's been necessary to use third-party software to turn this ISO file into a bootable USB stick. Site Manager 8 provides a downloadable command-line utility for creating Rescue Media USB sticks from ISO images.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



Once downloaded, the command line utility can be used to discover available USB drives and create Rescue Media with them

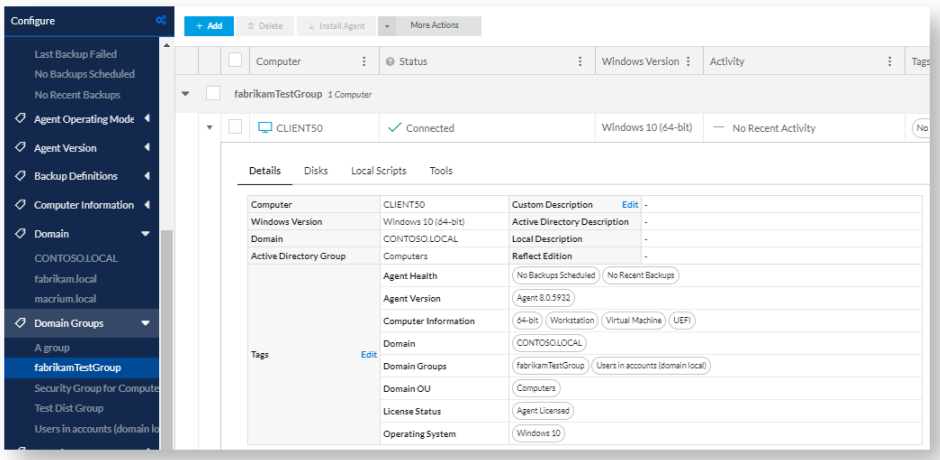
```
c:\tmp>RescueUsbBuilder_x64.exe --list
Title         : Removable USB Flash Drive
Name          : SanDisk Cruzer Blade USB Device
Device Number : 3
Description   : SanDiskCruzer Blade - H: MACRIUM_PE - 28.65 GB
Manufacturer  : (Standard disk drives)

c:\tmp>RescueUsbBuilder_x64.exe --create --iso universal.iso --device 3
Title         : Removable USB Flash Drive
Name          : SanDisk Cruzer Blade USB Device
Device Number : 3
Description   : SanDiskCruzer Blade - H: MACRIUM_PE - 28.65 GB
Manufacturer  : (Standard disk drives)
Device contents will be overwritten, continue (Y/N)? y
Creating rescue usb

Finding target volume
Copying files to device: 100%
Rescue USB created.
```

Improved Active Directory Integration

As part of the computers page improvements, Site Manager 8 has additional Active Directory information available.

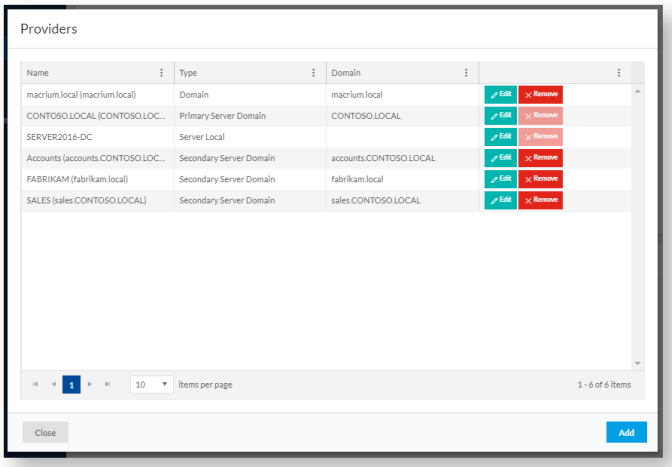
Agents now automatically send information on their Active Directory description and membership in any groups (OU, security and distribution groups across the whole AD forest) to the Site Manager server. These are displayed as tags in the computers page

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



These tags can be used to sort, filter and include computers in Backup Definitions. If the group membership is changed in AD, the Agent will detect this and update the Site Manager server.

All domains in the Active Directory forest visible to the Site Manager server are now added as login providers automatically as 'Secondary Server Domains'



When logging in, all groups permissions are now resolved across the whole forest - so a user in Domain A can be allowed access to Site Manager based on a group permission in Domain B.

Sync Repositories to Amazon S3

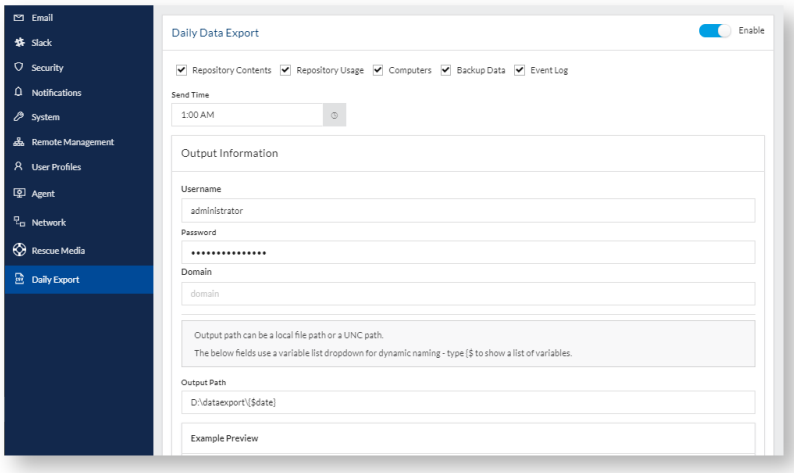
In addition to the existing FTP and network drive Repository synchronization available, Site Manager 8 has added sync to S3 compatible stores to help in replicating backup data into the cloud.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Amazon, Wasabi and Backblaze configurations are provided, but any S3 compatible store can be configured. See Remote Synchronization with Amazon S3 or Other Compatible Stores for more information.

Daily Data Export

To assist in custom scripting, ingesting Site Manager information into custom/third-party systems or auditing, Site Manager 8 now offers a daily CSV export of data which can be configured in **Settings**.



Upgrading From Site Manager 7 to 8

- Introduction
- Licensing Changes
    - Agent Licenses
    - Standalone Licenses
    - Metered Licenses
    - Staying with Version 7

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

- The Upgrade Wizard
- Upgrading in an Offline Environment

Introduction

With the introduction to Macrium Site Manager 8, existing version 7 license keys must be upgraded to version 8 to be recognized in Site Manager 8. This article covers the changes to licensing and how to perform an upgrade to Site Manager 8.

Licensing Changes

In Site Manager 8, any licenses must be version 8 licenses. Older licenses can be upgraded in version 7 Site Manager prior to update through the licenses page. When upgrading from version 7 to version 8, a wizard will guide you through the process of upgrading licenses as needed. In addition, licenses can be upgraded in Site Manager 7 ahead of the upgrade.

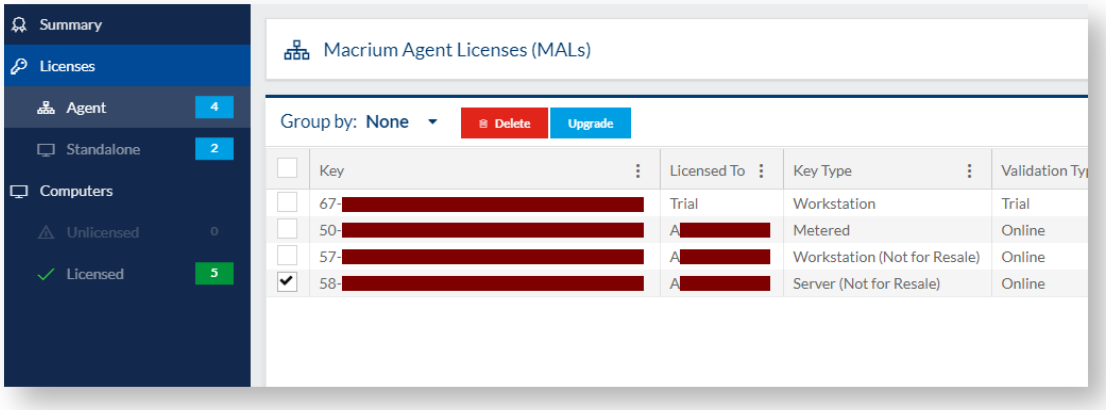
Agent Licenses

If an Agent license has active support, it will qualify for a free upgrade to version 8. If it is out of service, renewing the service on the key will allow it to be upgraded. See the Macrium Website for more details.

Any trial keys are also eligible for upgrade.

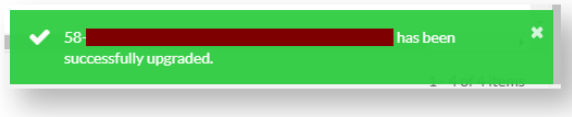
> License upgrade functionality will only be enabled when the Site Manager 8 release is available, as shown in the **About** page.

To a upgrade a key outside the version 8 upgrade wizard, the Licenses page has an upgrade option for Agent licenses:



If a single license is selected, the **Upgrade** button can be clicked and the Site Manager server will attempt to upgrade the license. The upgrade status will appear as a notification

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



A license must be in the valid state to be upgraded. An internet connection is required to perform key upgrades.

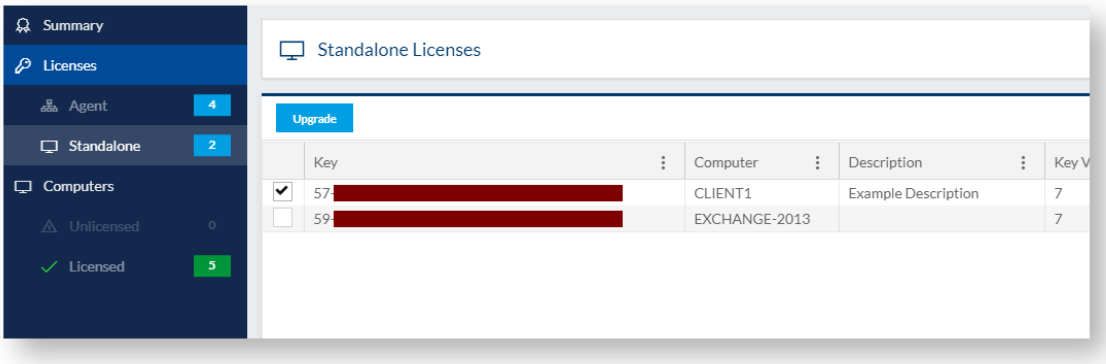
Keys can be upgraded for offline use at the Macrium Upgrade and Renewal Wizard

Standalone Licenses

As with Agent licenses, standalone Reflect licenses must be version 8 to be valid for Site Manager 8. Any version 7 keys will be marked as invalid and the Site Manager will require an Agent license for that Agent. Keys may be upgraded in the **Licenses Standalone** section of Site Manager. To be able to update a standalone key, the following conditions must be true:

- The key is a version 7 key
- The Agent is in the connected state
- The Agent version is at least 7.3.5920
- The standalone Reflect version is at least 7.3.5854

If a license is eligible for upgrade, the upgrade button will be live when selecting the license key;



Metered Licenses

Metered license keys are always considered the latest version - existing metered license keys will be detected as version 8 keys and no action need be taken to upgrade them.

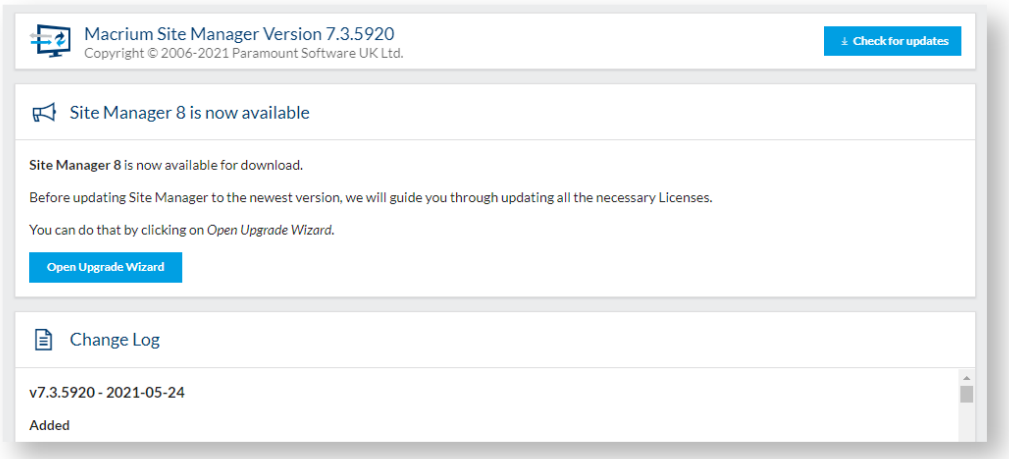
Staying with Version 7

If you do not wish to upgrade to version 8, Version 7 will remain supported and receiving bug fixes, which will be delivered via the normal upgrade mechanism. Site Manager 7.3.5920 and greater can accept version 8 keys as Agent and standalone keys.

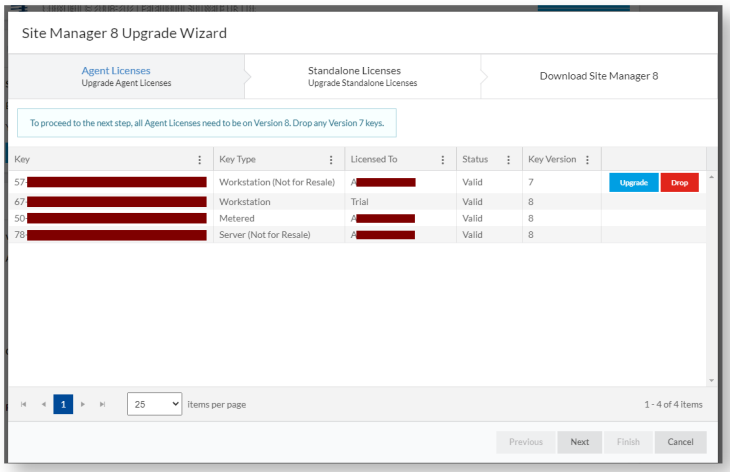
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

The Upgrade Wizard

When Site Manager 8 is released, Site Manager 7 will generate a notification that the release is ready and the **About** page of Site Manager will have the option to perform an upgrade



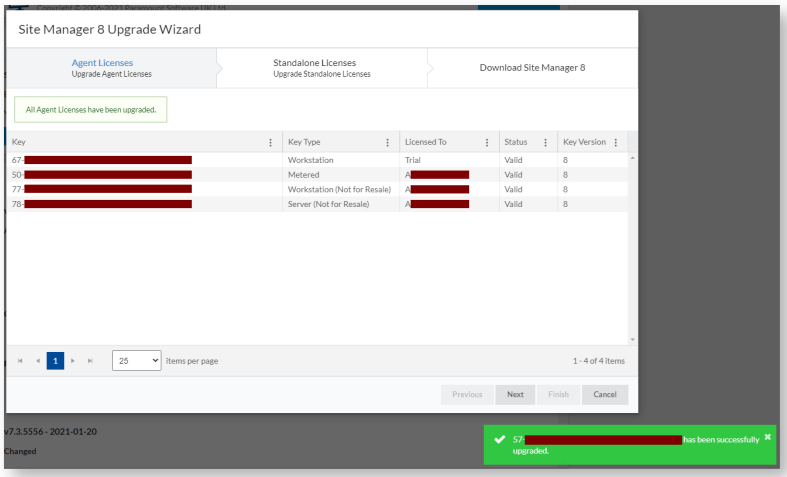
Clicking **Open Upgrade Wizard** will open the wizard to upgrade all licenses and start the upgrade process



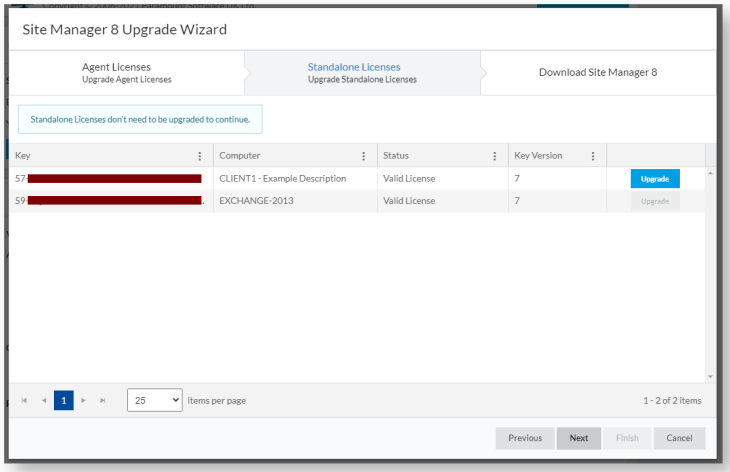
In the first stage, Agent licenses must be upgraded - any version 7 licenses must be upgraded or dropped to continue.

Once each license is upgraded or dropped, the UI will indicate that all licenses are valid and allow you to continue to the next stage

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

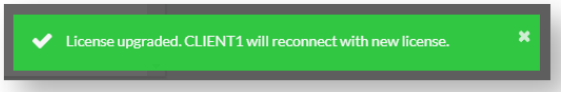


The next stage allows the optional upgrading of version 7 standalone Reflect licenses



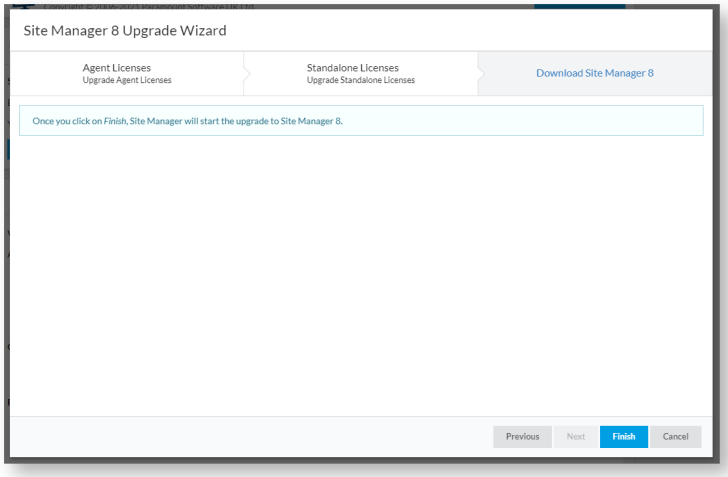
Here you may choose to upgrade standalone licenses - standalone licenses are not valid for use in Site Manager 8 and any version 7 licensed Agent will require an additional Agent license to operate.

Upgrading a standalone license will cause the Agent to reconnect with the upgraded license:

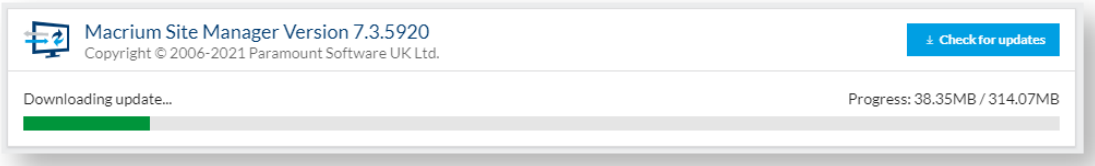


Once you click on next, the final page is displayed:

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



Clicking **Finish** here will close the wizard, start the download of the Site Manager 8 installer and upgrade the Site Manager



Upgrading in an Offline Environment

In an offline installation of Site Manager, the online upgrade tools and wizard won't work as they require an internet connection. In this case, the following procedure should be followed:

1. Visit the Macrium Upgrade and Renewal Wizard website to upgrade keys as needed
2. In your Site Manager, add the newly upgraded Agent keys
3. Remove the old version 7 keys
4. Upgrade any standalone Reflect installations on the Reflect computer directly
5. Download the Site Manager 8 installer and run on the server. This will perform an upgrade install

Release Notes

Site Manager 8 Release Notes

8.0.6503 - 2022-01-12

Added

- Added Windows Server 2022 version to Computers page display.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

- Added support for proxy servers to MultiSite connection (HTTP/S with CONNECT or SOCKS)

Changed

- Update Agent backup engine to Macrium Reflect 8 version 8.0.6392. See here for details
- Improved the MultiSite Remote View connection to be faster and more reliable
- Added TCP keepalives to Agent connections to improve behaviour when connecting via NAT routing or firewall
- Added re-evaluation of any Agent user scripts before connection and on hardware/IP change to facilitate VPN detection

Fixed

- Fixed extensive startup delays for clients with 50+ inaccessible domain providers.
- Fixed crash dump cleanup code not removing some old crash dumps
- Fixed unusual crash on startup when Windows takes over 10 seconds to bind a listen socket during Windows startup
- Fixed bug causing multiple event log events when an Agent with an active backup disconnects
- Fixed MultiSite Remote View of the licenses page not working

8.0.6305 - 2021-11-01

Added

- Added "Reset VSS" feature to *Computers* page under the *Tools* tab for each computer. This can be used to restart and repair VSS on the remote computer.

Changed

- Update Agent backup engine to Macrium Reflect 8 version 8.0.6161. See here for details
- Add additional support logging
- Renamed options in *Add Computers* wizard so that two entries no longer have the same title

Fixed

- Fixed error preventing the computers page from loading due to control characters embedded in backup failure messages
- Fixed the Repository browser and restore pages encountering issues with backups made on systems with non-capitalized NetBIOS names
- Fixed issue with the scheduler calendar displaying incorrect times for unusual weekly triggers where intervals were greater than 1 and the first backup happened in the week after the start date.
- Fixed some MultiSite connectivity issues

8.0.6078 - 2021-08-09

Changed

- Update Agent backup engine to Macrium Reflect 8 version 8.0.6036. See here for details

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

- Updated installer to not wait for service startup to prevent rollback on timeout
- Improved performance getting log details with MultiSite
- Improved performance with large numbers of Agents (Over 300)

Fixed

- Updated Remote Sync to take deletions into account when checking for appropriate disk space on the target
- Fixed deferred backup jobs running for computers that have never connected since the Site Manager service started up
- Fixed MultiSite API key changing when Network MAC addresses change too frequently - this was due to overly-eager hardware change detection
- Toggling scheduled backups on and off should no longer have long UI delays
- Fixed repeated passphrase change messages in the Event Log

8.0.6013 - 2021-07-05

Changed

- Allow extra time for Agent Reflect to launch on slower systems
- Add extra logging for Windows time and time zone changes
- Detect Agents running on Windows 11 and update Windows Version tags to include Windows 11

Fixed

- Removed spurious event log entries for failed configuration file loading when a file does not exist
- Fixed *Copy Path* function in Rescue Media page causing a JavaScript error
- Fixed default credentials not being used for Agent installs
- Fixed Remote Install working with default login credentials
- Fixed showing the user's display name in the top bar

8.0.5995 - 2021-06-22

Changed

- Update Agent backup engine to Macrium Reflect 8 version 8.0.5994. See here for details
- Split logging for Active Directory, Driver and Agent events into separate files
- Added a Password Confirmation dialog in the *Settings* > *Email* page when attempting to send test emails
- Improved Active Directory query performance on Agents
- Updated Azure repository configuration credentials page to match non-Azure repositories

Fixed

- Fixed emails not including backup log attachments or event name in the subject
- Fixed repository browser from preventing file deletion under limited circumstances

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

- Fixed intra-daily backup success notification settings resetting to follow backup success notifications on service restart
- Fixed slow shutdown caused by service shutdown while a repository scan was in progress
- Fixed Agent taking a long time to shut down when huge numbers of backup logs are present on the Agent

8.0.5973 - 2021-06-10

Fixed

- Fixed install failure on platforms which have never had a version 7 Site Manager Agent installed and which don't support SHA2 driver hashing
- Fixed Kerberos domain trusts causing a crash/hang in Site Manager server startup
- Fixed adding Metered license keys giving incorrect error message about upgrading
- Fixed the Scheduled Activity page always showing 'Active' button for Backup Definitions with no computers
- Fixed creating Backup Definitions without encryption producing a password length error
- Fixed the Agent not running on some systems on startup

8.0.5965 - 2021-06-07

Changed

- Update Agent backup engine to Macrium Reflect 8 version 8.0.5963. See here for details
- Added extra code to delete write-test files on Repositories
- Added additional information to errors in the UI caused by JavaScript
- Changed intra-daily forecast to show intra-daily frequency as hours and minutes instead of just minutes
- Improved Scheduled Activity computer results table to show icons for all result types
- Added an option to use Repository credentials in the Restore wizard rather than pre-filling the credential fields
- Added an Revert button to the password field when editing the password in the Repository wizard
- Updated password fields to clear on click and use a fixed length of password characters to reduce any possible information leakage
- Updated Backup Definitions wizard to produce an error if the AES encryption type is changed to a type which requires a longer password
- Site Manager browser logout is now temporarily disabled during support log generation (ctrl-shift-s)

Fixed

- Fixed Site Manager not allowing login via Microsoft accounts (username@hotmail.com etc)
- Fixed backups being stuck in the running state in Scheduled Activity view if Site Manager is restarted during backup
- Fixed daily email not considering backups with warnings as successful when generating list of computers without backups

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

- Fixed weekly triggers using an interval other than 1 from displaying the incorrect dates in the Schedules page in some cases
- Fixed the Scheduled Activity page always showing backup definitions with no computers as disabled regardless of slider selection
- Minor layout fixes on Licenses page
- Fixed Agent generating a warning that all backup sets have been deleted when using a 'Keep 1' retention rule and running the purge before backup
- Fixed the Computers page showing an 'Unlicensed' warning on computers using Virtual Machine Server Agent licenses
- Fix unusual crash if a background cleanup task triggers, runs and completes within 1 second of midnight
- Fix an Agent crashing on service shutdown if a log file changes during shutdown
- Fix missing ReflectTheme.dll in MIG component installation

8.0.5934 - 2021-05-26

Added

- Update Agent backup engine to Macrium Reflect 8 and CBT release level (8.0.5928). See here for details
- Show clock and time zone information on the Site Manager header
    - All times shown in the UI should now be in the Site Manager server's time zone, not browser time zone.
- Intra-daily backups available in Schedules page
    - Intra-daily stealth mode (backup logs are not produced for successful intra-daily backups, a daily table of results is available in the Logs page instead)
    - Additional notification options for intra-daily backups
- New computers page
    - User-creatable tags
    - Automatic tagging for Agents with problems, Active directory information and backup definition membership
    - Sorting and grouping by tags
    - New detailed information for each computer
    - Backup by tag option in Backup Definitions
- Update wizard for adding new computers
    - Full Active Directory browsing to locate new computers
- Added Universal Rescue Media (a single rescue media with multiple PE versions to allow for a single USB which can restore any computer)
- Added USB creation tool to Rescue Media page - this allows a USB boot device to be created from an ISO image without third-party software

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

- Added option to Remote Sync repositories to S3 compatible stores, including Amazon, Wasabi, Backblaze and any other manually configured S3 compatible server
- Added daily data export option to export CSV data from computers, licenses, backups, repositories (content and space usage) for audit and third-party integration purposes
- Dashboard updated to make status tiles clickable
- Added option to not show backup start/end notifications on Agents for scheduled backups
- Added option to use Wake-on-LAN in Run Now backups
- Added discovery and configuration of Domains in the same forest as the server's domain as login providers

Changed

- Added code to detect SHA2 driver hash capability
    - Computers which cannot support SHA2 driver hashing will not have the CBT driver installed. If installed from an older Agent install, it will be removed on upgrade
    - The Site Manager server now required SHA2 driver hashing. Installing or upgrading a Site Manager server install will fail on these platforms
    - Microsoft hotfixes are available for platforms with these issues (Windows 7 and Server 2008 R2)
- More compact forecast display
- Computers page shows more detail on backups in progress
- Support upload (ctrl-shift-s) now allows download of support information in the browser
- Support upload (ctrl-shift-s) can now collect data from Agents directly
- Passphrase protected private keys can now be used for HTTPS certificates in the Site Manager server
- Changed Site Manager XML file names to look better in Backup Logs
- Updated repository connection code to show repository connection errors directly in Backup Logs
- Site Manager now sends IP addresses of Repositories on backup so that Agents which can't DNS resolve Repository names can use the IPs
- Added MAC and IP address columns to Computers page (hidden by default)
- Added Backup Comment column to Repository browsing, verification and remote restore pages
- Update columns in computers CSV export

Fixed

- Fixed case where an IP address change was not synced to the Site Manager server from an Agent with multiple NICs
- Improve handling if a repository goes offline during a remote sync
- Repository browser now lists all computers with backup image files, even if they have since been removed from Site Manager
- Remote Syncs that end with a warning now show correct yellow status and icons in notifications
- Remote Sync in the dashboard progress widget will now say which Repository is syncing

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

- Site Manager UI can show timestamps in a mix of Site Manager server time zone and Web Browser time zone - all times are now in the server's time zone

Older Releases

For release notes for version 7.3 and earlier, see the Archived Release Notes

Archived Release Notes

This page contains release notes for version 7.3 and earlier. Current release notes are available in Release Notes

Site Manager Release Notes

7.3.5920 - 2021-05-24

Added

- Site Manager 8 upgrade wizard added
- Version 8 license upgrade tools added
    - In the licenses page, version 7 license keys can be updated to version 8 if eligible.
    - Site Manager 7 will accept and use version 8 keys
    - Standalone Reflect licenses can be upgraded if the computer is running the latest version of the Agent and Reflect 7

Changed

- Update Agent backup engine to Reflect and CBT release level (7.3.5854). See here for details
- Improved Repository logging for support

Fixed

- Fixed issue where an SFTP remote sync could continue failing after network connectivity is restored
- Fixed Repositories not showing error status in the UI
- Improved performance for large numbers of Agents

7.3.5556 - 2020-01-20

Changed

- Update Agent backup engine to Reflect and CBT release level (7.3.5555). See here for details
- Added Windows Server 2019 to possible Windows versions
- Add registry key to override Repository status polling frequency

Fixed

- Prevent VSS causing spurious hardware change detection and Agent reconnection during backups

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

7.3.5390 - 2020-12-15

Changed

- Added 60 second delay between an Agent coming online and allowing any backups to start. This is to reduce interrupted communication backup warnings when an Agent receives a security update after upgrade or has other communication issues
- Update Agent backup engine to Reflect and CBT release level (7.3.5365). See here for details
    - This update adds the option of using an internal scheduler for backups scheduled locally on the Agent. Users who have standalone Reflect should upgrade Reflect before converting locally scheduled tasks to this new scheduler. Centrally scheduled tasks are not affected.
- Added desktop and start menu icon for MIG
- Added registry key to bind management UI to a specific IP address
- Added registry key to disable local and domain administrators being able to login to Site Manager by default
- Reduced network timeout delays when adding offline license keys, updated UI to provide better guidance

Fixed

- Fixed support expiry notices in the license page from displaying spurious information
- Fixed bug with network authentication during a restore which could cause a Site Manager Remote Restore to fail authentication in some cases where a Restore initiated from the Agent directly would succeed
- Fixed crash in Site Manager when attempting to verify two backups files where one file is a copy of the other
- Fixed scheduled backups failing a computer's backup instead of deferring that backup if that computer disconnected in unusual circumstances
- Fixed licenses page showing Agent license information from very old Agents as standalone licenses
- Fixed backup failures at an early stage (such as a File and Folder backup not matching any folders on the Agent) not triggering backup failure notifications
- Fixed bug where once one offline license key was added, the UI would not close correctly

7.3.5240 - 2020-10-05

Added

- Site Manager Server now includes MIG (Macrium Image Guardian) to protect backup repositories hosted directly on the Site Manager server
    - For upgrades, MIG is not installed by default - after upgrade, the 'Modify install' feature can be used in the Programs Control Panel in Windows to install it.
- Added CPU priority and write rate limiting to Backup Definitions

Changed

- Updated to CBT version 7.2.7114
- Added a status column to the Agent specific Rescue Media wizard to show which agents already have Rescue Media built.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

- Improved the driver load sequence in Windows PE/RE when multiple drivers for the same hardware is present
- Improved driver collection process to identify driver files which are stored in multiple locations on the Agent computer and reduce duplication
- Added 'Disk label' matching rules in Backup Definitions to allow easy blanket exclusions of virtual or special disks
- Added a longer timeout during the Remote Install process for computers which take more than 5 minutes to copy the Agent installer MSI from the server
- Improved error handling in Remote Syncs to make error conditions like the remote server being out of disk space clearer and to avoid unnecessary retries

Fixed

- Fixed backup logs not being attached to success emails in all cases
- Fixed incorrect display when filtering the logs table for a computer which has no backup logs
- Fixed an issue where backup times could appear as midnight from some Agents installed on Windows in set to European system locales
- Fixed copying drivers from Agents failing for .inf files >2MB
- Removed unnecessary copying of USB drivers for USB controllers supported natively in Windows PE
- Fixed Using invalid domain names (.) causing remote install of an agent hanging
- Fixed changes to computer status causing options to uncheck themselves in the Restore wizard
- Fixed MIG protected repositories failing to delete dependent files when deleting a backup image in the Site Manager repository browser
- Fixed Volume and disk label matching rules in Backup Definitions not handling repeated spaces correctly
- Fixed shutdown hang caused by deadlock when sending emails during a backup finished notification while an Agent changes state
- Fixed service shutdown issue when running on a Windows debug kernel
- Fixed incorrect password entry dialog appearing when attempting to restore a password protected image
- Fixed multiple Remote Sync start notifications in some circumstances when a Remote Sync with the same time set for the start and end times is triggered while a backup is also running

7.2.5163 - 2020-08-25

Fixed

- Fixed crash when using unusual proxy configurations

7.2.5161 - 2020-08-25

Added

- Added Agent-specific rescue media

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

    - Critical drivers and static IP information are gathered automatically from Agents
    - Rescue Media can be created on-demand for each computer with appropriate options and drivers included
    - Drivers can be exported from Site Manager to allow for manual recovery
    - Rescue Media build progress is now shown in the dashboard
- Drivers that have been manually added to Site Manager will be pushed onto computers during Remote Restore for cases where the host's own drivers are incompatible with Windows PE (Windows XP systems)
- Added FTP and FTPS support to Remote Sync
    - SFTP remote sync has been changed to *File Transfer*
    - *File Transfer* Remote Syncs can be configured to use SFTP, FTP or FTPS protocols
    - An option to override the default port used has been added
- Added option for log and event log retention in *Settings -> System*
- Added a *cancel* option to the forecast for *Run Now* backups which have not started yet

Changed

- Update Agent backup engine to Reflect and CBT release level (7.2.5107). See here for details
- Updated licenses page to be clearer
- Updated notification messages and reorganized notification settings
- Remove 25 character name limit on Backup Definitions and Schedules
- Updated OpenSSL libraries for fixes and SSL improvements
- Remote Sync windows which cross the midnight boundary (e.g. 11PM -> 3AM) are now supported
- Remote Sync results now show a more meaningful message when no changes were found
- Updated Slack integration to use the webhook API
- When adding computers by IP address, use Windows Networking to resolve names if DNS lookup fails
- Removed MSMQ dependency from Site Manager server - Agents which use the old MSMQ communications system (Version 7.2.4091 - March 2019 and earlier) are not longer supported
- Site Manager will recover partial or failed backups and consolidations automatically

Fixed

- Fixed lock up when shutting down the Site Manager service with a Remote Sync in progress
- Fixed rare restore failure on Windows 7 due to network conditions
- Fixed spurious "Did not receive an end notification from Macrium Reflect" appearing before backup finish on some systems
- Fixed remote restore of password encrypted images failing with a read/write error
- Fixed Internet Explorer 11 display issues on the dashboard and other pages
- Fixed Event Log not refreshing when going back to the page after new log entries have been generated

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

- Fixed activity popup on the computers page not showing the correct computer when multiple selection is used
- Fixed dashboard notifications not being in the correct order when events happen within 1 second of each other
- Windows PE downloads will now use the Site Manager proxy server settings
- Fixed inconsistent date formatting (DD/MM/YYYY vs. MM/DD/YYYY) when the user default locale differs from the system locale in Windows
- Fixed repository browsing showing no backup files for computers with an active backup in progress

7.2.4898 - 2020-05-11

Fixed

- Fixed emails being rejected by some strict email servers since the 1st May 2020

7.2.4863 - 2020-04-27

Changed

- Added internal retries to repository access during remote synchronization to improve robustness during long synchronization operations

Fixed

- Fixed issue where some license keys could be saved into data files with trailing space characters, causing them to fail to validate
- Fixed license key checks happening continuously on a small number of systems with specific error conditions
- Fixed remote install problems on systems without Agent passphrases set
- Fixed Agent passphrase configuration appearing with neither option selected on the *Settings* -> *System* page under some circumstances
- Fixed Agent passphrases containing space and double quote characters not working with remote installation
- Fixed share authentication problems on the Site Manager interface which could occur when using a repository hosted on the same computer as the Site Manager server via IP address

7.2.4814 - 2020-03-27

Changed

- Update Agent backup engine to Reflect and CBT release level (7.2.4808). See here for details
- Added new remote install mechanism, this removes the requirement for WMI firewall rules. The WMI mechanism is still used as a fallback if the new method fails.
- Improve support logging for restore, login authentication, remote sync and repository management
- Reduce default retry attempts for remote sync to a local folder target

Fixed

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

- Fixed issue where an Agent running on the same computer as Site Manager server could affect the repository status when a backup fails
- Fixed issue where the service does not shut down in a responsive manner when many license key checks are in progress
- Fixed issue where Site Manager would not scan image files in one repository folder when a backup was on progress in a different, unrelated folder
- Fixed login authentication incorrectly failing for accounts with empty passwords
- Fixed Active Directory login permissions manager not listing accounts whose primary group is not "Domain Users"

7.2.4709 - 2020-02-04

Fixed

- Fixed issue with new and copied schedules reusing the same ID internally

7.2.4708 - 2020-02-03

Fixed

- Fixed some backups from appearing as failures and triggering retry-on-fail rules incorrectly.
- Fixed Email error messages being truncated.

7.2.4700 - 2020-01-29

Added

- Added ability to create rescue media ISO images from the Site Manager server.
- Added registry keys to disabled LDAPS when making Active Directory login requests.
- Added registry key to control network keep alive messaging rate for Agents behind NAT routers
- Added proxy server settings for internet requests to Site Manager configuration

Changed

- Update Agent backup engine to Reflect and CBT release level (7.2.4601). See here for details
- Updated restore to use Windows PE10 build 1709.
- Improved pushing of PE files from the Site Manager server in a network isolated environment.
- Agent Configuration Tool will now succeed tests if the agent is already connected to the same server.
- Remove unnecessary network checks when adding multiple computers.
- Truncate extremely long backup error messages in the User Interface. Full errors are available in the logs.
- Force a repository cache database update on Remote Sync start to ensure the latest changes are always reflected.
- Improve Remote sync logging.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

- Improved logging for switching passphrases and connecting to passphrase protected agents. This should reduce agents stuck in the Unauthorized state.
- Updated Event Log clear option to be clearer.
- Added full path to details in repositories page.
- Made unbrowsable partitions in backup files unclickable in the browse interface.
- Updated all Windows authentication entry fields to correctly handle NetBIOS (DOMAIN\User) and DNS (user@domain.tld) entries in the username field

Fixed

- Fixed issue where the Agent may attempt to connect to the incorrect IP address when DNS lookup returns a CNAME record
- Fixed some remote install failures appearing as successful in the user interface.
- Fixed computers page CSV export.
- Fixed UTF-8 decoding of localized error messages in backups.
- Ensure MultiSite connection is retried when waking from sleep.
- Fixed restores failing when restoring from a network share shared from the Site Manager server computer.
- Fixed lock ups caused by network timeouts attempting license key server checks.
- Fixed error preventing deletion of Remote Syncs.
- Fixed backups being prevented when a file named "c:\Program" exists.
- Fixed old scheduled backup failures appearing in daily emails.
- Fixed layout breaking when Site Manager web interface is displayed in a window less than 1650 pixels wide.
- Fixed Site Manager backup status being 'stuck' in computers table
- Fixed Event Log page displaying loading spinner forever if filtered to show 0 events

7.2.4479 - 2019-09-26

Changed

- Update Agent backup engine to latest Reflect and CBT release level

Fixed

- Fixed spurious Windows event logging happening on the Agent under some conditions
- Email addresses with labels are now accepted (e.g. John Doe <jdoe@example.com>)
- Fixed Agent updates failing on computers which have not been rebooted since the last Agent update
- Fixed computers which have been disconnected for extended periods of time from consuming license seats incorrectly
- Fixed emoji and other Unicode chracters in supplmentary planes not appearing correctly in email subjects
- Fixed slow shutdown caused by large numbers of repositories
- Fixed computer list corruption on restart under some circumstances

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

7.2.4447 - 2019-08-28

Added

- New *Scheduled Activity* view for configuring scheduled backups and remote syncs, moved from the Repository page.
- Added File and Folder type to Backup Definitions.
- Added ability to download multiple files and folders as a single ZIP file when browsing images.
- Creating desktop or start menu shortcuts is now an option in the Agent MSI installer user interface when manually installing.
- Remote Sync - Added option for backups to happen during the remote sync - they can only happen for computers which have had all their data transferred.

Changed

- Remote Sync - SFTP file uploads which are interrupted will now attempt to resume the upload (up to 10 times).
- Remote Sync - Added option for backups to happen during the remote sync - they can only happen for computers which have had all their data transferred.
- Login - user accounts which are linked to an email (e.g. user@hotmail.com) may now use the email to login.
- File and Folder, Exchange and SQL backups are now shown in the Repository Browser and participate in Remote Sync.
- Updated look for Backup Definitions, Schedules, Repositories and Verification pages.
- When an agent disconnects from the Site Manager server while a backup is in progress, a new warning will be displayed instead of a backup failure.
- When Agents are updated, they will add or remove desktop shortcuts according the the setting in Site Manager.
- Failures to start scheduled backups are now shown in the email summary.
- Added additional code to ensure that network shares do not stay mapped on Agents after backups fail.
- Improved sorting and file display in the image browser, show NTFS junctions and links differently to normal files

Fixed

- Fix rare configuration file corruption on service shutdown.
- Fix SFTP upload not handling spaces in paths correctly.
- Email - Fix GSSAPI authentication in SMTP causing spurious failures.
- Fixes for MultiSite connection not retrying after network drops.
- Fixes for system which are unable to contact Macrium MultiSite servers when running as a SYSTEM service.
- Fixed Agents being shown as having standalone Reflect even after standalone Reflect has been uninstalled.
- Fixed some timing based bugs in Agent comms where the Agent is retrying a dropped connection.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

- Fixed images manually stored in the root of a repository not being shown or remote synchronized.
- Fixed locking issues when browsing image files

7.2.4335 - 2019-06-19

Changed

- Updated CBT driver to ignore the PortableBaseLayer virtual disk used by the Sandbox feature in Windows 10 build 1903
- Added retry on connection failure to file upload as part of repository sync

Fixed

- Added additional code to reconnect agents with network issues
- Improved logging for image browsing failures

7.2.4314 - 2019-05-30

Changed

- Added features to keep TCP traffic alive when passing through stateful firewalls and routers
- Added feature to prevent deletion of old backup sets if retention rules are set to "Keep 1 Full Backup" and the set of disks backed up changes

Fixed

- Fix for being unable to communicate with a computer which has a lowercase NetBIOS name
- Fix Agent connections breaking when coming out of sleep
- Fix email bodies generating standards compliance errors in some gateways
- Fix email authentication *None* type not working
- Fix MultiSite data integration not providing all data under some circumstances

7.2.4290 - 2019-05-15

Fixed

- Fixed email not working over SSL
- Fixed Remote sync not showing in the forecast in some circumstances
- Fixed backups staying in "immediate" status in some circumstances
- Fixed Agent incorrectly displaying an error about metered licensing
- Fixed login for domain users granted permission to login through a local group

7.2.4279 - 2019-05-10

Fixed

- Fixed problem with authentication of domains which are child domains or part of a forest

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

- Fixed Agent not sending appropriate progress messages under all conditions

7.2.4276 - 2019-05-09

Added

- Added ability to grant non-Administrator users or security groups access to Site Manager
- Added ability to connect to non-joined Domains for login authentication
- Added CSV export to Computers page
- Added Agent Config Tool to test connectivity from Agent to Server
- Added option to disable automatic Agent updating
- Added option to Computers page to migrate Agents to another Site Manager

Changed

- Changed Agent to Server communications to use TCP/IP sockets instead of MSMQ for flexibility and performance reasons. See KnowledgeBase for more details.
- Changed MultiSite integration to show status in settings page and support upcoming MultiSite changes
- Improve performance of repository checks and reduce number of login events in Windows Event Log
- Updated email sending to support TLS 1.1 and produce more readable errors
- Updated Macrium Reflect Backup components to latest release

Fixed

- Fixed date not showing in Summary Email subject line
- Fixed Repository last synchronization times to display dates as well as times

7.2.4091 - 2019-03-13

Fixed

- Fixed about page being blank for offline Site Manager installations
- Fixed crash when remote syncronization credentials become invalid

7.2.4075 - 2019-02-26

Fixed

- Fixed standalone license keys not being read from some Agents
- Fixed license key table showing MAL licenses in the standalone license list
- Fixed drop-down selection on Run Now and Schedule Backup dialogs from sometimes failing to select the correct item

7.2.4000 - 2019-02-11

Changed

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

- Improved forecast performance with large numbers of scheduled backups

Fixed

- Fixed issue with restore, validation and image browsing interfaces failing to validate image file passwords under some circumstances
- Fixed issue with restore failing with an error in "iLib::GenerateXMLRestore"
- Fixed email settings showing the incorrect options for encryption after a page refresh
- Fixed disk view in new definition dialog being broken by new Chrome version
- Fixed dashboard notification widget options interface not updating when it should
- Fixed an issue where building rescue media on a computer with both the Site Manager Agent and Macrium Reflect installed could fail

7.2.3985 - 2019-01-23

Fixed

- Fix for VSS timeout errors on some systems
- Fix for Agent showing older Rescue Media creation interface
- Fix unusable dialog boxes when adding triggers on a smaller resolution screen

7.2.3971 - 2019-01-15

Added

- Updated the Agent to use Reflect 7.2 technology including updated CBT drivers and WinRE based restore environment
- Added CSV export to license and event log pages
- Added clear event log facility
- Added Azure repository type
- Added default install credentials for remote Agent install to settings

Changed

- Improved dashboard loading performance
- Improved forecast performance
- Updated event log page to improve look and performance
- Improved internal repository credential handling
- Made repository sync errors clearer

Fixed

- Fixed issue preventing backups on some headless Windows Server Core systems
- Fixed Site Manager not using HTTPS-only cookies when configured to use HTTPS

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

- Fixed Repository browsing not picking up changes when whole folders were manually deleted from repositories
- Fixed crash on startup when encountering corrupt image files

7.1.3778 - 2018-10-23

Fixed

- Initial setup wizard was not setting HTTPS mode correctly
- Forecast view was not showing weekly triggered backups which have multiple days of the week selected

7.1.3720 - 2018-10-09

Added

- Remote synchronization of repositories - a repository can now be configured to synchronize with an SFTP server or any Windows share (including Azure and AWS Storage Gateway) on a daily basis.
- Configuration backup and restore - from the settings page, Site Manager configuration can be backed up, downloaded and restored, to help disaster recovery or redeployment
- Added an option to set the description for a computer
- Added the Local Repository type. This repository type is to allow computers with locally attached storage to be backed up and managed by Site Manager

Changed

- Adding computers will now not start the network scan automatically - in addition, there is a new option to list computers from a Windows domain server
- Adding a MAL license key when the Site Manager server will now prompt for an offline activation key instead of failing
- Improved Event Log and Backup Log performance

Fixed

- Slack instructions now contain the correct link
- Removed older cryptographic cipher suites from HTTPS

7.1.3436 - 2018-07-24

Fixed

- Fixed image browser returning "Unable to start PSMounterService" error

7.1.3420 - 2018-07-20

Fixed

- Fixed last operation columns in computers view not displaying correctly
- Fixed repositories with no credentials showing the wrong status

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

7.1.3396 - 2018-07-18

Added

- New dashboard interface with resizable widgets and warning tiles
- New branding and colour scheme, including updates to side menus and tables
- Ability to open backups and download individual files from the browser
- Allow the number of days a computer has gone without a backup before a warning is added in the summary email to be set in the interface

Changed

- Changed license checking code to recheck licenses more frequently if the check failed due to network issues, this should help reduce problems caused by temporary internet disconnections during Site Manager startup
- Improve loading times when starting up the interface
- Improve a number of UI components including time pickers
- Improve backup summary emails to include computers which are waiting to backup, computers which failed to start backups and other conditions which may need attention

Fixed

- Fix a rare crash on server stop
- Fix backups not showing in the restore view if there are no repositories when the Site Manager service was started
- Fix deferred backups not being deferred correctly

7.1.3268 - 2018-06-13

Added

- Option to install agents without creating desktop shortcuts
- Added pause and cancel buttons to detailed backup progress dialog
- Added ability of the agent to run a user-supplied script to disable backups (e.g. when on WiFi or VPN)

Changed

- Improve computer name sorting
- Improve time display in time picker
- Additional Wake on LAN options for retry and timeout
- Improve Environment Check tool to be more flexible about different IP configurations

Fixed

- Fix issue with being unable to edit the 'Test Recipients' field for email
- Fix issue with broken screen layout when editing schedule triggers multiple times on a smaller resolution screen/window

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

- When restarting the server, paused backups should no longer be lost from the dashboard progress widget

7.1.3017 - 2018-03-29

Added

- Implement metered licensing
- Wake on LAN option in schedules

Fixed

- Agents which cannot receive communications from the server should no longer appear as managed in the UI
- Fix crash in restore PE environment when source image cannot be read
- Improve performance of the dashboard when large numbers of updates are happening
- Fix unauthorised agents generating unnecessary network communications
- Fix fortnightly schedules triggered close to midnight on a Saturday occuring on the wrong week
- Fix crash when removing an agent immediately after refreshing the agent status

7.1.2916 - 2018-02-27

Fixed

- Fix exit to login screen on restore
- Fix email notification defaults not being applied until settings are saved

7.1.2910 - 2018-02-26

Added

- New calendar view of schedules
- Email notification of individual events

Changed

- License keys now require an internet connection on startup to validate
- Performance improvements
- Updated settings page to be more responsive
- Improve forecast display and performance

Fixed

- Fixed retention rules not being applied to old backups when changing partitions in a Backup Definition
- Fixed case where remote install of agent could fail claiming computer is offline when it isn't
- Fixed memory leak when adding multiple computers with large numbers of backup logs simultaneously
- Fixed consolidation rules not being correctly applied when a Backup Definition is changed after backups have been taken

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

- Fixed rare crash on login
- Fixed backup summary computer showing nonsensical numbers when a Site Manager has no computers
- Fixed rare instance of computers being lost from the dashboard on reboot
- Fixed agent version displayed in 'Programs and Features'
- Fixed performance issues when running with over 200 agents

7.1.2860 - 2018-01-24

Fixed

- Fixed summary emails not appearing correctly on iPhones and other clients
- Fixed agent not logging events in the Windows Event Log correctly

7.1.2821 - 2018-01-08

Added

- Added *Browse* capability the repositories
- Added function to delete backups from the repository browse feature
- Added network information diagnostic to the detail panel in computers view
- Added warning to agents which require a reboot for the CBT component to function
- Improved speed of file listing from repositories
- Added region selection to AWS Storage Gateway repositories
- Added new filters to Backup Definitions to exclude some disks/partitions from the backup
- Added computer health information to summary emails
- Added different computer icon to show which computers are Virtual Machines

Changed

- Improved error handling for Repository connection errors due to network problems
- Improved performance with large numbers of agents
- Improved performance of agent related data requests
- Updated logos and icons
- Added warnings for deleting a Backup Definition which has been used to create backup images
- Added paging in restore and verify file lists to better handle large numbers of files
- Added icons for full, differential and incremental images to restore and verify tables
- Updated 'Unprotected Computers' dashboard widget to show more useful information
- Disabled cancelling of backups in places it's not valid to cancel
- Moved log resync function to details panel of the agent
- Improved performance with large number of active backups

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Fixed

- Fixed issue where restore does not show backups from some NAS repositories
- Fixed issues where transient network errors could cause a repository to require manual intervention before reconnecting
- Fix issue with support upload uploading the wrong data
- Fixed confusing error when adding a version 7 upgrade key with a base v6 key fails
- Fixed spurious timeouts and backup failure messages happening when a verification operation takes an extremely long time
- Fixed license key upgrade dialog not being hidden correctly in some situations
- Fixed complex Backup Definitions with overlapping rules not backing up the correct backup set
- Fixed some display issues with selected months in Schedule triggers

7.1.2678 - 2017-11-06

Fixed

- Fixed issue where computers with both the Agent and Site Manager server installed would generate large numbers of Windows Event Log events
- Fixed issue with verification page not allowing file additions
- Fixed issue with a crash on computers using third-party encryption tools

7.1.2657 - 2017-10-20

Fixed

- Fixed Backup Definition rules becoming unavailable after creating a new Backup Definition
- Fixed Backup Definition wizard last page being incorrectly aligned
- Fixed monthly Schedule triggers not displaying the active months correctly

7.1.2625 - 2017-10-03

Changed

- Central Management Console is now Macrium Site Manager
- Updated user interface, numerous fixes and updates
- Update license page layout
- Updated 'Unprotected Computers' dashboard widget to group computers and be clearer about errors
- Improved performance of user interface
- Agent backup technology is now based on Macrium Reflect 7.1 technology
- Site Manager is able to work with repositories protected with Macrium Image Guardian

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Central Management Console Release Notes

v6.3.1846 - 2017-09-29

Changed

- Internal changes to support upgrade to Site Manager 7.1

v6.3.1844 - 2017-07-04

Changed

- Update 'Disk Image Insight' widget description to be more accurate

Fixed

- Fix a bug where an unauthorised computer can appear in the error state
- Fix broken Knowledgebase links

v6.3.1833 - 2017-06-14

Added

- Interface and wizard to upgrade to version 7 of CMC when released
- Added facility to upgrade licenses to version 7 on both Macrium Agent Licenses and standalone Reflect licenses installed on agent computers
- All trial licenses will automatically be upgraded to version 7 licences
- Added 'Standalone Keys' view to 'Licenses' page, showing all computers with standalone licenses, whether they exempt the computer from consuming a MAL and an upgrade facility

Changed

- Agents which repeatedly fail to patch to the latest release will be flagged as having an error in the computers view. To fix this, perform a manual full install or remote full install on the agent
- Show additional information for Macrium Agent License keys such as support information and version
- Tidy layout of 'Image Status' widget

Fixed

- Starting a Run Now backup now updates the forecast immediately
- Macrium Agent Licenses which become invalid can now be removed
- Improve handling of unicode values in computer descriptions
- Fix cancelled backups having a duration of 0 seconds in summary emails

v6.3.1791 - 2017-04-17

Changed

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

- Improved backup performance in some cases

Fixed

- Remote management integration fix
- Log view will no longer display a loading spinner forever when there are no logs or computers
- Scheduled backups can fail for systems with very large and complex disk configurations
- Fixed repository loading forever in some cases
- Fixed Environment Check tool to continue with checks if LLMNR broadcast IP check fails

v6.3.1787 - 2017-04-10

Added

- Added settings for remote management integration
- Added start date for schedule triggers

Fixed

- Fixed bug where a month by day schedule trigger with multiple weekdays set would not show some days on the forecast
- Fixed bug causing backup errors on some systems with multiple simultaneous user sessions
- UI fixes for overlapping fields and button issues at some resolutions
- Fixed bug where a failed update download would require a server restart to recover

v6.3.1773 - 2017-03-23

Fixed

- Fixed edit definition dialog. Navigation buttons inaccessible
- Fixed edit retention rules. Fields overlap each other in Firefox and Edge

v6.3.1769 - 2017-03-22

Added

- Add Windows Event Log notifications - this can be configured in the Notifications section of the Settings view
- Added 'Last Activity Time' column to the Computers view. This column is hidden by default

Changed

- Updated definition view to show computers which are fully and partially backed up more clearly and improve performance
- Improve performance of the computers view during heavy activity
- Improve performance of all views which list computers
- Improve performance when multiple simultaneous backups are being performed
- During restore, check that the image file was created from the computer which is being restored

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Fixed

- Fixed rare issue where the dashboard would not come out of the 'initializing' state
- Fix multiple tooltips being on screen at once in the forecast view
- Fix update available pop-up message appearing while already downloading an update
- Fix some rare network logon issues during backup
- Fix scheduled backups not being updated when a computer is affected by licensing issues
- Fix issue where attempting to update a repository with incorrect credentials would take that repository offline
- Fix issue which caused the service to crash when stopped in service manager

v6.3.1757 - 2017-03-10

Fixed

- Repositories showing 'Unknown Error' in some conditions
- Improve Agent network handling

v6.3.1750 - 2017-03-03

Added

- Automatic logout of the console after period of inactivity (configurable in security settings)
- Additional logging for launching backup on remote agents

Fixed

- Fixed issue where antivirus on a client could block backup and stall all scheduled backups
- Fixed issue where sometimes the dashboard would not leave the 'initializing' state

v6.3.1738 - 2017-02-22

Added

- Added drag and drop reorganisation of Dashboard widgets
- Added detailed progress log button to progress widget and Computers page
- Added additional information to the forecast to show which stage the backup is performing
- Added additional information to the backup progress widget to show backup source and target
- Added ability to set multiple agent passphrases simultaneously

Changed

- Made notification of new Management Console versions more obvious
- Repositories with incorrect credentials now enter an error state instead of repeatedly retrying the credentials
- Schedules and Definitions in the 'Scheduled Backups' section of the Repository page are now links back to the appropriate page
- Added key version to the Macrium Agent License table in the Licenses page

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

- Limited the number of notifications in the Dashboard notifications widget to 100 for performance reasons

Fixed

- Added scroll bars to verification view when a large number of files are verified
- Fixed forecast display not updating when backups complete
- Fixed a scheduled backup hanging if it is run when another scheduled backup to the same computer is already in progress
- Fixed computers sometimes appearing as both 'Managed' and 'No Agent'
- Spacing on disk and partition tables in the computers view is fixed
- Fix issue with email not being sent in some circumstances
- Fix Definition page not showing the correct definition as being selected in the left hand menu under some circumstances

v6.3.1713 - 2017-02-02

Fixed

- Fixed issue where some log files were not limited in size
- Fixed issue where fields under settings would only show the numeric parts of mixed alphanumeric content

v6.3.1708 - 2017-01-31

Added

- Ability to rearrange dashboard panels using drag and drop.
- Update agent preinstallation to have a user interface and provide diagnostics on network and communications.

Changed

- Updated remote installation of Agent software to distinguish between offline computers and computers with firewalled WMI components.
- Update startup sequence so that large numbers of agents are handled more efficiently.
- Remote installation of Agent software is now limited to 10 simultaneous installs to reduce network and system load. If more than 10 installs are requested, excess installs will wait until an earlier one completes before starting.
- Updated Amazon AWS Storage Gateway repositories to store local share information in the Storage Gateway, making re-adding AWS Storage Gateway repositories simpler.
- Improved computer view to no longer close menus during high update activity.
- Updated computer connection code to fall back to IP based message sending when communication cannot be established with an agent.
- Improved handling of domains in Repository create/edit interface

Fixed

- Upgrading an agent now correctly blocks scheduled backups for that agent and vice versa.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

- Fixed email summary showing SQL and Exchange Backups as 'Image' backups.
- Fixes for validation on Settings page.
- Layout fixes for Internet Explorer 11.

v6.3.1699 - 2017-01-16

Changed

- General performance improvements.

Fixed

- New widgets added to the *Dashboard* were not persisted in some cases.

v6.3.1694 - 2017-01-11

Added

- New security option to configure agent passphrase usage to simplify setting up and maintaining a deployment-wide security policy. Existing installations will generate a new random passphrase which can be seen and modified in the security section of the Settings page.

Fixed

- Intermittent connectivity issues
- Corrected various UI text labels

v6.3.1680 - 2016-12-26

Added

- Number of Computers linked to a *Backup Definition* is now featured prominently in the UI.
- New Event Log events added for Email reports.
- Failed log files are now attached to Email Summary reports.
- Email Summary Reports can now show error messages.

Changed

- Updated a 3rd-party UI library (*Contains several fixes & improvements*).
- Assorted minor UI improvements.

Fixed

- Invalid data entered during *Restore* wizard could prevent progress through the wizard.
- Duplicate Email Summary reports being sent for some users.

v6.3.1669 - 2016-12-15

Added

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

- CMC system restore will now copy required drivers from the client Windows OS for the PE rescue environment. This enables automatic system restores to cater for NIC and RAID hardware not natively supported by Windows PE.

Fixed

- Problems with starting the Agent service on some Windows 7 32-bit computers. This has been resolved.

v6.3.1666 - 2016-12-12

Added

- Amazon AWS Cloud Storage Gateway integration. You can now associate an AWS Cloud Storage Gateway with a repository. This enables easy tracking of the upload buffer and other parameters provided by AWS.
- System image restore now copies static IPv4 assignments to the Windows PE rescue environment.
- When launching the Macrium Agent version of Reflect, if the Agent service isn't successfully communicating with the CMC then an appropriate diagnostic error message is now displayed.

Changed

- New tabbed layout for the computers view makes fixing problem computers easier.
- New layout for the licensing view makes managing licenses more intuitive.

Fixed

- Scheduled backups could run twice if the first backup was initiated a second prior to the schduled run time. This has been resolved.
- SMTP server configuration was incorectly setting 'Plain Text' authentication. This caused emails to an SMTP server without authentication to fail. This has been resolved.
- Summary backup emails could incorectly report the backup duration by 1 hour.
- Many small bug fixes and enhancements.

v6.3.1630 - 2016-11-15

Fixed

- Backups could fail to authenticate against repositories causing the failure 'The user name or password is incorrect'. This has been resolved.

v6.3.1629 - 2016-11-14

Added

Backup Queue improvements:

- The 'Backup Now' function in Backup Definitions now queues jobs on the chosen Repository, reducing network flooding
- Schedules now contain a backup options section to improve the reliability of backups. This adds the following features:

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

- Scheduled backups for offline computers may now be deferred until the computer is online instead of failing.
- A number of attempts can be set for failing backups. If a scheduled backup fails, it will be reattempted up to 10 times after the specified number of minutes has passed

Summary Emails

- Column configuration, email sending time, and inline email view. Choose which columns appear in the summary email, preview the results and enter the time of day for automatic sending.

Dashboard Widgets

- The 'Backup Status' and 'Computers' widgets can now be clicked to view the detail behind the numbers.

Changed

- The verify view UI has been redesigned to make the verification steps more logical.
- License summary section is now more readable.
- Computer now have an 'Upgrading Agent' status.

Fixed

- Backup forecast view could hang indefinitely when displaying the forecast. This has been resolved.
- IE11 compatibility Improvements.

v6.3.1596 - 2016-10-21

Initial public release of the Macrium Central Management Console (CMC)

The Macrium CMC enables backup, restore and monitoring of multiple networked computers running Macrium Reflect using a Web browser user interface. Supported browsers are Google Chrome, Firefox, Microsoft Edge and IE 11.

A Macrium Agent service is installed on each remote computer which then communicates using Microsoft Message Queueing (MSMQ) to a single installed instance of the Macrium Server service. This service also exposes an http server service on a configurable port which enables web browser sessions to manage the Macrium Agent installed computers.

Interface Overview

Accessing the Site Manager Interface

Once installed, the Site Manager interface is available via web browser. Chrome, Firefox, Edge and Internet Explorer 11 are supported. If this is the first time the Site Manager has been run on this computer, the security configuration profile selection screen will be shown. For more details, see Installation and Update.

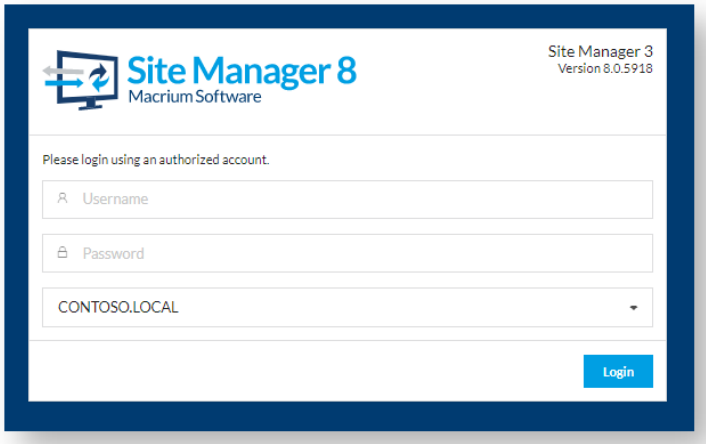
For the default simple setup profile, the Site Manager is accessible only from the computer it is installed on via **http://localhost:2904**

In the default secure setup, Site Manager is accessible from **https://<IP or DNS name>:2904**

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Logging In

If Site Manager has been configured to require a login, the following screen will be shown:

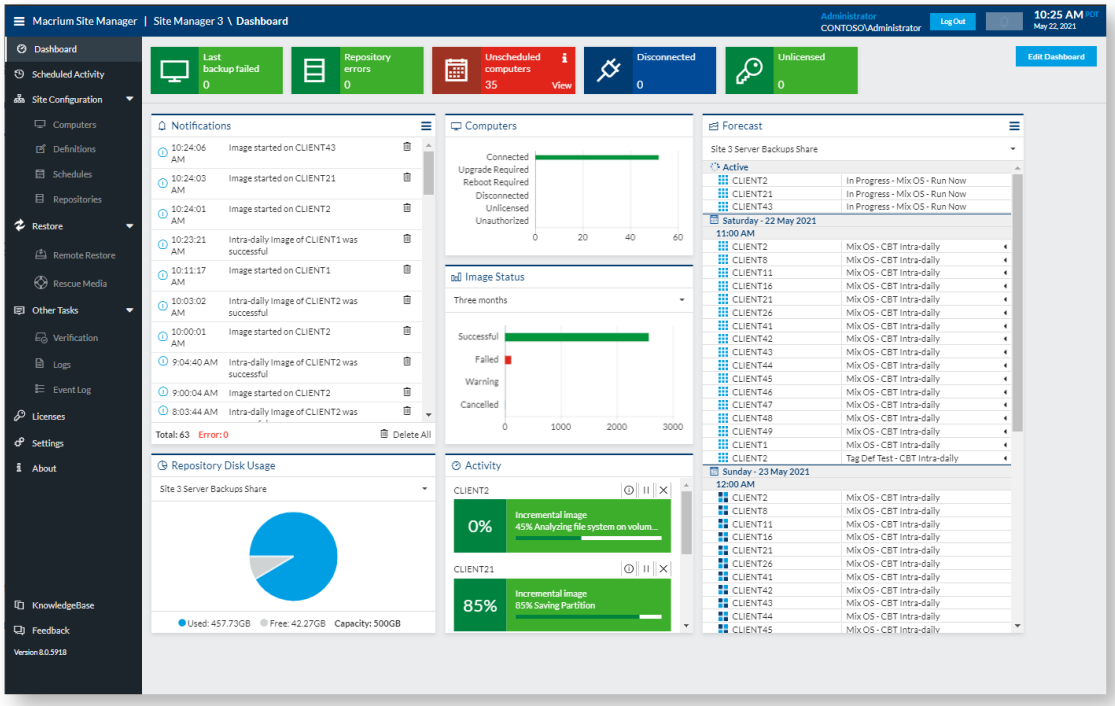


Select a login provider to authenticate against its associated authentication resource. Some login providers are created automatically and enable domain and local administrators to login. More information can be in Access Control.

If the Site Manager installation is not configured to require login, the dashboard page is shown instead.

The Dashboard Page

The Dashboard page is shown after login:



Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

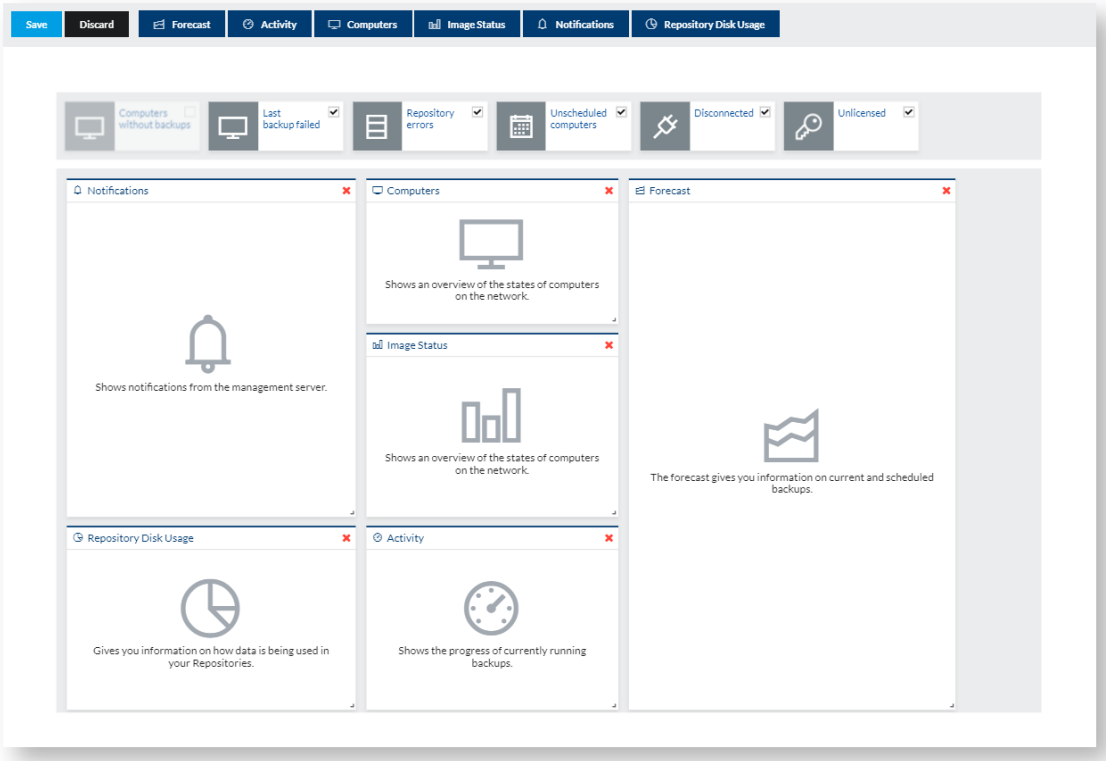
The Dashboard page shows a fixed set of warning tiles at the top, to indicate whether there are any items of concern in the Site Manager deployment and a number of different widgets to monitor the status of the Site Manager and connected computers. The overall layout of widgets and the configuration of each widget is stored on a per-user basis, so different users can set up their Dashboards in different ways.

The warning tiles are:

Warning Tile	Description
Computers without backups	Number of computers which have not had a backup created within the time limit specified in **Settings Notifications Backup Expiry Period (Days)**
Last backup failed	Number of computers where the last backup failed.
Repository errors	Number of repositories which are in an error state.
Unscheduled computers	Number of computers which are not part of a scheduled backup or have a locally scheduled backup in Macrium Reflect.
Disconnected computers	Number of computers which have been added to Site Manager but which are not currently connected.
Unlicensed computers	Number of computers which cannot backup because they don't have a valid license (either a standalone Reflect license or a server-assigned Agent license)

To edit the widget layout, click on the **Edit Dashboard** button on the top right of the screen. The Dashboard will enter edit mode:

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



The top bar allows new widgets to be added to the Dashboard - clicking a button will add a widget to the Dashboard below the existing widgets. Multiple widgets of the same type may be added (e.g. adding two Repository Disk Usage widgets to show disk usage on two different repositories). The configuration may also be saved or changes discarded here.

Below this, individual warning tiles may be turned on or off.

In the large Dashboard area, the currently enabled widgets can be moved by dragging them, resized by dragging the resize handle on the bottom right or deleted by using the delete button on the top right.

The available widgets are:

Widget Name	Description
Forecast	An overview of any upcoming backups - may be configured to show different repositories or time periods
Activity	Progress bars and information for any currently backing-up computers.
Computers	Overview of the status of computers currently being managed, and their connection status.
Image Status	A bar chart of image results for a chosen time period.
Notifications	The events and notifications which have been generated by the management server, with tools to filter and delete them.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

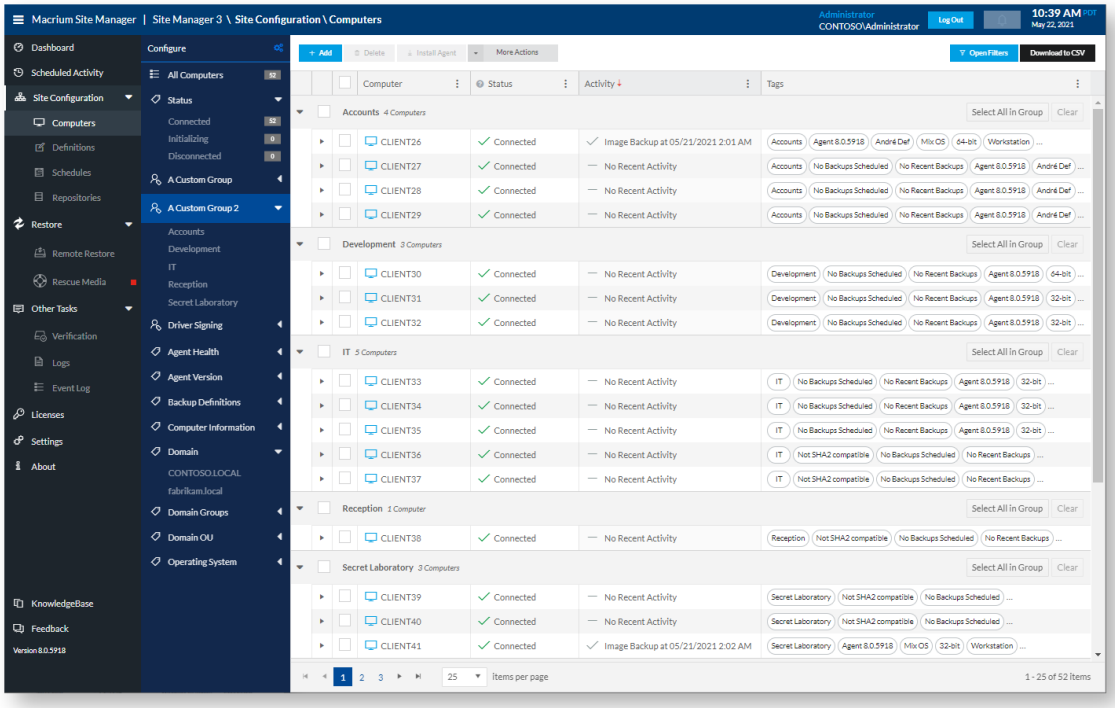
Widget Name	Description
Repository Disk Usage	The free and used space on a repository, shown in pie chart format.

Setup Pages

These pages are grouped under the 'Setup' heading in Site Manager and contain all the setup and configuration steps for Scheduling Centrally Managed Backups.

Computers

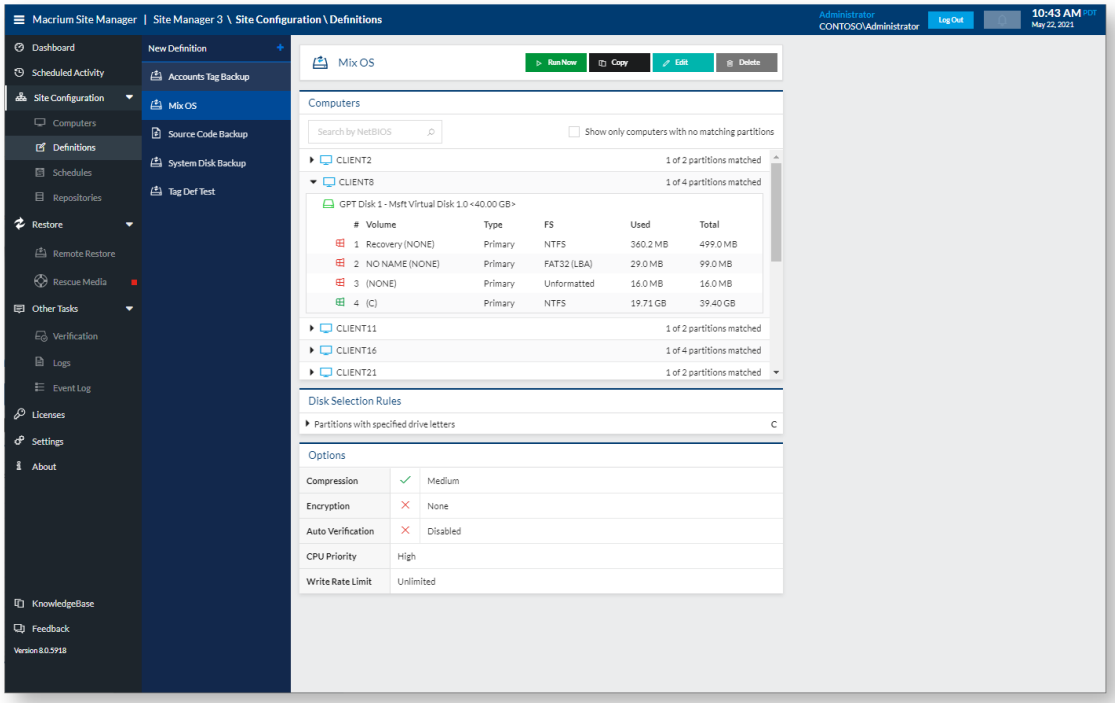
The Computers page manages the connected client computers of the Management Console and provides tools to add, remove and configure them.



Backup Definitions

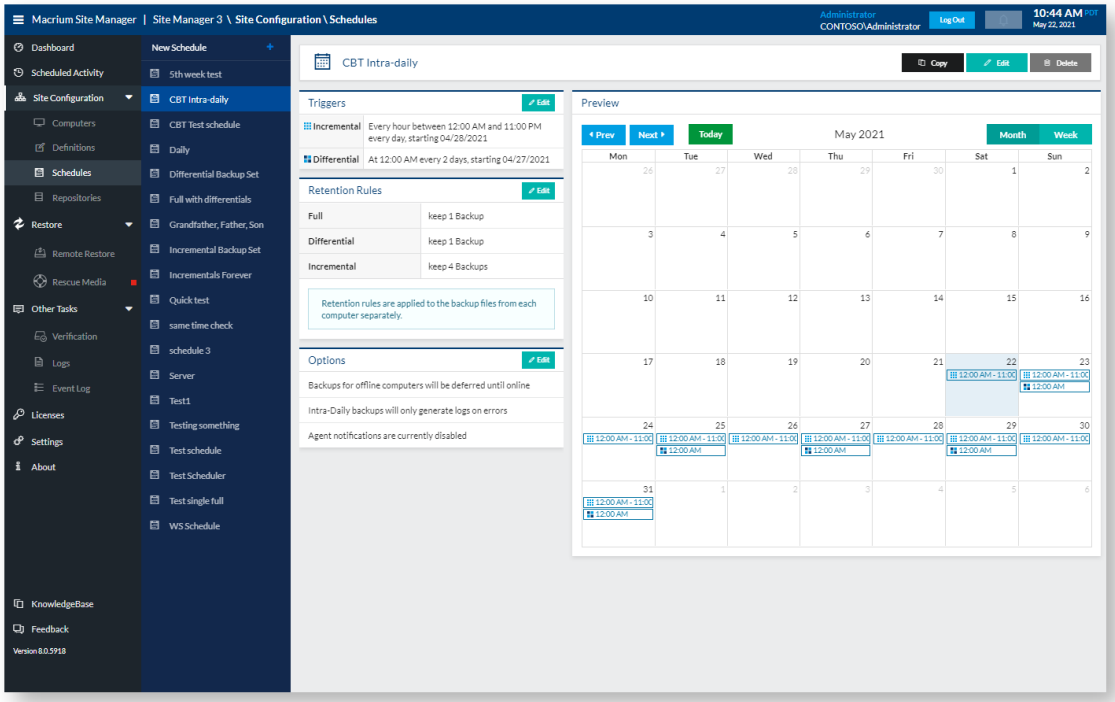
The Backup Definitions page contains definitions of what and how computers should be backed up. These definitions can be run manually or scheduled to run automatically:

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



Schedules

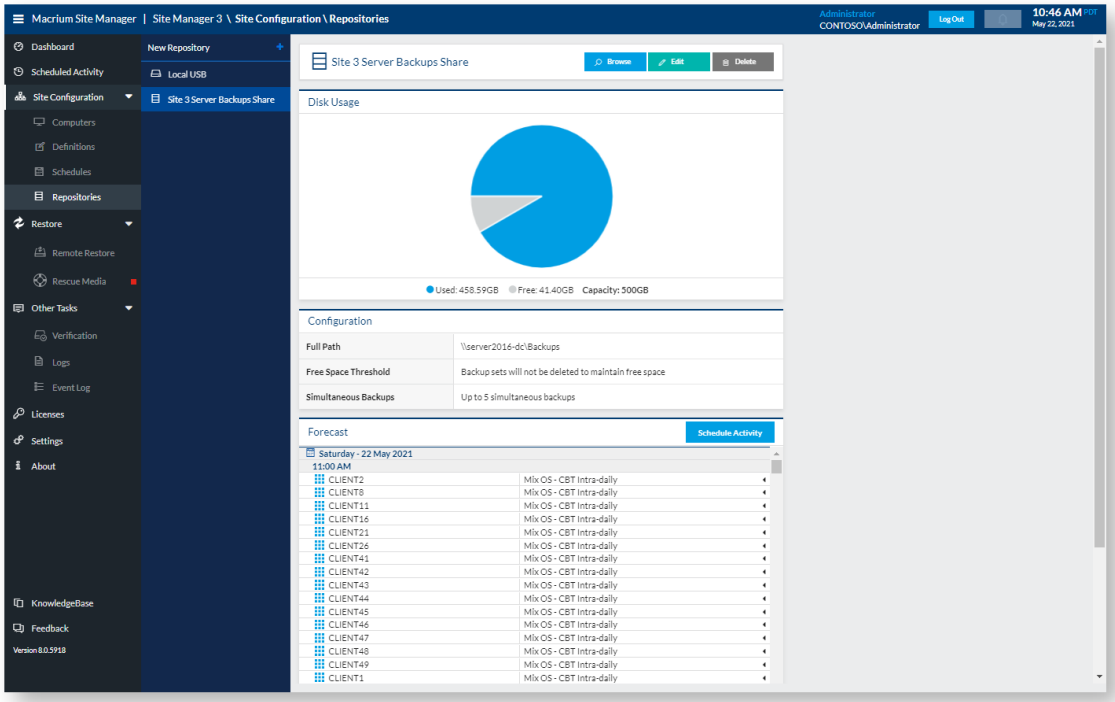
Schedules describe when backups should be run and the rules governing the retention of backups.



Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Repositories

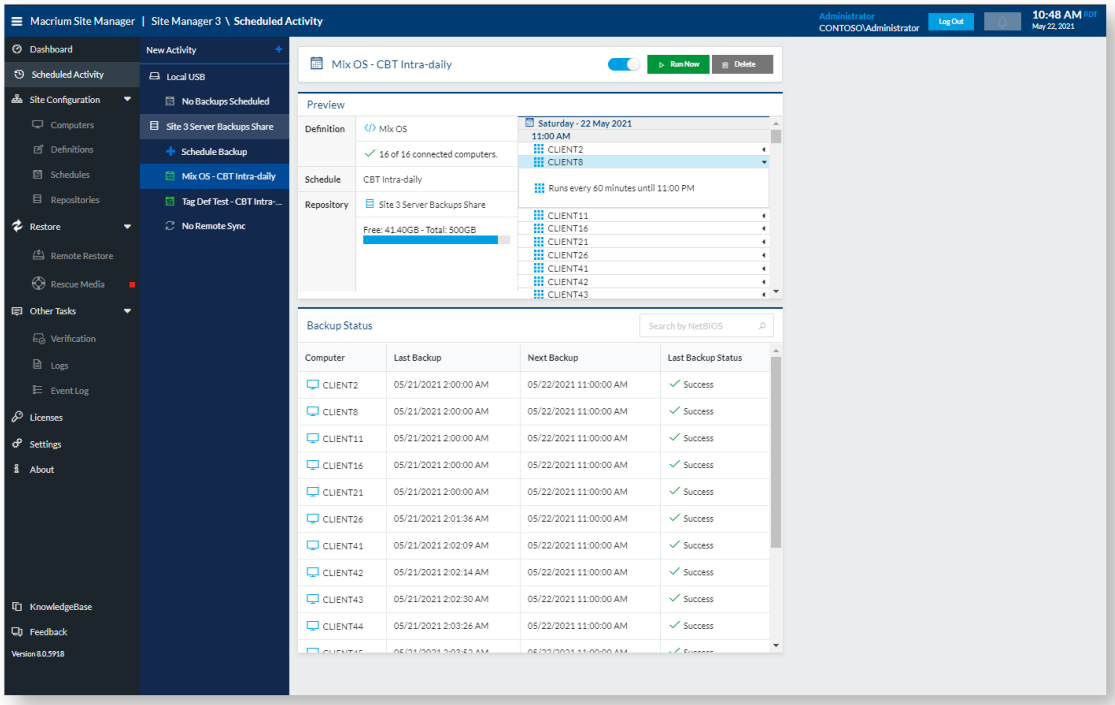
Repositories are locations which backup data is saved and managed. The repositories page can be used to create, manage and browse the contents of repositories.



Scheduled Activity

The scheduled activity page controls all regularly scheduled backups and remote syncs defined by the other setup pages. This page can be used to schedule a backup definition to backup to a repository according to a schedule.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

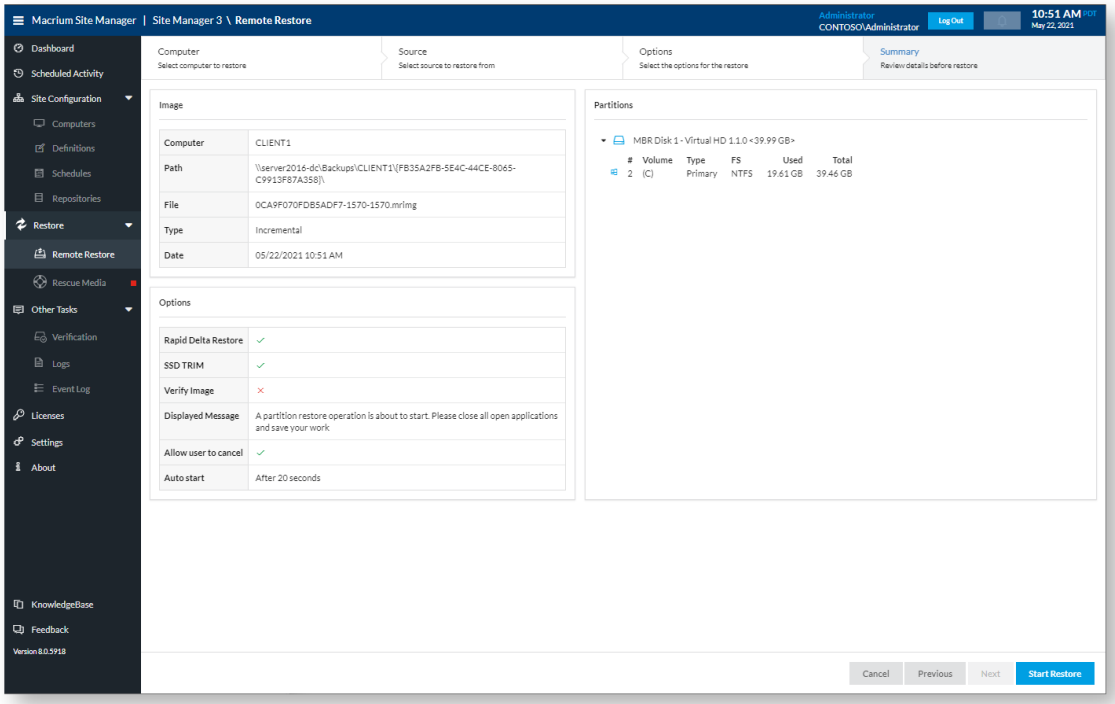


Restore

Remote Restore

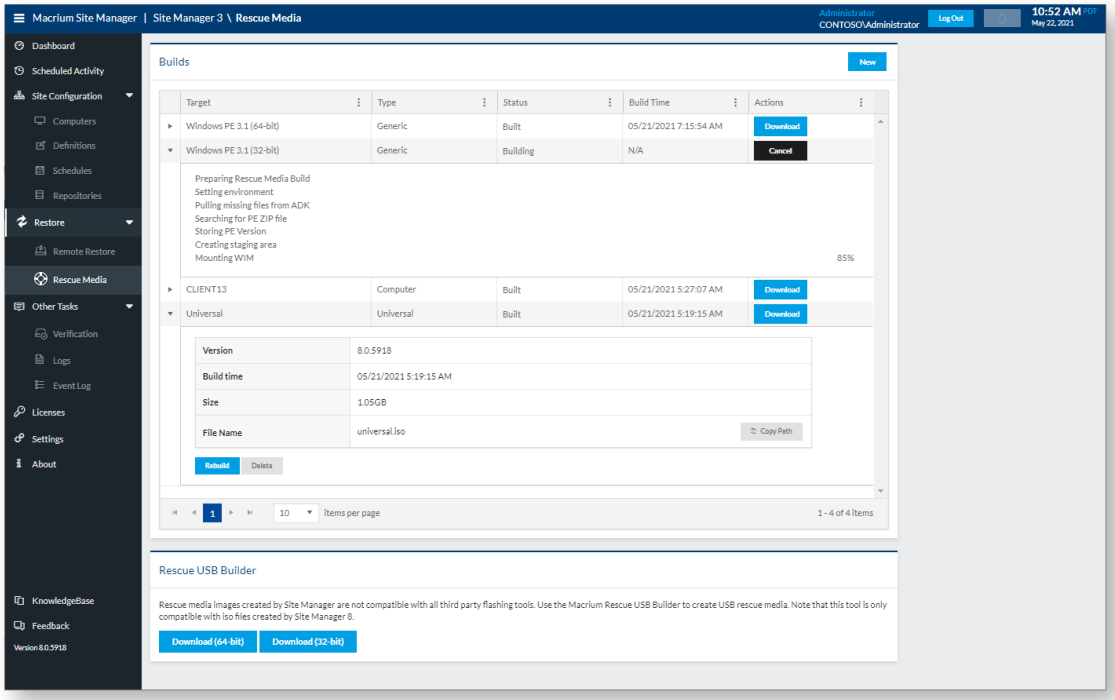
The Restore page allows image stored in repositories to be remotely restored onto a managed computer in a simple manner. See Restoring an Image through Site Manager for details.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



Rescue Media

This page is used to create and manage rescue media for disaster recovery. See Rescue Media for more information.



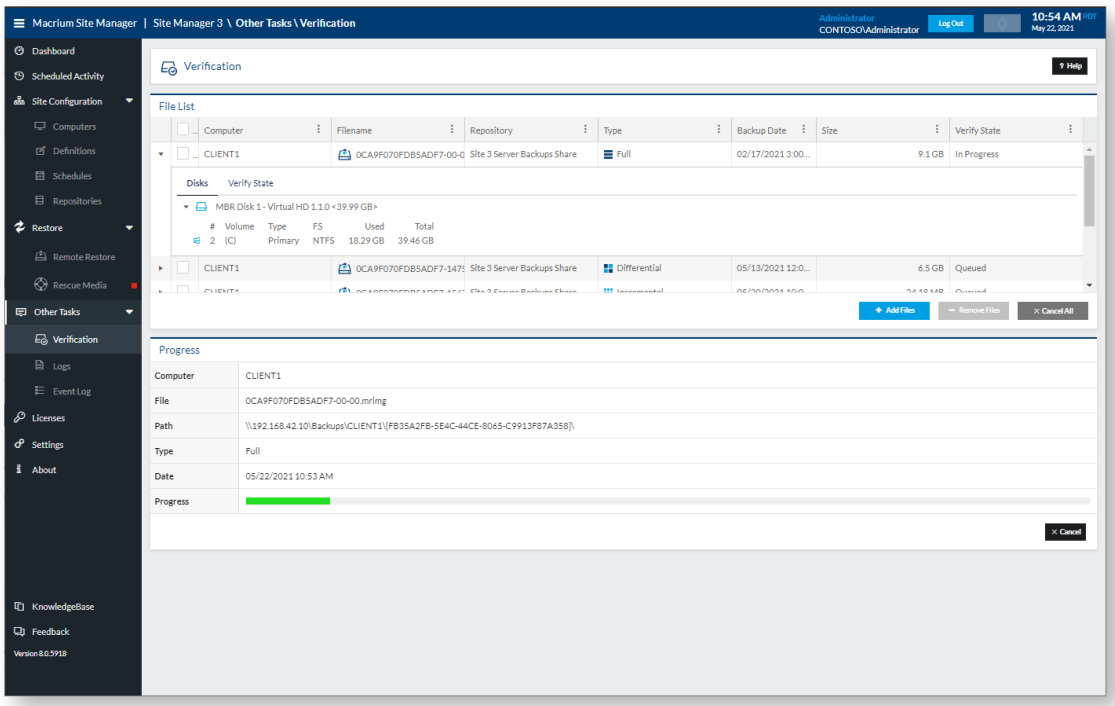
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Other Tasks

These pages contain functions outside of setting up automated backups, restoring images or configuring Site Manager.

The Verification Page

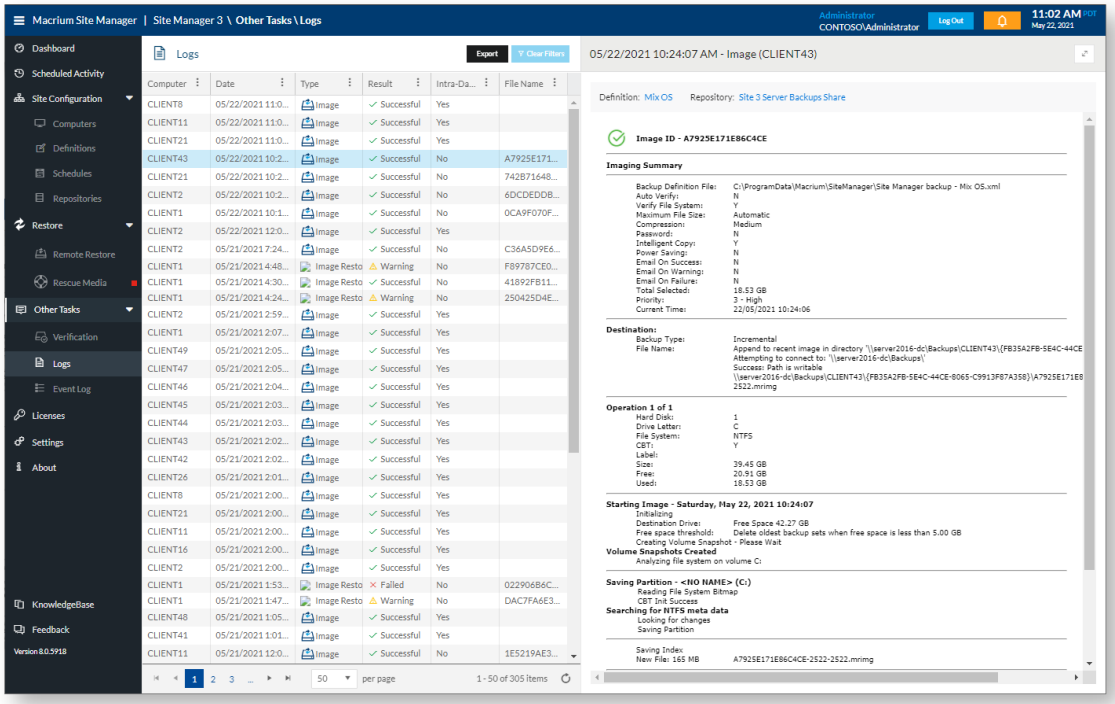
This page is used to verify the integrity of any backup images stored in your repositories. See Verifying Backups for more information.



The View Logs Page

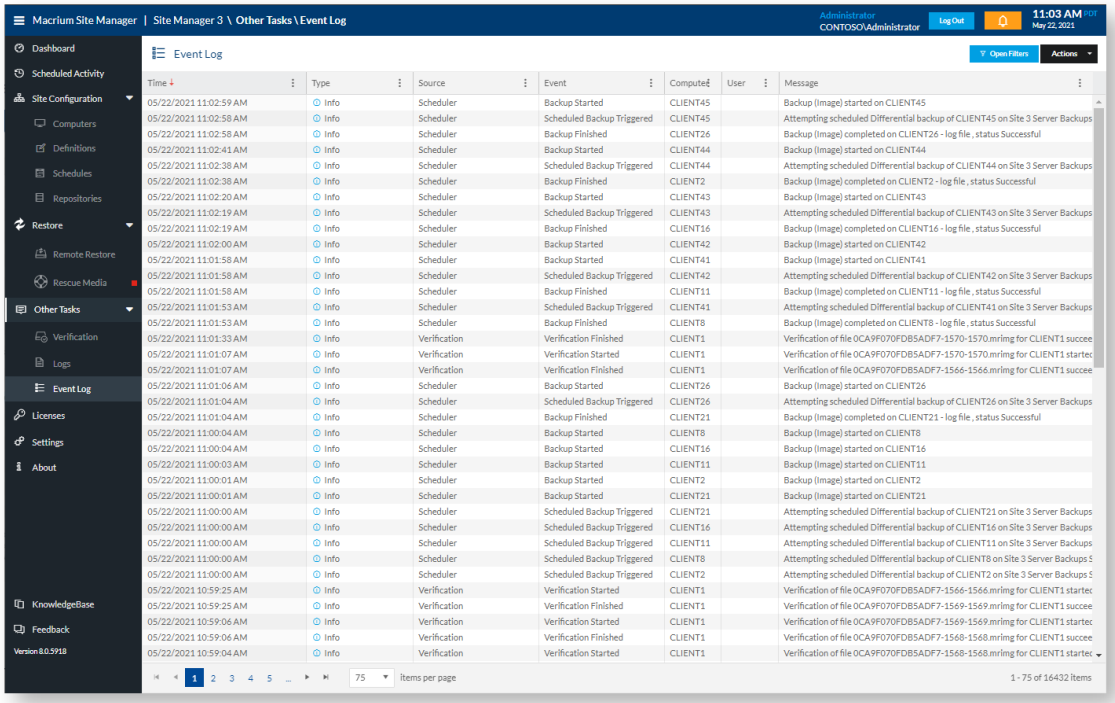
The View Logs page is used to review backup history and gives access to all backup logs on connected computers. For more detailed information see Reviewing Backup Logs.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



The View Event Log Page

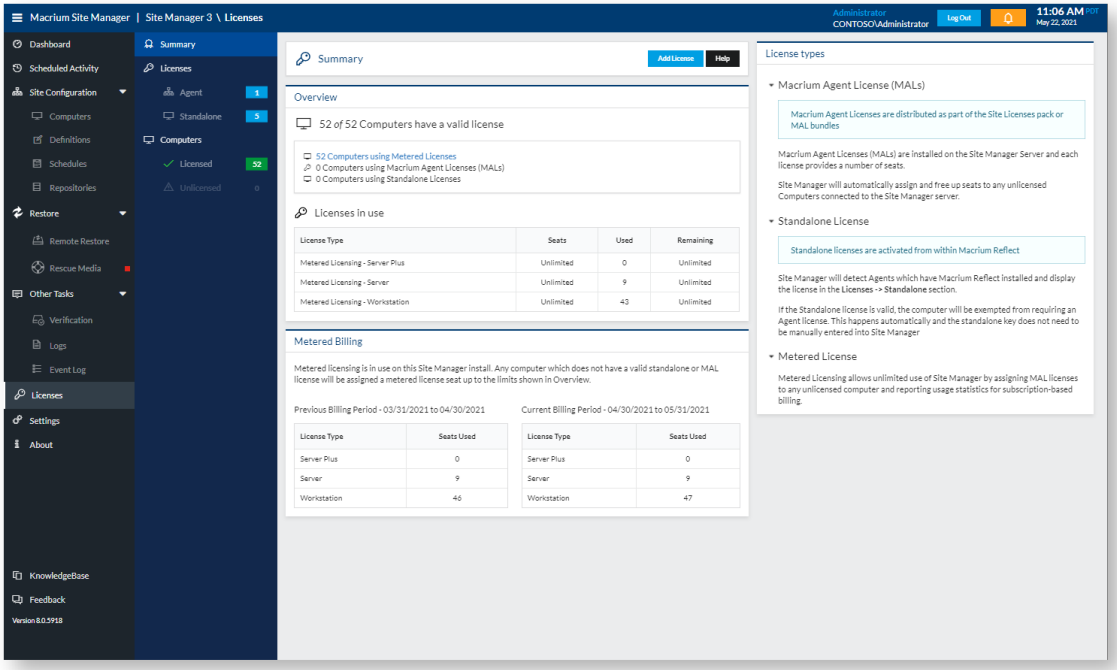
The event log contains a log of all the actions that have been taken in Site Manager and can be used to help review activity and audit the system. See Reviewing Event Logs for more details.



Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

The Licenses Page

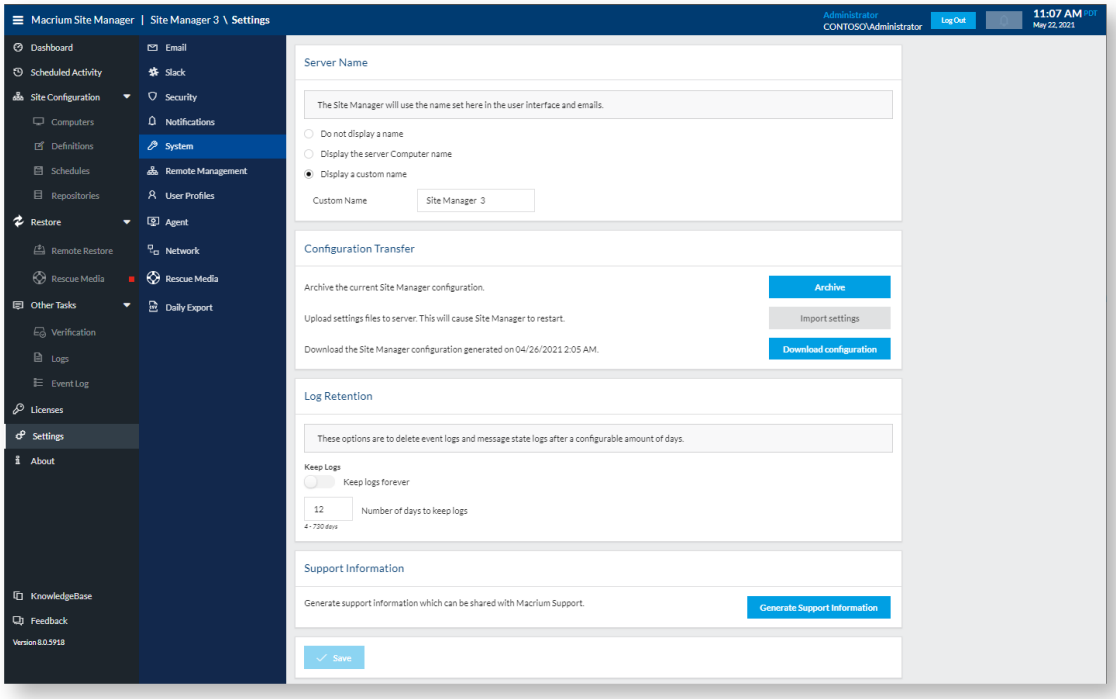
The Licenses page is used to display license information for connected clients and allow management of Macrium Agent Licenses to enable clients without standalone Macrium Reflect installed to be licensed and managed. See Licensing for more details.



The Settings Page

The Settings page contains settings for security, third-party integration and controls for features such as notifications. See Configuration and Security for more information.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



Installation and Update

Installing the Site Manager Service

The Site Manager service can be installed on any computer or Virtual Machine running Windows 7/Windows Server 2008 R2 or greater. As the service must be running to perform scheduled backups, it should be installed on a computer which is not turned off during these times.

SHA256 Driver Hashing

The Site Manager server uses driver components that require SHA-2 driver hashing. The Site Manager installer will fail on Windows 7 and Windows Server 2008 R2 unless an appropriate hotfix is installed See This Microsoft article for more detail. Later versions of Windows support SHA-2 hashing natively and do not require any hotfixes.

Download

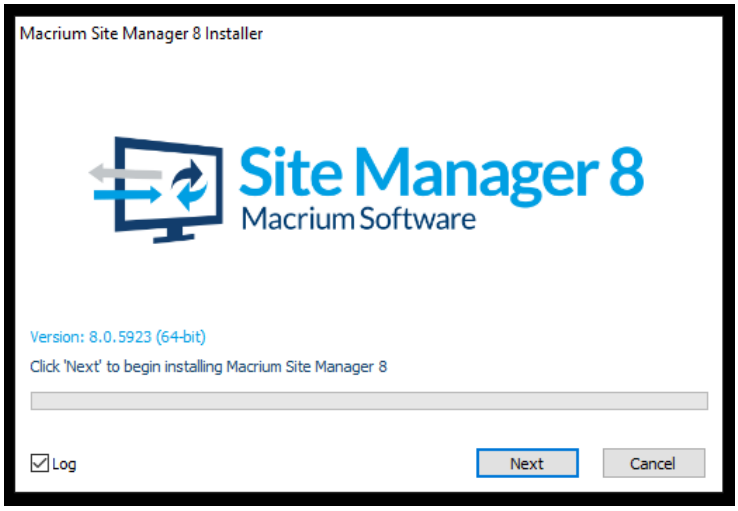
The Site Manager Server is available for download as either a 32-bit Windows Installer or a 64-bit Windows Installer. The version installed must match the architecture of the Windows OS.

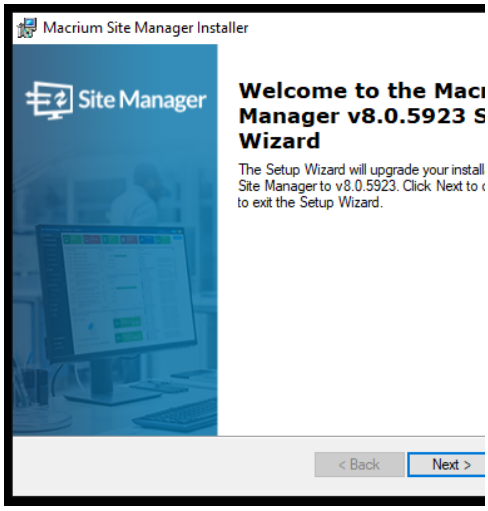
Download Site Manager for Windows 64-bit

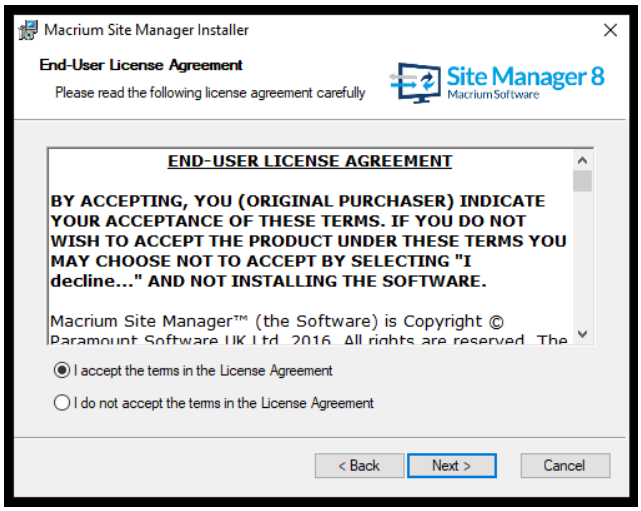
Download Site Manager for Windows 32-bit

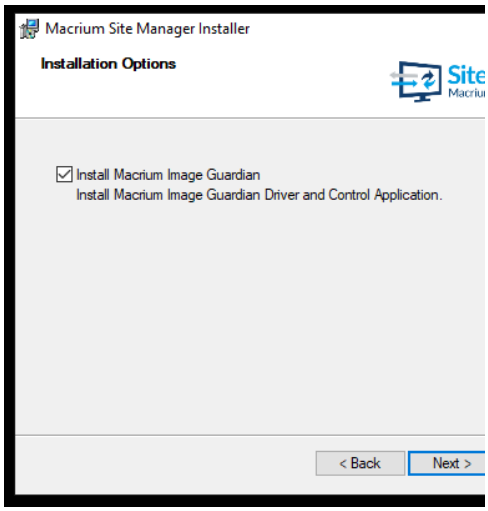
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

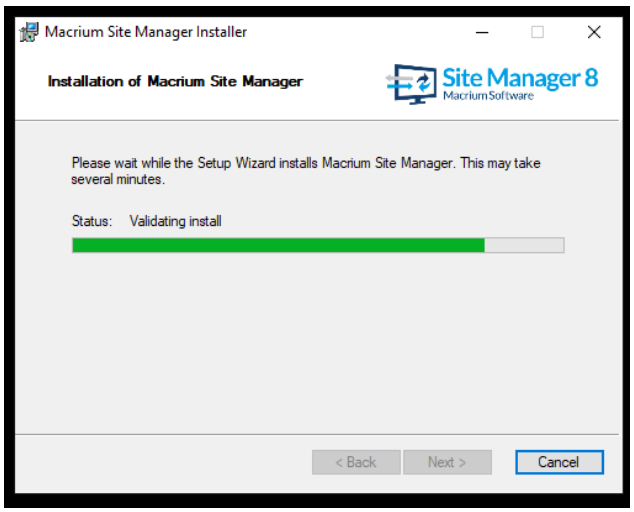
The installer provides a standard install interface:

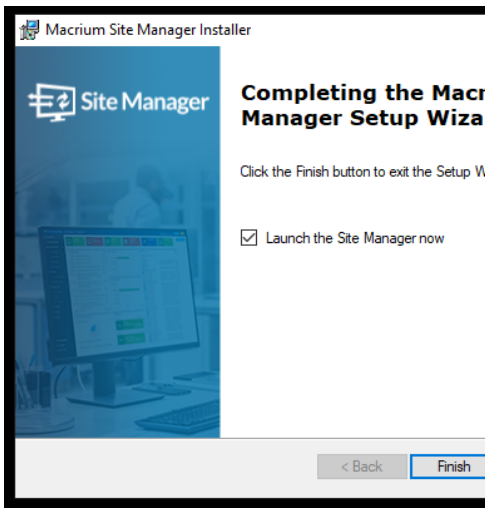












Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Install Options

During install, The following options are available:

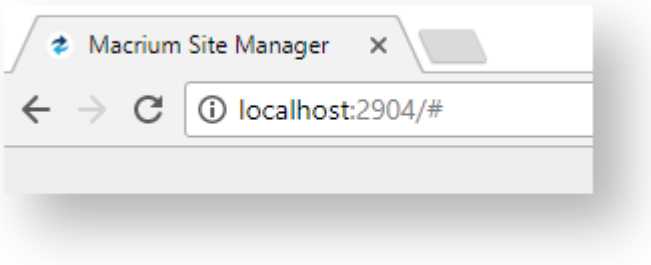
Option	Description
Install Macrium Image Guardian	If selected, the Macrium Image Guardian driver and configuration application will be installed with Site Manager. This can be used to provide additional anti-malware and anti-ransomware protection of Site Manager backup image files. See Macrium Image Guardian for more information
Launch the Site Manager now	If selected, a web browser will be launched with the Site Manager interface after **Finish** is pressed.

Initial Configuration

Once installed use a local web browser to connect to the running server on the default port 2904. (http://localhost:2904).

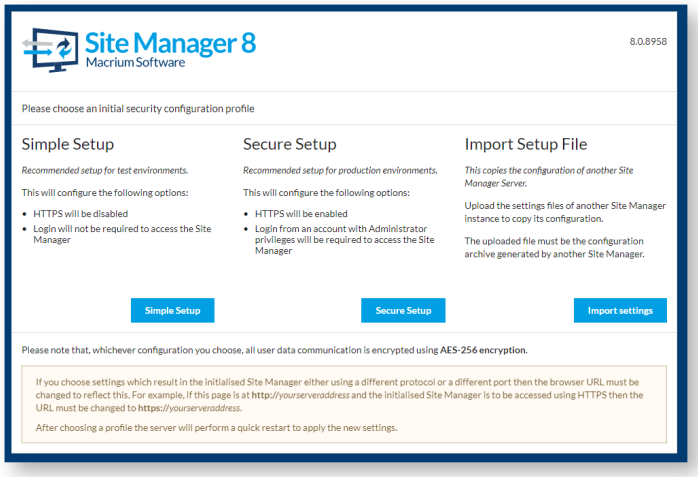
Upgrade Installs

If you are upgrading from a previous installation of Site Manager, the protocol (http or https) and port will be set to the previously configured values



The first time you access the web interface, you will be prompted to select a security level to complete the security configuration:

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



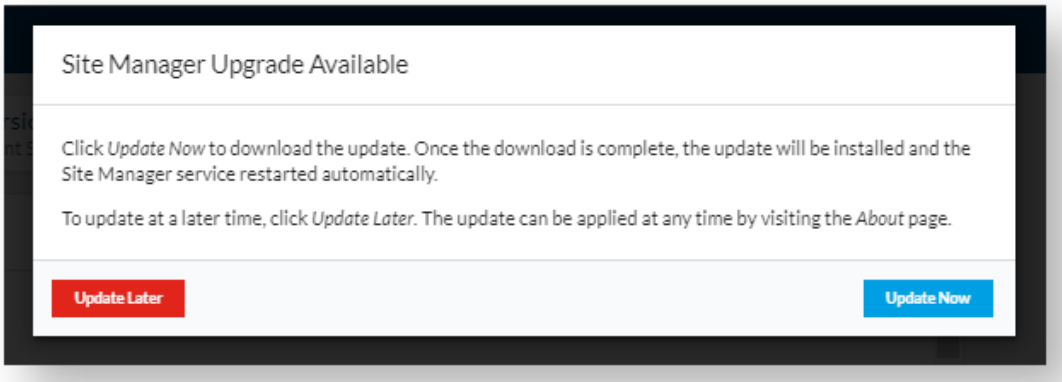
The recommended security level is **Simple Setup** for internal and test installations and **Secure Setup** for production environments. **Import Setup File** may also be chosen to import a saved configuration from another Site Manager server.

Note: These security settings may be changed at any time from the **Settings** page of Site Manager.

> After selecting your security configuration Site Manager will immediately restart

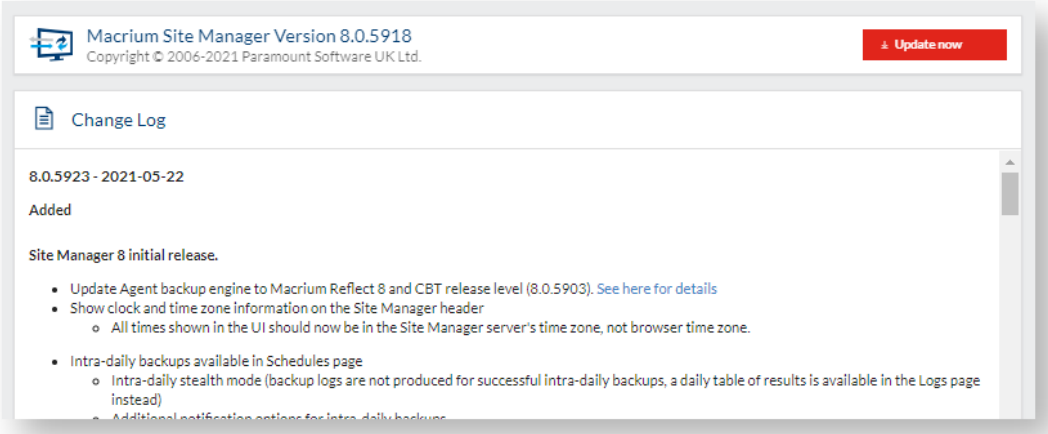
Update

The Site Manager service will periodically check for updates with Macrium servers. If there is an update available, the following message will be shown on login:



If you click **Update Now** on this message or visit the **About** page, and click **Update Now,** a download of the Site Manager will start.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



When the download completes, Site Manager will apply it and automatically restart. When the Site Manager service restarts, it will update the individual agents which are connected. Any offline agents will be updated as soon as they connect to the Site Manager.

> Any backups in progress during the update will continue and the agent performing the backup will not be upgraded until the backup has completed.
>
> Due to the time and network traffic that upgrading causes, we recommend that upgrading the Site Manager is only done when there are no scheduled backups running.

Licensing

Overview

The Site Manager server can be installed and run with no license key or restriction on running. However, when adding computers to the Site Manager to be managed, each computer requires a license to be successfully managed.

There are two models for licensing - a license is deployed to the client computer as part of a standalone Macrium Reflect install or licenses can be added to the Site Manager server and dynamically allocated to client computers as needed. Licenses allocated in this way are called Macrium Agent Licenses

Standalone Licenses

If a computer to be managed already has an installation of Macrium Reflect with a valid Macrium Reflect license, this computer can be managed by Site Manager with no further licensing required. The Site Manager will automatically detect that the client computer has a valid Reflect license when it connects for the first time after the agent has been installed - no configuration is necessary.

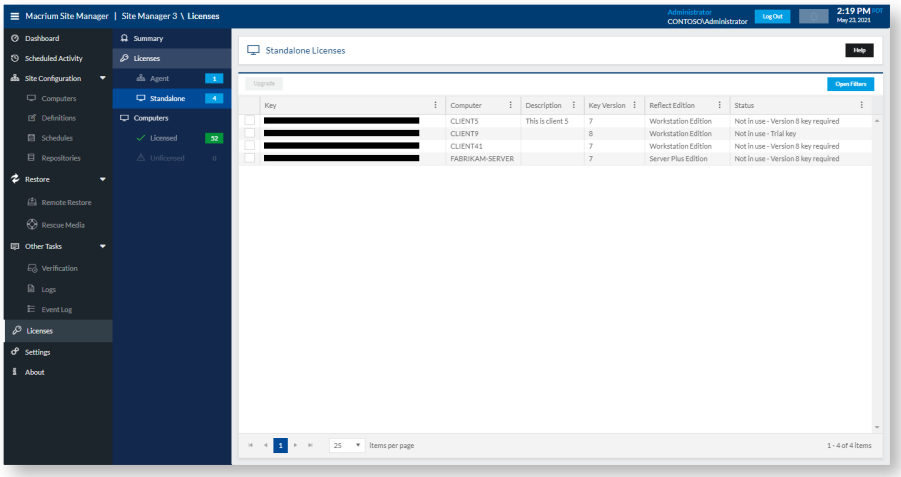
Managing computers with standalone Macrium Reflect licenses has the following benefits -

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

- Ease of transition from managing computers individually to via Site Manager - no licensing changes are needed to start using Site Manager
- No dependency on Site Manager server - if a computer has a standalone license, then it will be able to run and use Macrium Reflect even if it cannot contact the Site Manager server. This is especially useful for laptops and other devices which are not always connected to the LAN
- Extended options for servers - Individual servers which have the Server Plus edition of Macrium Reflect can still use Reflect to conduct Exchange and SQL backups, even though these features are not included with the Macrium Agent License edition of Reflect.

Macrium Reflect 8 Home, Workstation, Server and Server Plus licenses qualify as valid licenses for Site Manager. Licenses earlier than version 8, Free Edition or any trial licenses are not valid.

Computers using standalone keys may be reviewed on the **Licenses Standalone** section. This shows all computers with standalone keys and whether they are valid for use within Site Manager:



License keys can be upgraded by selecting the appropriate license and using the **Upgrade** button. This will check a version 7 key with Macrium license servers and if the key is eligible for upgrade, the key will be upgraded and set on the Agent computer, so that it appears in Reflect. For this function to be available, the following conditions must be met:

- The computer must be running the most recent Agent version
- The computer must be running at least Reflect 7.3.5854 (This version will accept the upgraded version 8 key as valid)
- It must have a version 7 key
- The Agent must be in the connected state

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Macrium Agent Licenses

Macrium Agent Licences (MALs) are installed on the Site Manager Server and each license provides a number of seats. These seats are automatically assigned to computers as they are connected to the Site Manager server. If a computer is removed from the Site Manager server, the seat is freed for use elsewhere. This makes using MALs quick and easy to use as they require no special client configuration. Multiple seats can be managed with a single key, making key and license management easier.

The drawback of these licenses are that they are dependent on communication with a Site Manager server - if the client computer cannot contact the Site Manager server, the agent cannot be used to perform backups as a standalone edition of Reflect could.

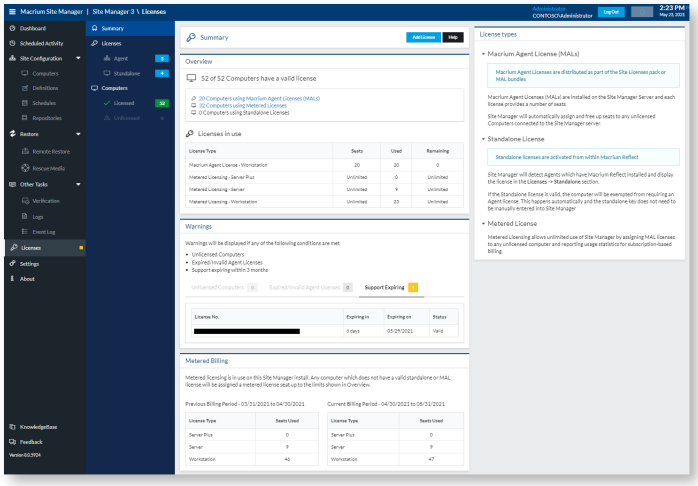
Metered Agent Licenses

Metered licensing is available to MSPs and other Macrium partners. This provides unlimited use of Site Manager and provides regular billing on actual use counts. Site Manager reports usage counts to the Macrium license servers, which use the information to produce billing based on high watermark usage.

Metered keys are managed as a special Agent license key with a type of **Metered**. Only one metered key per Site Manager is permitted and when in use, additional statistics about metered license usage is displayed on the **Status** page.

Managing Macrium Agent Licenses

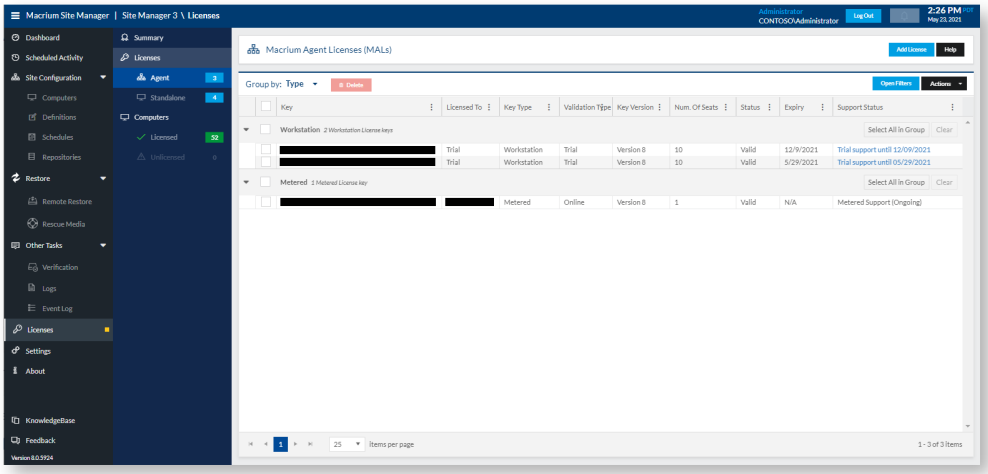
The **Licenses** section of the Site Manager interface provides an overview of Macrium Agent License seats available and used in the **Summary** section.



This page also displays warnings if any agents are unlicensed or there is a shortfall in the appropriate license type. This may occur when there are insufficient workstation licenses for all workstation computers but excess server licenses. In this case, Site Manager will assign a server license to a workstation.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

The individual Macrium Agent License keys can by added, removed and viewed on the **Licenses Agent** tab:



The fields shown are.

Field	Description
Key	The license key
Licensed To	The user or company the key is licensed to
Key Type	The type of key. This may be **Server**, **Workstation**, **Server (VM)** or **Metered**
Validation Type	**Trial**, **Online** or **Offline**. If a key is added when there is no working internet connection, it can be added as an offline key if you have an appropriate validation key from Macrium. Online validated keys require regular checks with the Macrium license server, but are easier to add, remove and manage.
Key Version	The version of Site Manager the key is valid for. Currently only Version 8 keys are available.
Num. of Seats	The number of computers which may be licensed by this key.
Status	**Valid** or **Invalid**. This shows the status of the key as determined by the Macrium license server
Expiry	The date the key expires if the key is a trial.
Support Status	Whether this key has paid support and when the support expired/will expire

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Pressing the **Add License** button will allow you to add a license. Please note if you enter an older version 7 key, you will be prompted to upgrade the key to version 8, if the key is eligible for upgrade. Version 6 keys cannot be added at all, please contact Macrium Support for assistance in upgrading these keys.

In addition to multi-seat Macrium Agent License keys, standalone keys from Macrium Reflect (Workstation and Server editions) may be added as 1 seat Macrium Agent Licenses. These licenses are treated like any other Macrium Agent License and are not tied to specific computers.

This is intended to ease the transition to using Macrium Agent Licenses for customers who have a number of existing Reflect licenses. If you want to use the Reflect license as a standalone license on a specific computer connected to Site Manager, you do not need to enter the license here

Offline Keys

If the Site Manager server is not connected to the internet, adding a MAL will display a code and link to the Macrium website which can be used to activate the key for offline use and provide a validation key which can be entered in the Site Manager interface to enable the offline key.

Configuration and Security

- Security
  - Agent Communications
  - Web Interface Access
- Configuration
  - Email
    - SMTP Configuration
    - Notification Email
    - Backup Summary
  - Slack
  - Security
    - Access Restriction
    - User Permissions
    - Connection Settings
    - Agent Security
  - Notifications
    - Warnings
  - System

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

- Server Name
- Configuration Transfer
- Log Retention
- Support Information
- Remote Management
- User Profiles
- Agent
- Network
  - Proxy Settings
- Rescue Media
  - Working Directory
  - Export Drivers
- Daily Data Export

This section is intended to discuss the security involved in Site Manager and show how these features and other features can be configured through the Site Manager interface.

Security

The various forms of network communication in Site Manager have some built in security with options for further configuring them.

Agent Communications

Communications between agent and Site Manager server are always encrypted using 256-bit AES encryption. This happens automatically, key generation, negotiation and encryption are all done without any additional configuration. In addition, a passphrase can be set in the Site Manager. This passphrase is set on any successfully connected agent and prevents any other Site Manager taking over that agent unless the new Site Manager has the same passphrase set.

The purpose of this passphrase is for use in high integrity or untrusted environments where a guarantee that only the Site Manager server that has been configured for that agent can access that agent is required.

> If a passphrase has been set on an agent, it will fail to connect to a Site Manager which does not have the matching passphrase set. Reinstalling the agent will reset the passphrase.

The agent passphrase can be set in the **Agent Security** section of the **Security** settings below.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

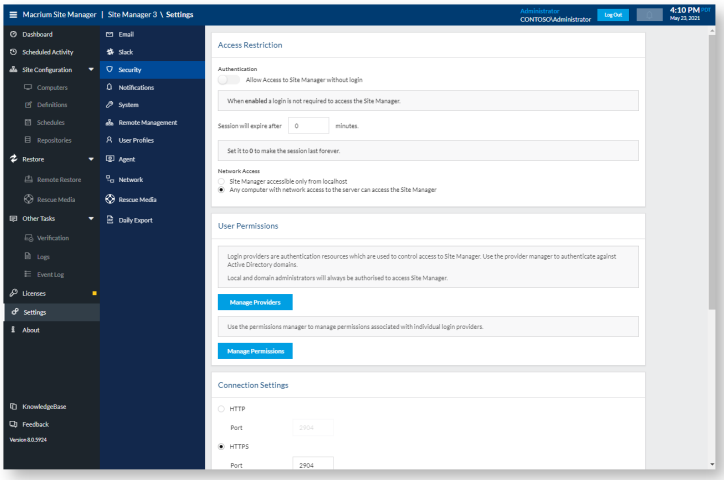
Web Interface Access

The web interface used to access the Site Manager interface can use HTTP or HTTPS. By default the Site Manager uses HTTP access but is only accessible from the computer it is installed on. This restriction can be removed in the **Connection Settings** section of the **Settings** page.

If the interface is exposed to a potentially insecure network or the internet, we recommend using HTTPS. When HTTPS is first enabled, a default self-signed certificate is used. This certificate is not recommended for use outside secure networks as it is shipped with every Site Manager installation. Any certificate in OpenSSL .PEM file format can be used in place of the built in certificate. If you have keys in a different format, the OpenSSL command line utility can convert a variety of formats. See https://www.openssl.org for details.

Configuration

To configure the settings for Site Manager, access the **Settings** page from the main menu:



This is divided into a number of sections which are explained in more detail below

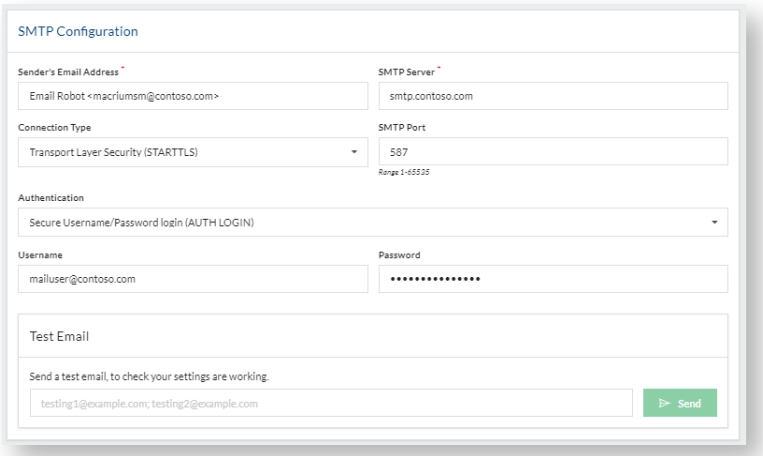
Email

The Email section is divided into three subsections - **SMTP Configuration** for setting up server details, **Notification Email** for configuring where notifications (Backup start, end and others) are sent to and **Backup Summary** for configuring daily status emails.

SMTP Configuration

This section allows Email server settings to be configured, including security settings.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

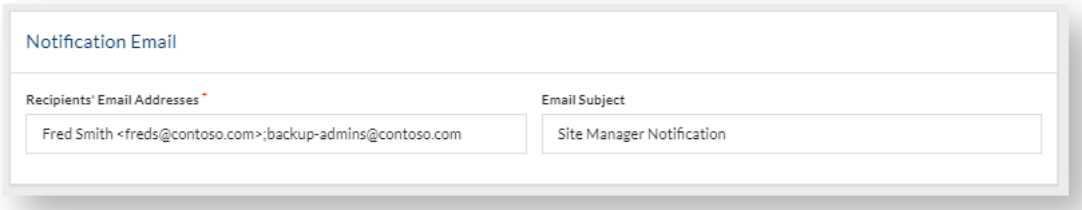


Option	Description
Sender's Email Address	The email address the summary emails will be sent from.
SMTP Server	The address (DNS or IP) of the SMTP server to use for sending.
Connection Type and Port	The type of connection used by the SMTP server. Supported options are: • Plain Text • Secure Sockets (SSL/TLS) • Transport Layer Security (STARTTLS)
Authentication	The authentication method used by the SMTP server. Supported options are: • None • Auto-Detect • Challenge/Response Authentication (CRAM-MD5) • Secure Username/Password login (AUTH LOGIN) • Username/Password login (AUTH PLAIN) • Microsoft NT LAN Manager (NTLM)
Username and Password	The username and password for the SMTP server. If left blank, no username will be used.
Test Email	Sends a test message to the recipients entered in the test box. If there are errors in the send, they will be reported back.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Notification Email

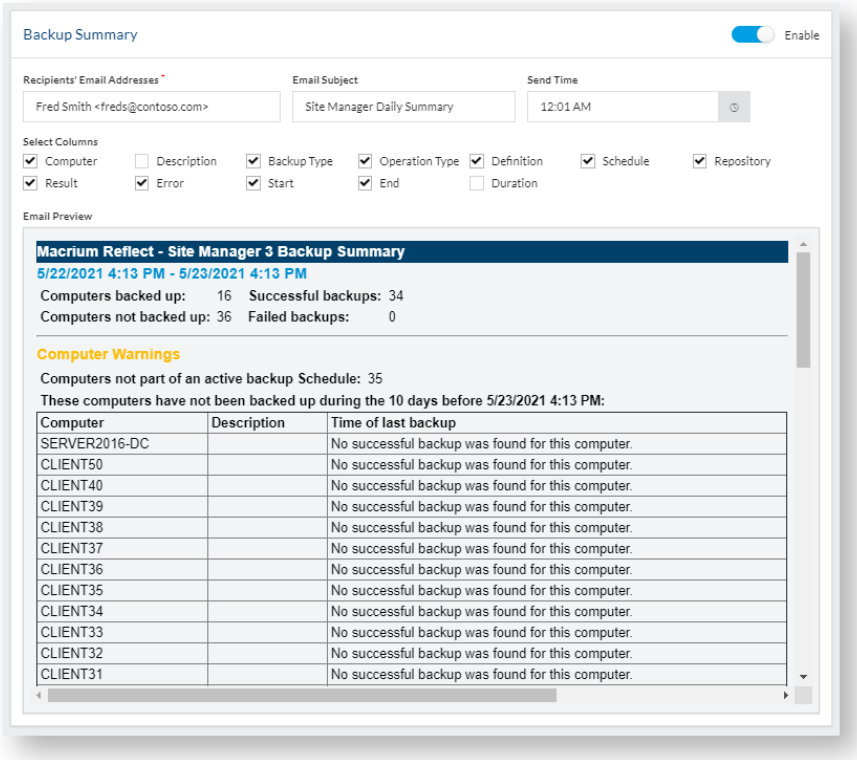
This section allows the recipients and subject to be specified for notification emails. These setting are applied to any notification emails sent according to the **Settings Notifications** section.



Option	Description
Recipients' Email Addresses	Email addresses to send notification emails - may be a semicolon separated list
Email Subject	Subject to be set on notification emails

Backup Summary

The summary section allows configuration of daily backup summary emails as below:



The options available are:

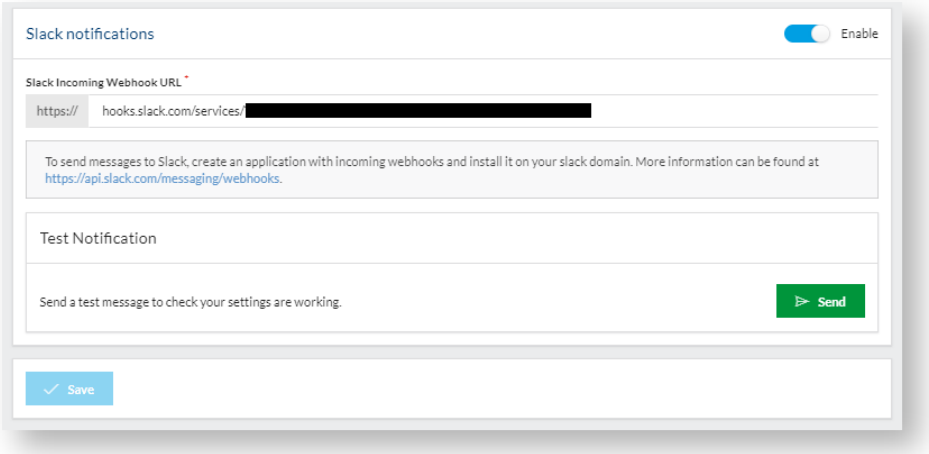
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Option	Description
Enable	This toggle can be used to turn summary emails on or off
Recipients' Email Addresses	Email addresses to send notification emails - may be a semicolon separated list
Email Subject	Subject of the email
Send Time	The time when the daily email will be sent
Select Columns	Which columns should appear in the summary email. Changes to this section are reflected in the email preview underneath

A preview of the daily email with the selected columns is shown below the settings.

Slack

The Management Console supports sending notifications to Slack. Once configured, the types of notifications can be configured in the Notifications section, below.



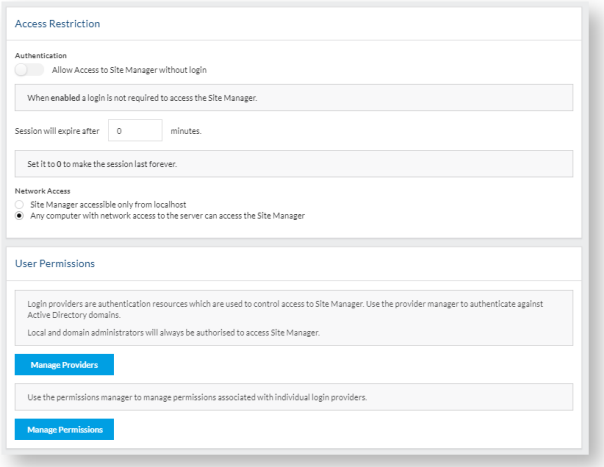
Option	Description
Enable	Toggle this to enable/disable Slack notifications.
Slack Incoming Webhook URL	Webhook to use to post Slack messages. This can be configured in Slack management by creating a private app. See Slack Webhooks for more information

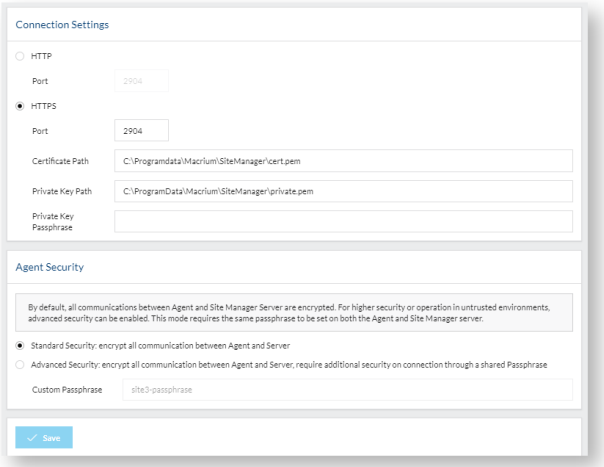
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Option	Description
Channel	Here you can specify which channel you wish to post to in Slack. You may wish to create a new channel in Slack for your notifications.
Test Notification	This button sends a test message the the slack channel configured above.

Security

Here you can customize the various security options for the Management Console.





Access Restriction

This section controls general access settings to Site Manager - which network interfaces the Site Manager UI is available on and whether user login is required.. Finer control is provider under the **User Permissions** section.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Option	Description
Allow Access to Site Manager without login	If enabled, any new connections to Site Manager will allow direct access without a login. This may allow unauthenticated users access to configuration and contents of backups and should only be used in a secure environment.
Session will expire after X minutes	Session expiry time can be set so that if the Site Manager interface is left open in a web browser, it will automatically log out after a specified number of minutes being idle.
Network Access	Setting this to **Site Manager accessible only from localhost** will make the Site Manager interface only accessible from a web browser running on the server itself. Otherwise the interface is available from any IP address.

User Permissions

Dialogs to manage login providers and Site Manager access permissions can be accessed here. The provider manager is used to create, configure and delete login providers and the permissions manager is used to set permissions for each provider. For more information see: Access Control.

Connection Settings

This section allows you to configure HTTP/HTTPS connection settings for the Management Console. The defaults should be fine for most installations but you may wish to provide your own SSL credentials and possibly alter the ports if they conflict with other applications on your server.

By default, Site Manager supplies a self-signed certificate for HTTPS operation. As this key is shared between all Site Manager installations, it should not be considered secure if the Site Manager server is exposed to the internet or in any sensitive deployment. In these cases, we recommend an alternate key is used.

The keys supplied must be in OpenSSL .PEM format.

Different certificate management systems and providers use different names and file extensions to identify certificate files. The Site Manager server requires files using PEM format, under any file extension. These files can be identified by opening them in a text editor:

- Valid certificate files will contain a Base64 encoded certificate in a section denoted by `-----BEGIN CERTIFICATE-----`
- Valid private key files will contain a Base64 encoded key in a section denoted by `-----BEGIN PRIVATE KEY-----`
- If both the certificate and key are in the same file, the same file should be specified for both fields in Site Manager configuration

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Option	Description
Port	The port used by the Site Manager HTTP and HTTPS servers
Certificate path	The public certificate to be used by the internal Site Manager HTTPS server
Private key path	The private key which matches the certificate specified in the **Certificate path**
Private key passphrase	If the private key file requires a passphrase to use, it can be set here

Agent Security

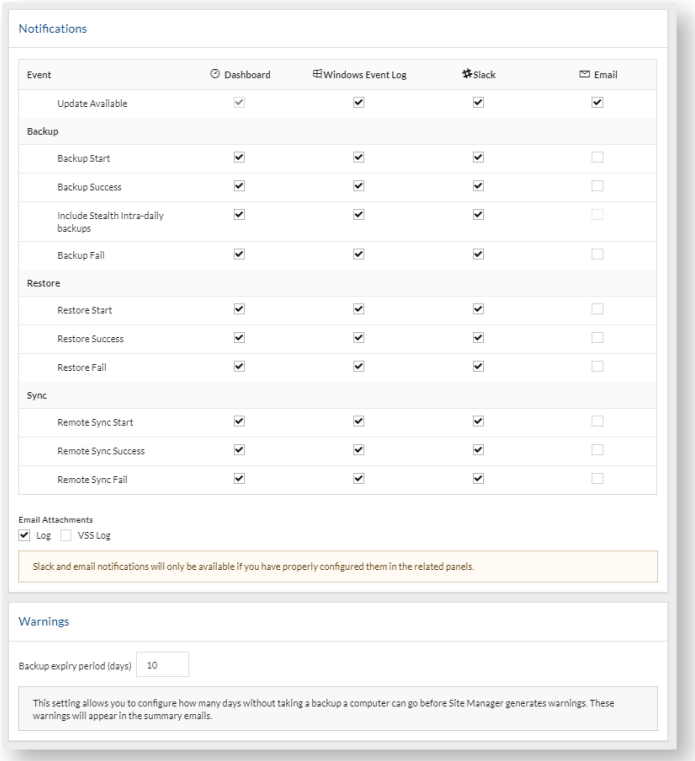
This section contains additional security settings for Agent communications. It allows an additional passphrase to be set - using a passphrase means that once communication has been established with an agent on a remote computer, the remote computer will only communicate with Site Manager servers which have the same passphrase set. This is intended to prevent any rogue processes emulating a Site Manager server and gaining access to the agent on a remote computer.

If a computer is added after previously having a passphrase set, the computer will be listed as **Unauthorized** in the computers list. To manage the computer, either the Site Manager server must have the correct passphrase, the passphrase on the agent must be changed (Requires local administrator access to the computer) or a passphrase can be entered on the Site Manager server to allow one-off access.

Notifications

Here you can select which notifications appear in the User Interface, the Windows Event Log, over Slack or email (if configured).

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



The options available are:

- **Update available** - sent when a software update to the Management Console is available.
- **Backup Start** - sent when a backup has started to run on a managed computer
- **Backup Success** - sent when a backup has completed successfully on a managed computer
- **Include Stealth Intra-daily backups** - this controls whether backup success emails should include intra-daily backups with the stealth option set. These backups do not create normal log files unless an error is encountered.
- **Backup Fail** - sent when a backup has completed unsuccessfully on a managed computer
- **Restore Start** - sent when a restore has started to run on a managed computer
- **Restore Success** - sent when a restore has completed successfully on a managed computer
- **Restore Fail** - sent when a restore has completed unsuccessfully on a managed computer
- **Remote Sync Start** - sent when a repository starts remote synchronization with another server
- **Remote Sync Success** - sent when remote synchronization with another server succeeds
- **Remote Sync Fail** - sent when remote synchronization with another server fails

Additionally, there are options to set whether relevant backup logs should be attached to emails and how many days without a backup should be allowed before the daily summary email warns that a computer is unprotected.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

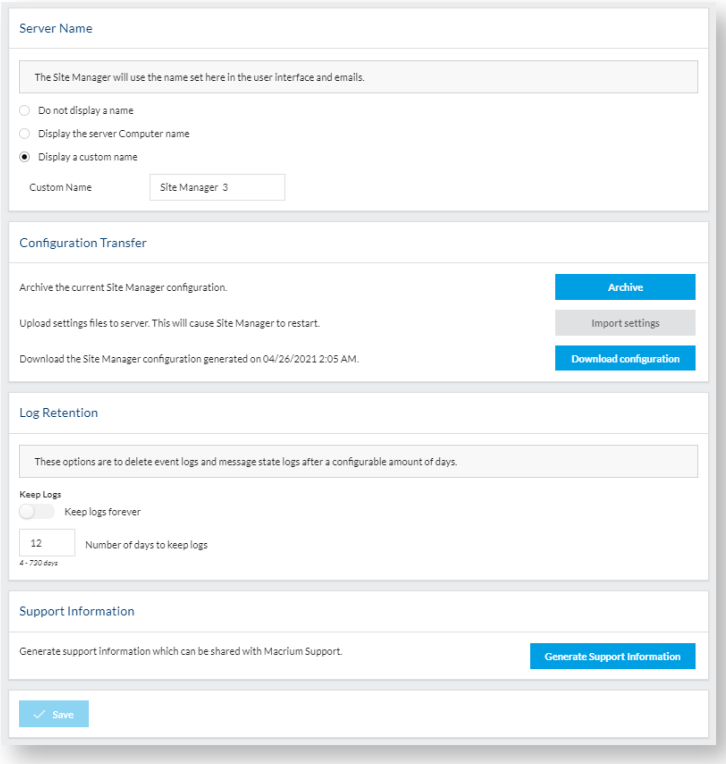
Warnings

The number of days a computer can go without backups before being flagged as having an error in the dashboard, computers page and daily status email is configurable here via the **Backup expiry period** setting.

System

The system section contains options for modifying the behavior of the overall system. The options available are as follows:

Server Name



Option	Description
Server Name	Allows a custom server name to be set. This server name will be shown in the title/tab bar of the browser, at the top of the Site Manager interface and in email subject lines. This allows organizations with multiple Site Manager installs to easily tell them apart. The naming options are: • **Do not display a name** - this is the default setting • **Display the server Computer name** - uses the NetBIOS name of the server

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Option	Description
	• **Display a custom name** - the name entered in the **Custom Name** field will be used

Configuration Transfer

This section has options for backup up, downloading and restoring the Site Manager configuration:

Option	Description
Archive	Update the configuration archive on the Site Manager server with the current Site Manager configuration. Once complete, the timestamp shown by the **Download configuration** option will be updated
Import settings	Upload a previously create Site Manager configuration backup and apply the settings to this Site Manager server. The current Site Manager configuration will be overwritten
Download configuration	Download the latest created archive in the browser. This can be used to provide a backup of Site Manager settings in case of server hardware error

Log Retention

This section allows logs (both backup logs and event logs) to be automatically deleted after a number of days. This will only happen if the **Keep Logs Forever** option is unselected. This option will affect both the backup logs and event logs.

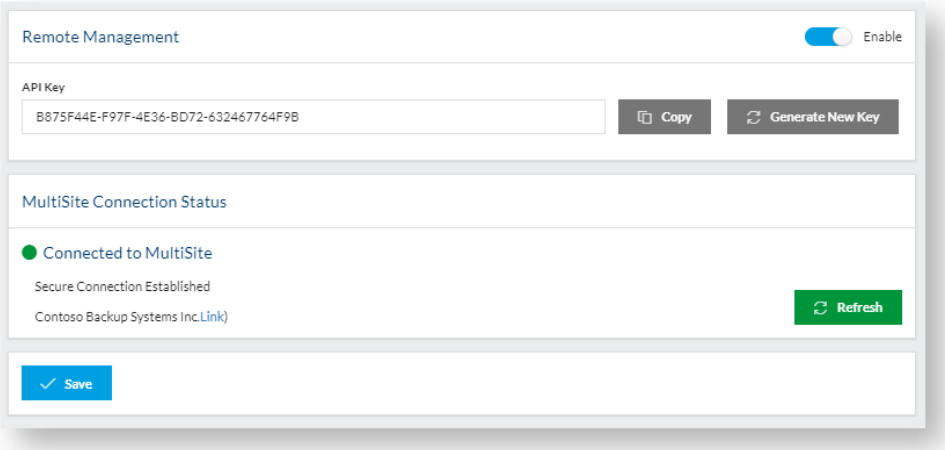
Support Information

This section allows gathering of support information and upload to Macrium servers or download as a zip file. It should only be used under the direction of Macrium Support.

Remote Management

The Remote Management section controls integration with Macrium MultiSite. If remote access is enabled and the HTTPS port configured in the **Security** section is exposed to the internet, the Site Manager can be managed by Macrium MultiSite.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



The options in the **Remote Management** section are as follows:

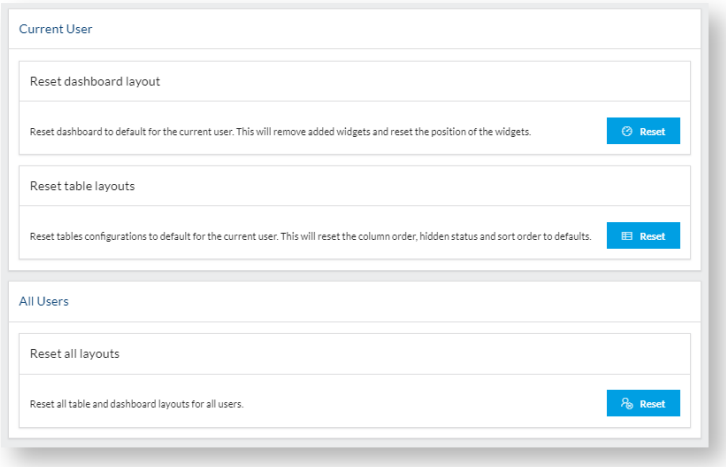
Option	Description
Enable	Enables the remote management interface for Macrium MultiSite on the same port used for HTTPS access. This does not affect HTTPS access.
API Key	This key is required to authorize MultiSite to access the Site Manager.
Copy	Copies the API key to the clipboard to make transferring it easier.
Generate New Key	Generates a new API key, replacing the old key. Note that if this Site Manager is managed by Macrium MultiSite, the key must be updated in MultiSite for continued access.

The **MultiSite Connection Status** section will only appear if Remote Management is enabled. This section will show the current status of the Site Manager's connection to MultiSite. The **Refresh** button retries the MultiSite connection if there are issues.

User Profiles

This section controls the per-user configuration of the Site Manager Dashboard and interface

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

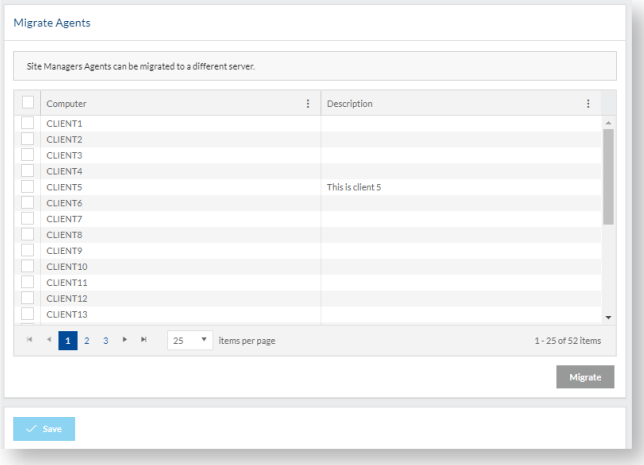


Option	Description
Reset dashboard layout	This option will restore the dashboard to the default layout, removing all widget layout and notification tile customization. This only applies to the currently logged in user
Reset table layouts	This option will remove any changes to the table layouts on all Site Manager pages. This includes moving, hiding or sorting columns. This only applies to the currently logged in user
Reset all layouts	Removes all customization for all users and resets Site Manager to default layout settings

Agent

This section controls how Site Manager agents and remote agent installation work

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



Option	Description
Install Settings - Quiet Agent Install	Setting this option will change the default install options for the remote agent install to install the agent without creating desktop or start menu shortcuts. Quiet install settings will only be updated on an agent when the remote install feature is used or the agent is upgraded through Site Manager
Install Settings - Auto Update	If this option is set, the server will automatically update the agents when a new version is available
Maximum Simultaneous Updates	This option specifies the number of updates that will be performed simultaneously
Install Credentials	

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Option	Description
	This option allows you to set credentials which will be used to install remote agents. This is useful if the majority of computers you wish to install agents on are on a domain which is not the same one used to log in to the Site Manager server
Server Connection Details	To change these fields while agents are connected will cause the server to send the new details to the **connected** agents. When an agent receives the new details, it will drop the connection and try to reconnect to the server. If the agent is not able to reconnect or if it wasn't connected when the details were changed the details must be manually set on the agent via Agent Config tool or remote install
Server Connection Details - Server IP	Additional IP addresses the Agent should use to communicate with the Site Manager. Any IP addresses here will be tried before DNS name resolution or NetBIOS name resolution is attempted.
Server Connection Details - Server DNS	Additional DNS names the Agent should use to look up the Site Manager server IP address. Any DNS addresses here will be tried before NetBIOS name resolution is attempted.
Server Connection Details - TCP Port	The TCP/IP port used by Site Manager to communicate with Agents. If this is changed, the Site Manager server will update all connected Agents and restart.
Migrate Agents	This section allows Agents to be moved from one Site Manager server to another - the selected Agents will attempt to connect to the server using the NetBIOS, DNS or IP addresses specified and if successful, the Agent will connect to the new server and drop into the disconnected status on the current server. If the Agent cannot contact a Site Manager server using the entered network details, they will remain connected to the current Site Manager server.

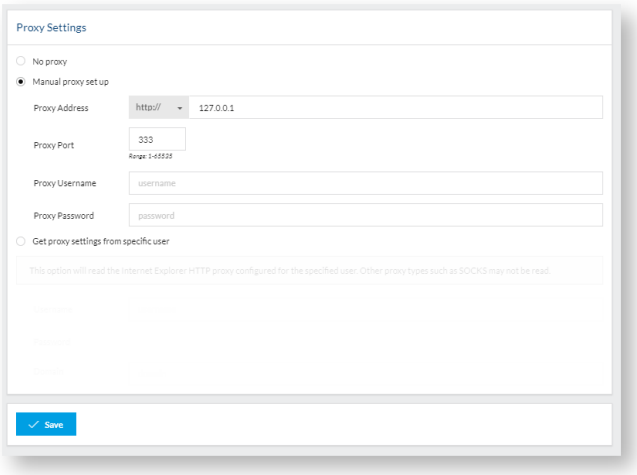
Agent Server Connection

When installed via the Remote Install feature, Agents will automatically be configured with the NetBIOS name of the Site Manager server, plus any details configured here. The Agent will try all connection details to connect to a Site Manager server.

Network

This section contains options controlling how the Site Manager server access the internet.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



Proxy Settings

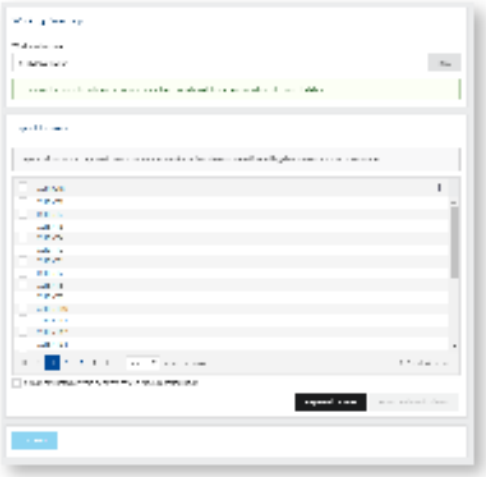
A proxy server may be configured here. Site Manager will use this for all HTTP/HTTPS requests to the internet.

Option	Description
No Proxy	Site Manager will access the internet directly
Manual Proxy Setup - Proxy Address	This is the address and type of the proxy server to use. The proxy type is selected from a dropdown (HTTP, HTTPS and SOCKS options)
Manual Proxy Setup - Proxy Port	Port of the proxy server
Manual Proxy Setup - Proxy Username	Username used to authenticate with the proxy server
Manual Proxy Setup - Proxy Password	Password used to authenticate with the proxy server
Get Proxy Settings From Specific User	If account details for an account on the local domain or computer are entered here, the Site Manager server will attempt to read Internet Explorer proxy information from this user's profile on the Site Manager server.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Rescue Media

This section contains options controlling how Site Manager builds rescue media.



Working Directory

The Working Directory is the folder on the Site Manager server which is used as temporary space for Rescue Media building and to store the Rescue Media ISO images.

Option	Description
Working Directory	The path on the server to use for the Rescue Media working directory. This must be a local filesystem running NTFS. If this directory is changed, the old directory will be left intact and must be deleted manually.
Test	Tests that the Rescue Media working directory is accessible and writable.

Export Drivers

Site Manager collects drivers needed to build Rescue Media from connected Agents. These drivers may be exported for use in disaster recovery by using the **Export all Drivers** or **Export Selected Drivers** options. This will copy all the drivers to the **drivers\export** folder in the Rescue Media working directory,

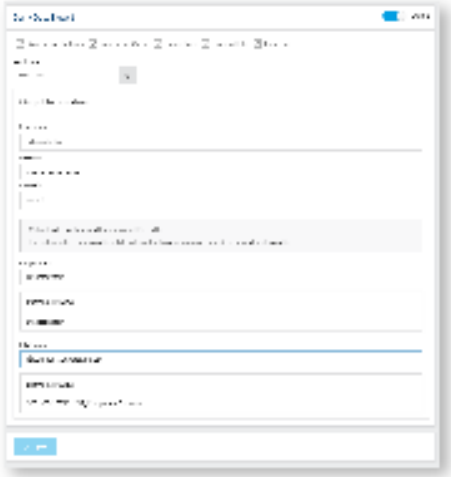
The **Group extracted drivers by Agent Rescue Media configuration** option places the exported drivers into subfolders based on the relevant Windows PE version for that computer - e.g. all computers which require Rescue Media based on Windows PE 10 64-bit will have their drivers exported to the **drivers\export\PE10x64** folder.

This can be useful when extracting drivers to create custom rescue media.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Daily Data Export

This section controls Site Manager's creation of a number of CSV files that can be exported on a daily basis to assist in auditing, third-party integration or custom scripting.



The initial options allow the types of export to be selected and the export time. The export types are:

Export Type	Description
Repository Contents	A list of backup images stored in each repository, along with type, path and size information
Repository Usage	This generates two files - one with an overview of each repository, including status, path, free space and space used by backups. The other file contains a breakdown of space used on each repository broken down by computer, including number of backups and disk space usage changes since last export.
Computers	A list of agent computers, along with status, last backup time and other information from the **Computers** page.
Backup Data	A list of backups attempted in the last 24-hours, including success or failure
Event Log	The last 24 hours of the event log

This section configures the file and folder information for the export. The credentials used to write the files can be controlled by specifying a username, password and domain for the account. If left blank, the SYSTEM account on the Site Manager server is used.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

The folder and file paths can be specified here using replaceable parameters - this allows a number of configurations, including creating each day's exports in the same place (overwriting old files), giving each day's export file a name based on the date, or placing each day's exports into a different subfolder.

Replaceable parameters are specified by placing them in curly braces with a dollar character - `{$example}`. Available parameters are:

Parameter	Description
`{$date}`	The date in `YYYYMMDD` format
`{$time}`	The time in `hhmm` format
`{$isotime}`	ISO 8601 timestamp of the export time - `YYYY-MM-DDThhmmss`
`{$servername}`	Name of the Site Manager server as specified in **Settings System**
`{$exporttype}`	Type of export. When exporting multiple export types, this should be used to prevent each export type overwriting the other. Possible values are: • Repository Contents • Repository Status • Repository Changes • Computers • Backup Data • Event Log
`{$increment}`	If a file already exists with the name generated, the export will overwrite the old file with the new one unless **increment** is used. Increment is a simple number that is incremented to create a unique file name for the export. For example, if the filename field is set to `filename.csv`, each day, the old file will be overwritten. If the field is set to `filename-{$increment}.csv`, the first day's export will create the file `export-1.csv`, the second day will create `export-2.csv` etc

Access Control

- Introduction
- Login Providers
- Managing Login Providers
- Configuring Permissions

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Introduction

Site Manager can be configured to allow different users on the Site Manager server or a Windows Active Directory Domain to login to Site Manager.

By default members of the Administrators group on the Site Manager server and members of Domain Administrators on the Site Manager server's domain can login. Additional domains and permissions can be configured as described below.

Login Providers

Login providers serve as the interface between Site Manager and an authentication resource. There is a unique login provider for each authentication resource so that permissions for each resource can be managed independently by configuring the associated provider. Three types of Login Provider currently exist:

Login Provider Type	Authentication Resource	Included by Default	Notes
Server Local	User Account Control	Yes	Authenticates local users. Local administrator accounts will always have permission to access Site Manager.
Primary Server Domain	Active Directory	Yes (if the Site Manager server is joined to a domain)	Authenticates users on the domain the Site Manager server is joined to. It is created automatically and can not be removed by the user. Domain Administrators can log in using this provider. **Domain disconnections** If the server is moved from its domain then the provider will be converted to a Domain provider. A new Primary Server Domain provider will be created when Site Manager upon reconnecting to a domain.
Secondary Server Domain	Active Directory	Yes (if the Site Manager server is joined to a domain in a forest)	Authenticates users on domains within the forest the Site Manager server is joined to. It is created automatically and can not be removed. **Domain disconnections** If the server is moved from its domain then the provider will be converted to a Domain provider. A new set of Secondary Server Domain providers will be created on start up.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Login Provider Type	Authentication Resource	Included by Default	Notes
Domain	Active Directory	No	This provider interfaces with Active Directory domains other than that which the Site Manager server is connected to.

Active Directory compatibility

Site Manager must connect with a Domain Controller which supports LDAP v3 for permissions to be set for accounts on the Domain. LDAP over SSL will be used if available.

Managing Login Providers

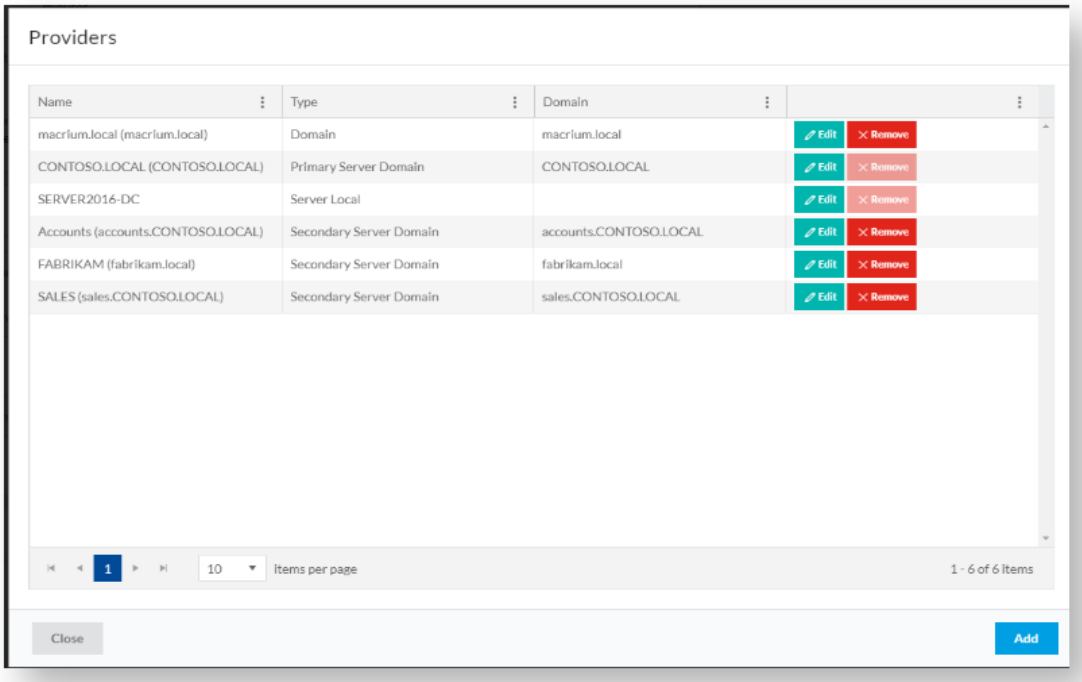
Disabling Domain Forest Searching

Site Manager automatically creates Local, Primary Server Domain and Secondary Server Domain providers on startup.

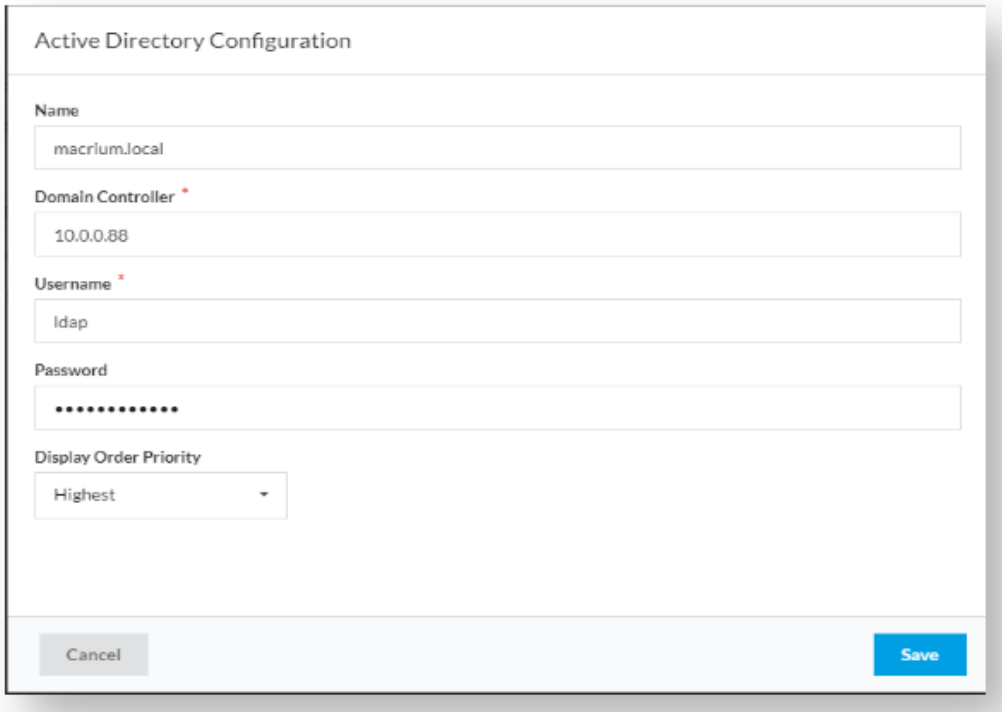
Users can stop Site Manager creating domain providers by setting the registry value "Configure default providers" in the key "HKEY_LOCAL_MACHINE\SOFTWARE\Macrium\Site Manager" to 0. This will prevent Site Manager from creating any providers except the primary domain and local computer providers.

While the automatic providers should cater for most needs, custom domain providers can be created to connect to domains outside of the forest the Site Manager server is in. Beware that members of authorized groups can only access Site Manager if they are on the same domain as the group. This differs from the automatic domain providers which support cross domain authorization.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



All providers are listed within the provider manager dialog. Providers can be configured or removed by clicking the respective buttons in the table. New providers can be created by clicking the **Add** button, which opens the a dialog to configure a new Domain provider.



A Domain provider can be configured with the following fields:

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Field	Notes
Name	A friendly name which is displayed to users. If no name is provider then the provider will be named after the domain it is associated with.
Domain Controller	The host name of a domain controller. This can be in the form of a DNS-style name, a NetBIOS address or an IP address. **Custom ports** Site Manager will communicate with the domain controller using LDAP. To use custom ports (other than the default of 389 or 636) specify the domain controller in the **hostname: port** format.
Username	The username of an account on the domain. The credentials of this account will be used to perform any lookups against the LDAP server.
Password	The password of the account specified by the username entered in the previous field.
Display Order Priority	The order the provider will appear in dropdown lists like on the login page and the permissions modal. There is also an option to hide the provider from lists other than the table in the provider manager which may be useful if there are unused automatically generated providers.

After clicking "Save", Site Manager will check the validity of the configuration. If a provider can be created then the configuration is saved and a provider is added to the list of providers in the previous window. Otherwise, the an error message will appear explaining the problem.

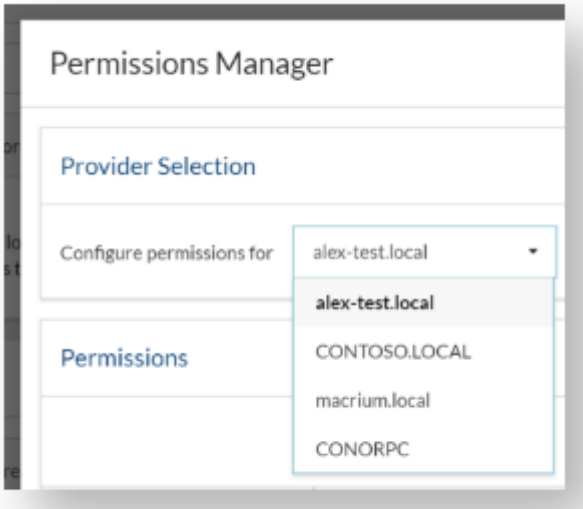
Configuring Permissions

Default permissions

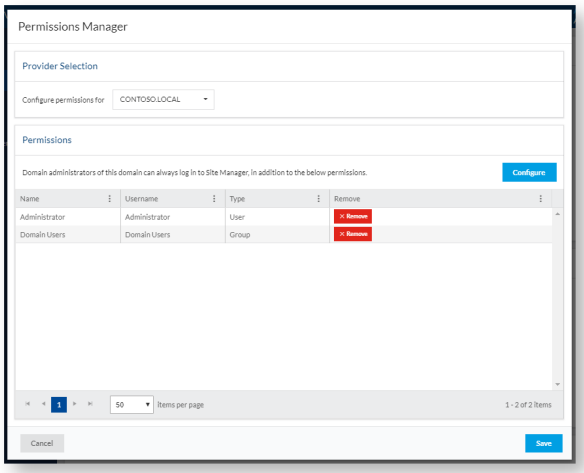
Admins of the domain the Site Manager server is connected to and local administrator accounts are granted Site Manager access by default. Permissions for domain admins can be disabled by setting the registry value "Disable Default Admin Access" in the key "HKEY_LOCAL_MACHINE\SOFTWARE\Macrium\Site Manager" to 1. Local administrators will always have permission to access Site Manager.

Next to the **Manage Provider** button on the security settings page is the **Manage Permissions** button. Clicking this button will open the permissions management window.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

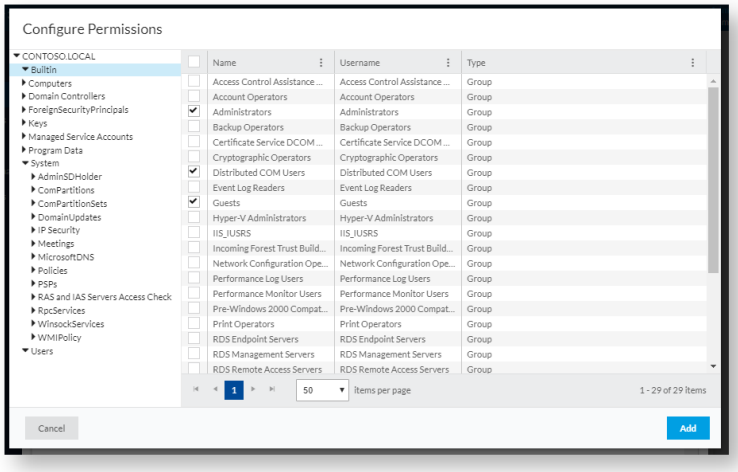


Permissions are configured separately for each provider. Select the correct provider from the dropdown before configuring permissions.



A table listing the active permissions is below the provider selection field. Here the names of authorized users and groups are displayed. All members of an authorized group are given the permissions of that group (membership is applied transitively). Permissions can be deleted by clicking the **Remove** button. Click **Configure** to add permissions. Changes to permissions can be discarded by clicking cancel.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



The structure of the directory is navigable through the tree on the left, which shows the folders and Organizational Units which have been configured on the domain. On the right is a table listing the users and groups in the selected folder. Rows can be selected to add corresponding permissions when the **Add** button is pressed.

Macrium Image Guardian

- Introduction
- Installation
- Upgrades
- Configuration
  - Protecting Site Manager Repositories
- Advanced Usage Scenarios
  - Protecting a Repository hosted on a NAS or other external system

---

Introduction

Site Manager 8 includes Macrium Image Guardian, which provides ransomware protection for backup files that are stored on the Site Manager server.

Macrium Image Guardian works by preventing unauthorized delete or write operations being performed on backup image files by any process that does not have a valid Macrium code signature.

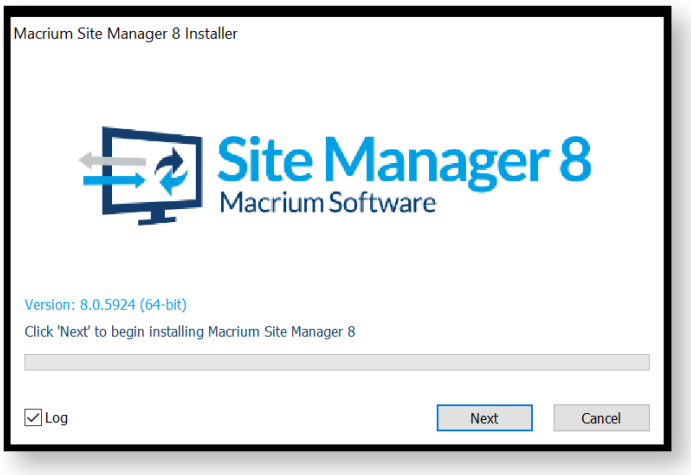
Image Guardian has been used by Macrium Reflect to provide malware protection since version 7.1.

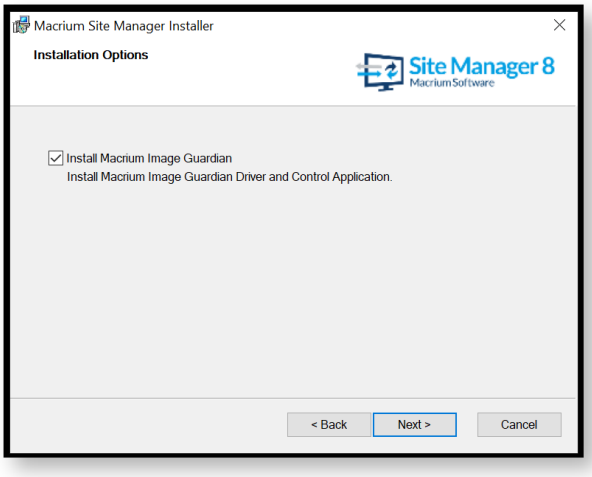
Learn more about Macrium Image Guardian in Macrium Reflect here

Installation

When you install Site Manager for the first time, the installation wizard will show you an option to install Image Guardian:

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.





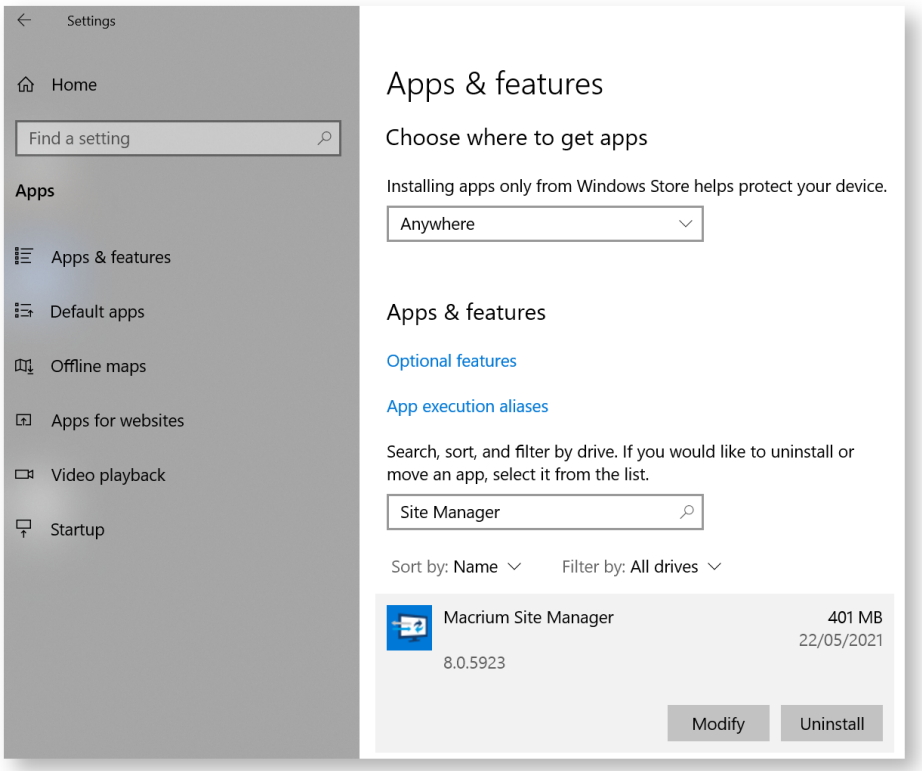
Once it has been installed, the computer may need to be rebooted before the Image Guardian driver is loaded and Image Guardian can provide protection.

Upgrades

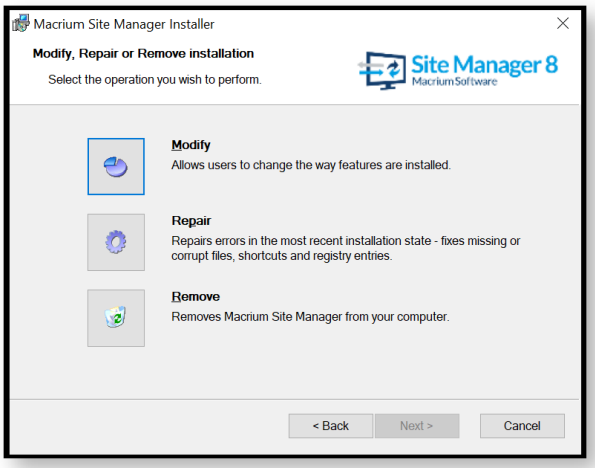
When upgrading in the Site Manager user interface, the Image Guardian status will be preserved. If it was *previously* installed, it will be installed and upgraded with the Site Manager server. If it wasn't, however, it *will not* be installed.

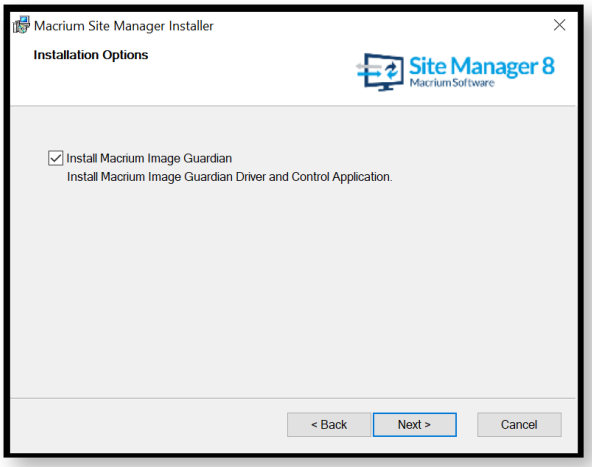
To change whether Image Guardian is installed after Site Manager installation, use the **Modify** option on the **Programs** (or **Apps and Features** in Windows 10) control panel

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.





As with first time installation, you might need to reboot your computer before the Image Guardian driver is properly installed and usable.

Upgrading the Image Guardian Driver

If Image Guardian is installed and an upgrade to the Image Guardian driver is installed, the Site Manager installer will set this update to happen on next reboot and the system will continue using the older driver until reboot. This is done to ensure that Image Guardian protection is not lost on upgrade.

If this happens, the Image Guardian configuration tool will warn that a reboot is pending and refuse to allow reconfiguration of Image Guardian settings until this has been performed

Configuration

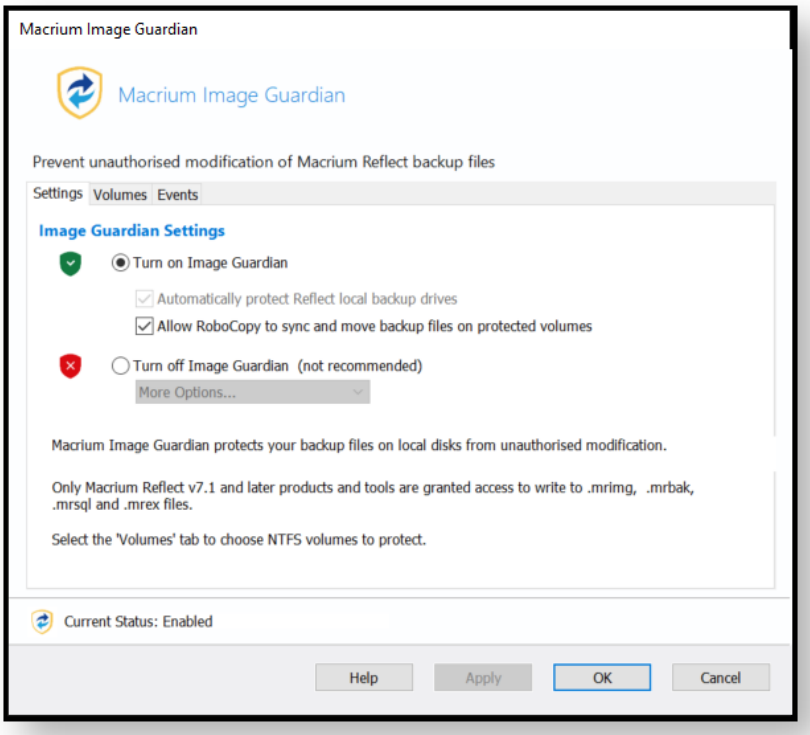
Once Image Guardian has been installed, you can configure it by running the Image Guardian configuration app. A desktop icon and start menu entry will be created by the Site Manager install.

This is located in:

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

```
C:\Program Files\Macrium\Common\MIGPopup.exe
```

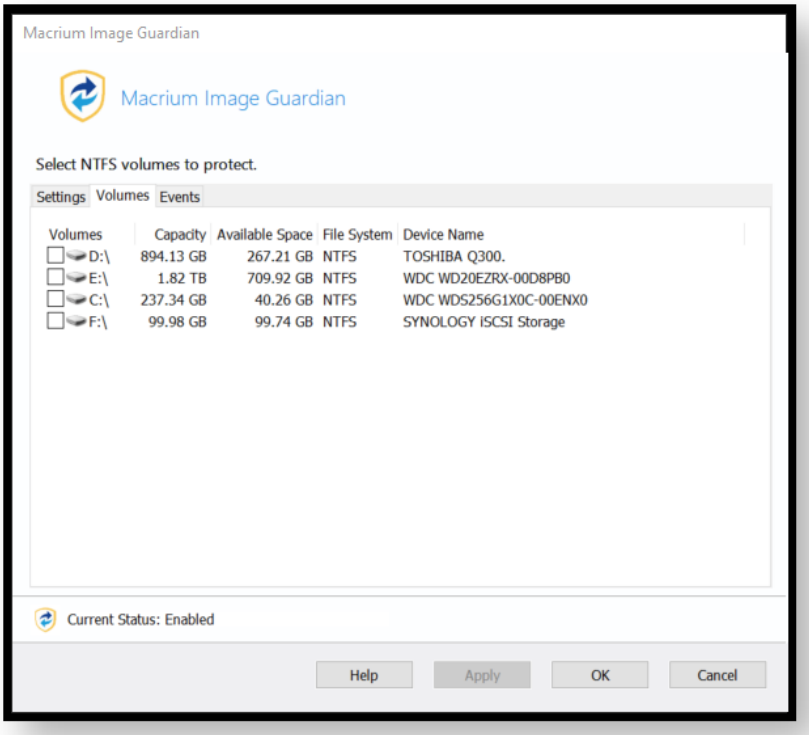
Running this program will display the following interface



This is where you can enable and disable Macrium Image Guardian. You can also disable it temporarily for fixed time periods to allow you to perform server maintenance.

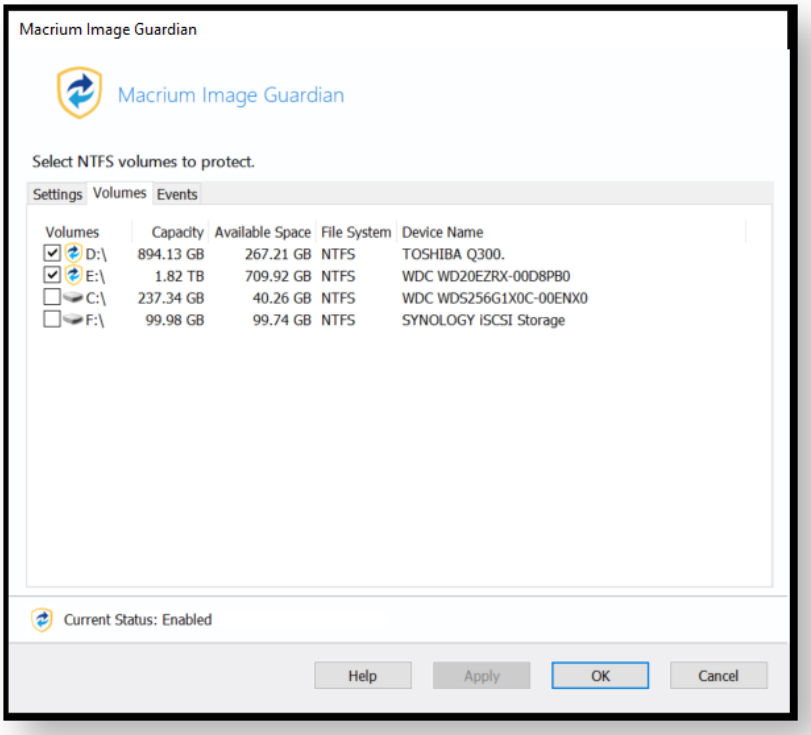
To enable Image Guardian on particular volumes, first Image Guardian must be turned on in the **Settings** tab, and then the volume selected in the **Volumes** tab

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



This tab shows a list of all local disk partitions and their Image Guardian status. Once Image Guardian has been turned on globally in the **Settings** tab, the appropriate volumes selected in the **Volumes** tab, pressing **OK** or **Apply** will save the configuration. After this has been done, the **Volumes** tab will show protected volumes with an Image Guardian icon:

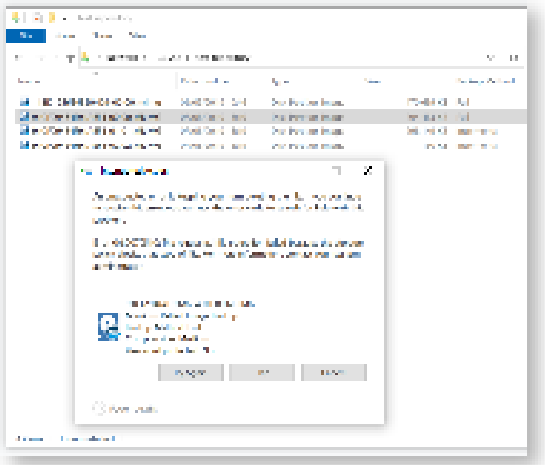
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



Protecting Site Manager Repositories

To protect a Site Manager repository, you should identify the volume with the repository share and enable Image Guardian on this volume. For example, if Site Manager has a repository on **\\sitemanagerserver\repository** which corresponds to **c:\repos\repository**, the **C:** volume should be protected. Once this is done only Macrium Reflect, Site Manager or the Site Manager Agent will be able to modify or delete image files. This means the files cannot be reached and encrypted by ransomware.

Any process which cannot be cryptographically authenticated as a Macrium process will be denied access to delete or write to backup image files:



Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

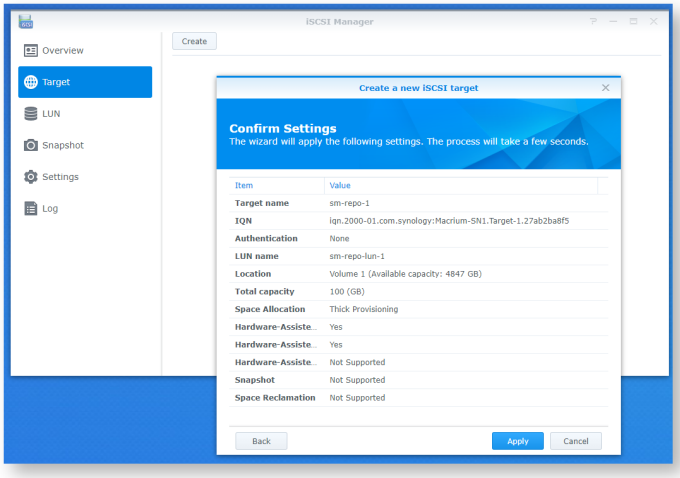
Advanced Usage Scenarios

Protecting a Repository hosted on a NAS or other external system

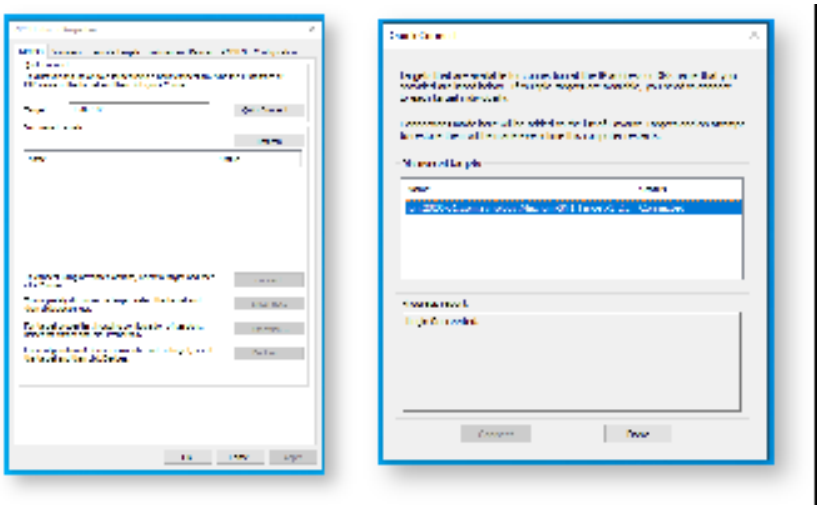
Macrium Image Guardian can be used to protect volumes on any locally attached disk or storage system, but often repository data resides in a NAS, which can't be directly protected by Site Manager.

To provide protection in these cases, the Site Manager server can be used as an intermediary between the NAS and Agents by attaching the NAS disk via **iSCSI**.

Many NAS devices and storage systems allow storage to be exposed via iSCSI, for example on a Synology NAS, iSCSI Manager can be used:

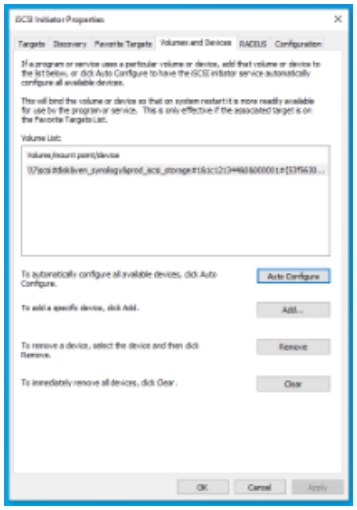


Once the iSCSI target has been created on the NAS, it can be connected to the Site Manager server by using the Windows iSCSI initiator:



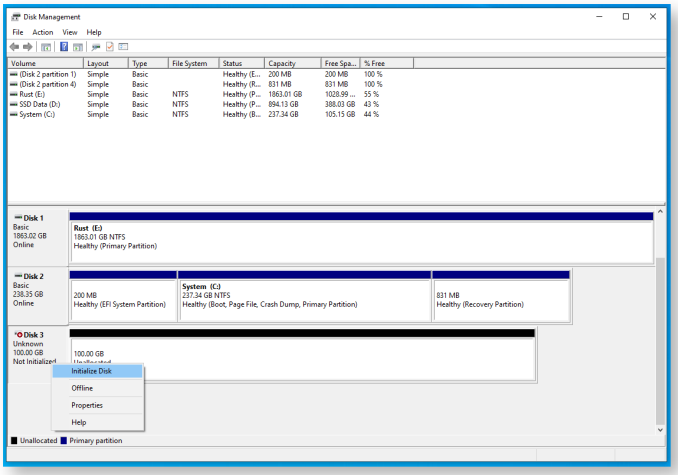
Once the initiator has connected to the iSCSI target, the target LUN can be mounted in the **Volumes and Devices** tab. In the simple case here, using the **Auto-Configure** option is suitable.

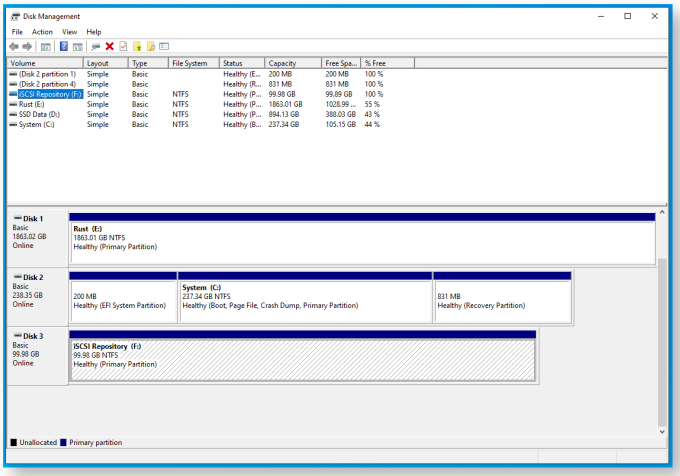
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



We recommend using CHAP or other authentication to the iSCSI backend to ensure that no malware, ransomware or other malicious software can gain access to the iSCSI target directly.

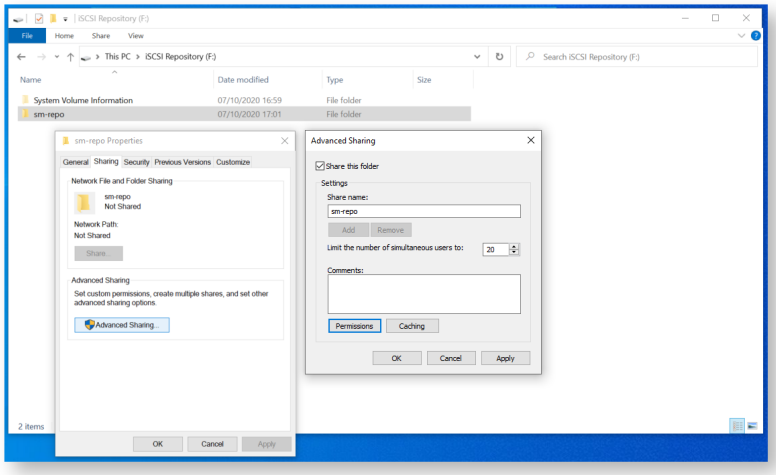
Once the target is connected, it will appear as any other disk in Windows and can be initialized, partitioned, formatted and have a drive letter (or mount point) assigned in the Windows Disk Management tool





Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

With this done, an appropriate folder can be created and shared on the iSCSI target. This share can then be used to create a Site Manager repository.



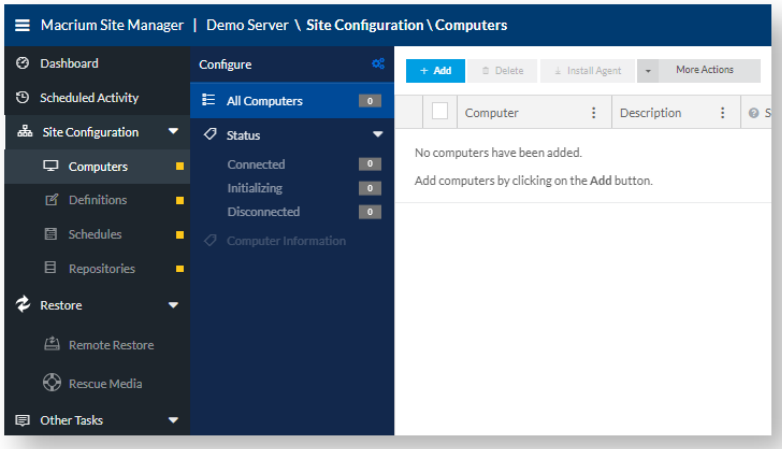
Performance Notes

In this configuration, all backup traffic will be channeled through the Site Manager server instead of going direct from Site Manager Agent to NAS.

If the Site Manager server has poor network connectivity to either the Agent computer or the NAS, backups may be slower than a direct connection.

Scheduling Centrally Managed Backups

Configuring the Site Manager to perform centrally scheduled backups can be done by following the **Site Configuration** section of the menu on the left hand side of the user interface as shown below:



The sections are:

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

1. Computers - This section allows you to add client computers to the Site Manager, remotely install the Site Manager agent and monitor communication status between agents and Site Manager.
2. Definitions - This section is used to create Backup Definitions - a set of template based rules which allow you to quickly define backups for multiple computers simultaneously. A Backup Definition can also be run directly from this page, creating a single point in time backup
3. Schedules - This section is used to create Schedules - a set of rules which determine frequency of backups (daily, monthly etc.), which type of backup is created (full, differential, incremental) and what backup retention rules apply.
4. Repositories - Repositories are storage locations for backups

Once these sections have been configured, backups can be run by using the Scheduled Activity page.

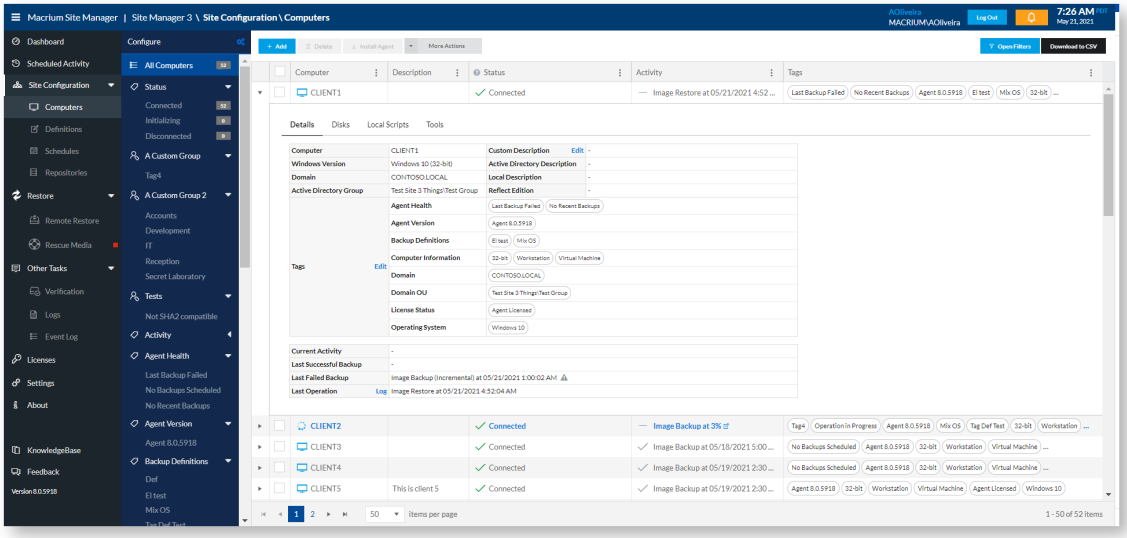
Setup - Computers

- Viewing and Managing Computers
  - Toolbar Buttons
  - Groups and Tags Side Menu
  - Computer Statuses
  - Computer Details
    - Details
    - Disks
    - Local Scripts
    - Tools
- Adding New Computers to Site Manager
  - Domain Computers
  - Network Computers
  - Add Computers Trying to Connect to Site Manager
  - Adding Computers Manaully
- Installing the Site Manager Agent
  - Installing the Agent via Remote Install
    - Steps to Remote Install
    - Problems with Remote Installation
  - Installing the Agent Manually
  - Adding Computers With Agents Preinstalled
- Deleting Clients from Site Manager

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

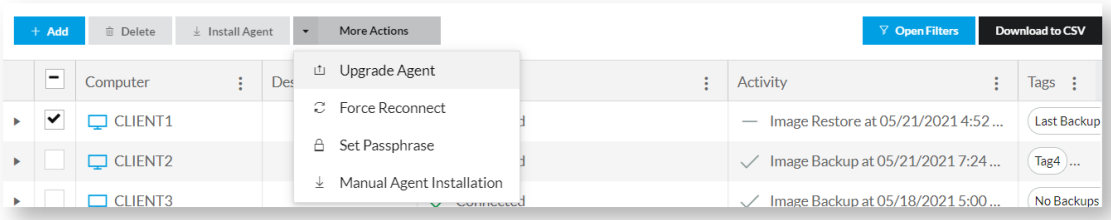
Viewing and Managing Computers

Remote computers are viewed and managed from the **Computers** page of Site Manager, under the **Site Configuration** heading on the left hand side column. This page displays a list of all managed computers:



The dark blue side menu may be helpful to filter the computers by Groups and Tags.

Toolbar Buttons

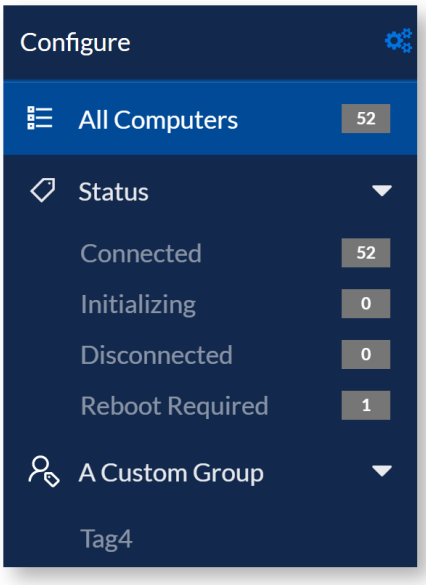


- **Add** - Adds new computers to Site Manager. See the section later on this page for details.
- **Delete** - Deletes selected computers from Site Manager.
- **Install Agent** - Uses remote MSI tools to install or reinstall the remote agent on computers.
- **Upgrade Agent**- If automatic upgrade of Agents is turned off in settings, this button can be used to initiate Agent upgrades.
- **Force Reconnect**- Disconnects and reconnects the computer and updates computer data from the selected computers.
- **Set Passphrase** - Allows the passphrase for the selected agent to be updated to the one used installing the Agent.
- **Manual Agent Installation**- Exports the computers table data as CSV. This can be imported into other tools.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

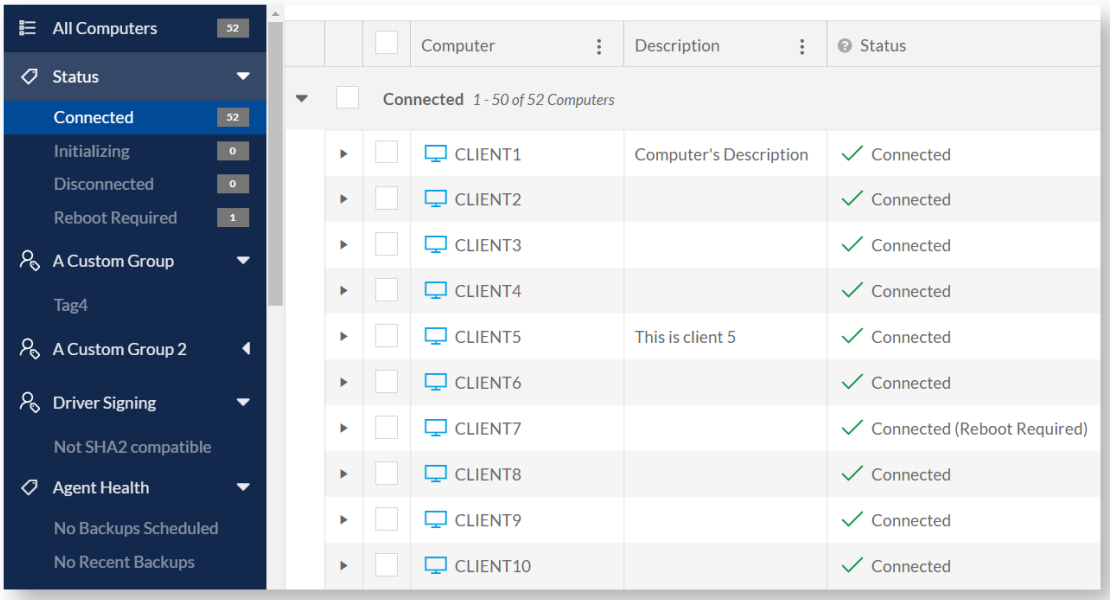
- **Open Filters** - Opens the filters of the table.
- **Download to CSV -** Downloads the content of the computers table to CSV.

Groups and Tags Side Menu



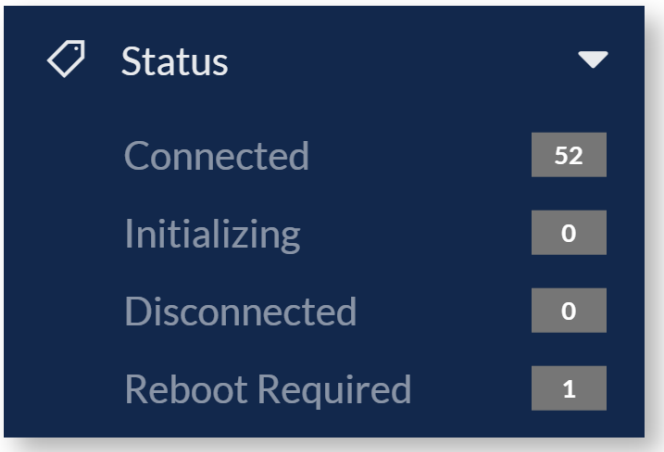
- **Configure** - Configure Groups and Tags and their visibility. More information about Groups and Tags can be found here.
- **All Computers** - Shows all the computers.
- **Status** and **A Custom Group:** Groups to filter the computers by.

Clicking on a group or a tag filters the computers.



Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

The group can be collapsed or expanded by clicking on the icon



To know how to hide groups from the side menu and from the tags column, click here.

Computer Statuses

The following table contains all the possible statuses for a computer:

Agent State	Description	Additional Information
Connected **Connected (Reboot Required)** **Connected (Upgrade Required)**	The computer is online and running a remote agent.	If the status is **Connected (Reboot Required),** the computer is online, as in the **Connected** status, but there is a reboot pending due to an agent upgrade. The Agent will continue to function normally but will not use the CBT driver until it's rebooted. **Connected (Upgrade Required)** Agents are running out of date Agent software. These Agents will either upgrade automatically or require the **Upgrade Agent** function to be used depending on the Site Manager settings.
Initializing	The Agent is negotiating their connection with the Site Manager Server.	Initializing Agents cannot be interacted with until they enter the **Connected** state.
Installing Agent		These Agents cannot be interacted with until the install or update operation is completed.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Agent State	Description	Additional Information
Upgrading Agent	The Agent is in the process of installing or upgrading Agent software	
Unlicensed	The computer does not have an appropriate standalone or Macrium Agent License.	A new license can be added by going to the Licenses page. Alternatively, if a copy of Macrium Reflect is installed on an **Unlicensed** computer and the computer status refreshed, it will change state to **Connected**.
Unauthorized	Mismatch between the passphrase on the Agent and Server	**Set Passphrase** in the toolbar allows the passphrase for the selected agents to be updated to the one used installing the Agent. If the passphrase set on the server and the agent match, the computer will re-initialize and enter the **Connected** state.
Disconnected	The Site Manager agent is not connecting to the server	Agents in this state may not have an Agent installed or may be experiencing communications issues. To resolve this, the Agent can be installed by the **Install Agent** function or manually on the Agent computer. If the agent is already installed on the computer, see the Troubleshooting Agent Communications page for more details.

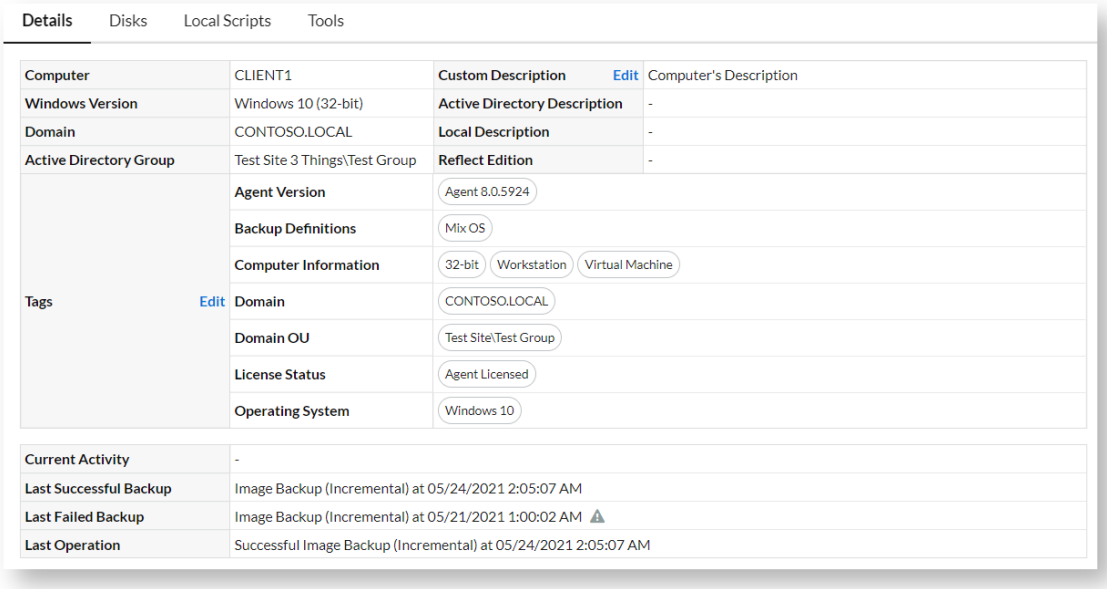
Computer Details

Each managed computer row can be expanded to show detailed information on the computer. To open or close the computer detail information, click the ▶ marker on the left hand side of the computer row. The information is divided into tabs, as follows:

Details

Shows the basic details of a computer as well as the last activity data.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

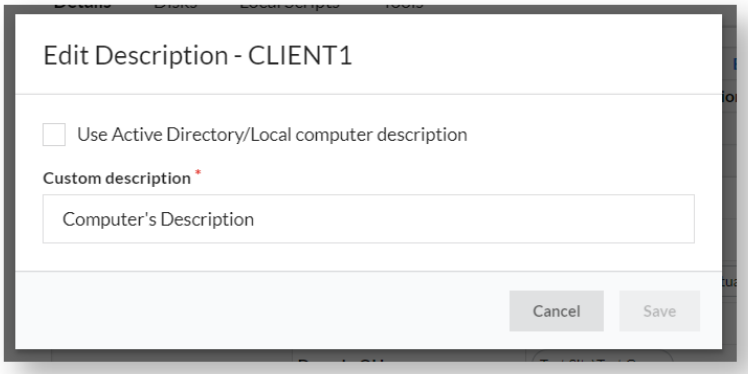


Description and *Tags* can be edited by clicking on **Edit**.

Custom Description

Identify a computer by its description. It can be edited by clicking on *Edit.*

It can show the Active Directory/Local computer description or a custom description can be provided.

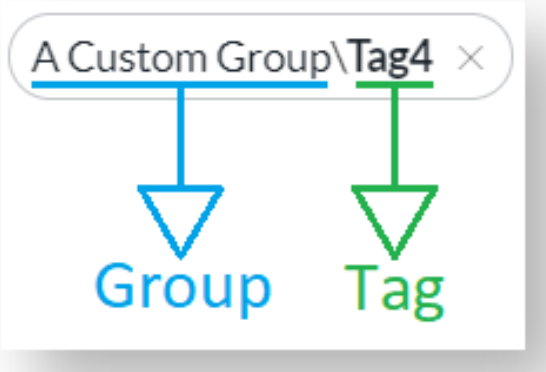


Tags

Tags are useful to group some of the computers in meaningful ways. To know more about tags, click here.

This is what a Group and Tag look like:

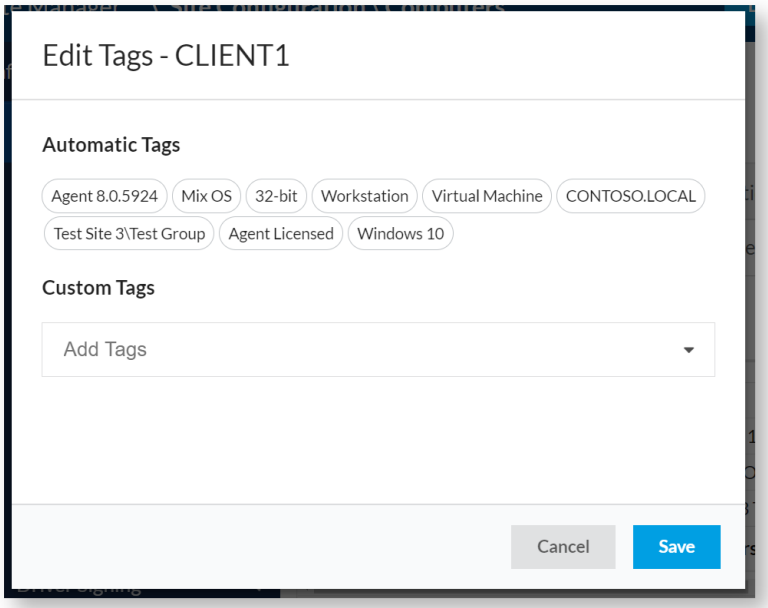
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



The Group and the tag are separated by the **** character. Everything before the \ is the group and everything after is a tag.

If the separator character is not present it means it's only showing the tag name.

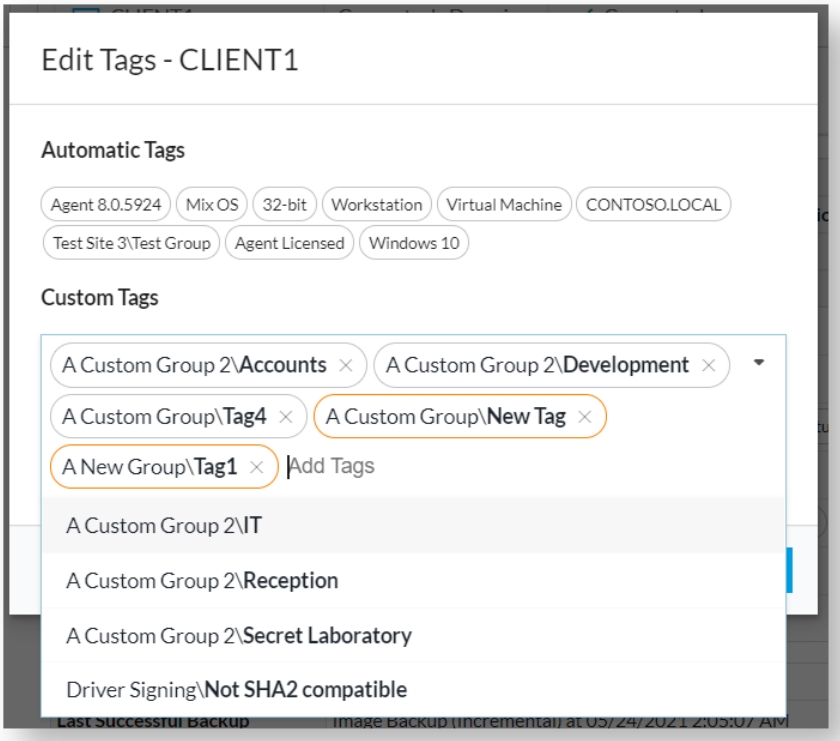
Automatic tags are calculated automatically and cannot be edited directly.



Assigning a Tag

Tags can be assigned to a computer from this view.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



Existing tags can be assigned to a computer by selecting them on the dropdown menu.

Groups or tags can be searched for by start typing on the input.

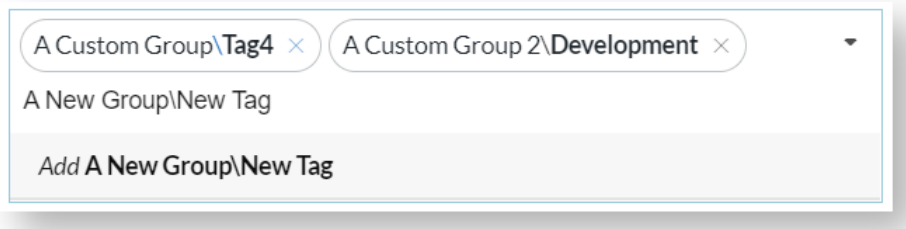
Shortcut

If you don't want to type the full group name when searching for a group or a tag, press **Tab** and it will automatically fill the rest of the group name for you.

The same is valid for the tag name.

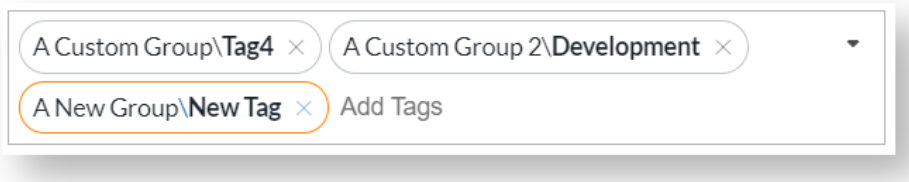
Creating New Groups or Tags

New groups and tags can also be created and assigned to a computer in one go. That can be done by typing a new group or tag and press *Enter* or clicking on the *Add* option.



After adding the new group or tag, it will show as orange - meaning it is a new group or tag.

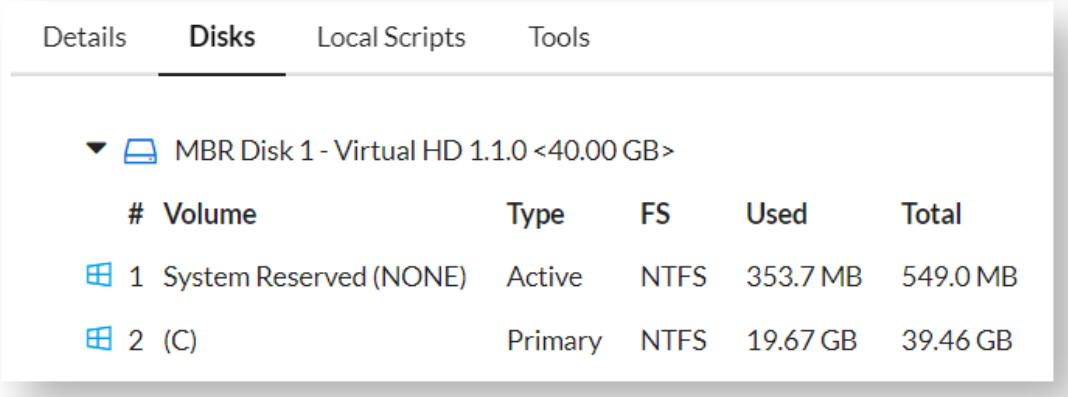
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



In the example above, a new group called *A New Group* will be created and a new tag called *New Tag* will be added to that group.

Disks

The disks and partitions on the computer are shown here, to help in determining how and what to backup from this computer.

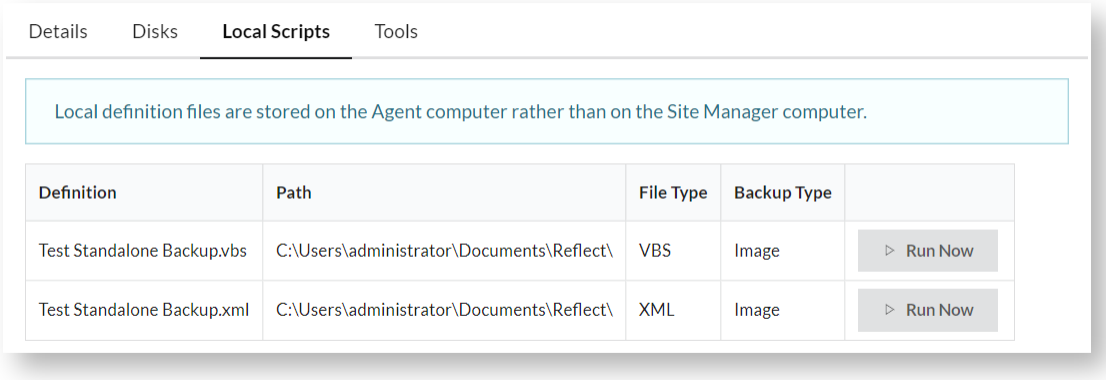


Local Scripts

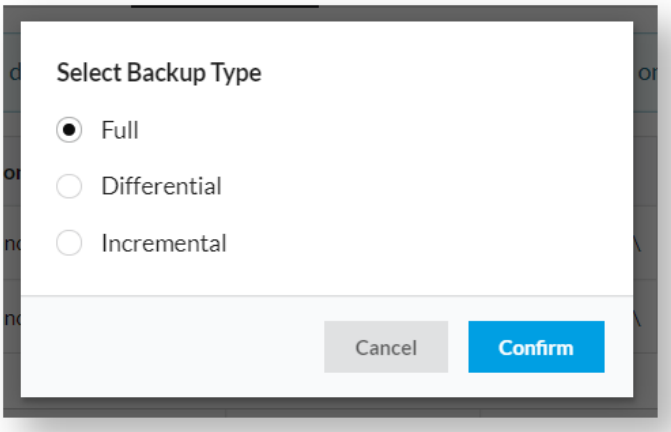
The legacy tab contains information from agents about standalone Macrium Reflect installations. This tab is included to help with the transition of backup scheduling from being locally scheduled on each computer to being centrally scheduled on the Site Manager.

A list of .xml backup definitions and script files stored locally on the computer are listed here and may be run manually from Site Manager with the '**Run Now**' option.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

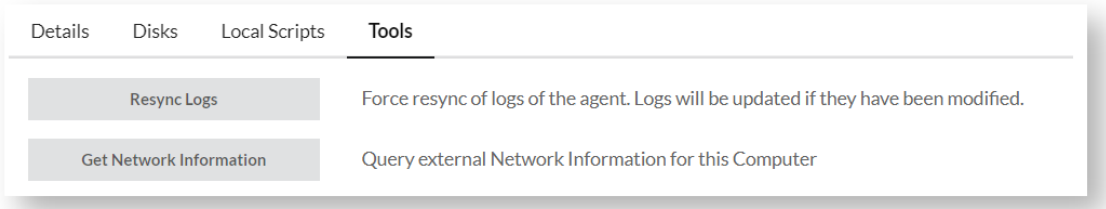


After pressing 'Run Now' a dialog will pop up to select the type of backup (Usually Full, Differential or Incremental but may have other options for different backup types) and confirm the backup:



Tools

Some extra features that are less used can be found in this view: *Resync Logs* and *Get Network Information*.



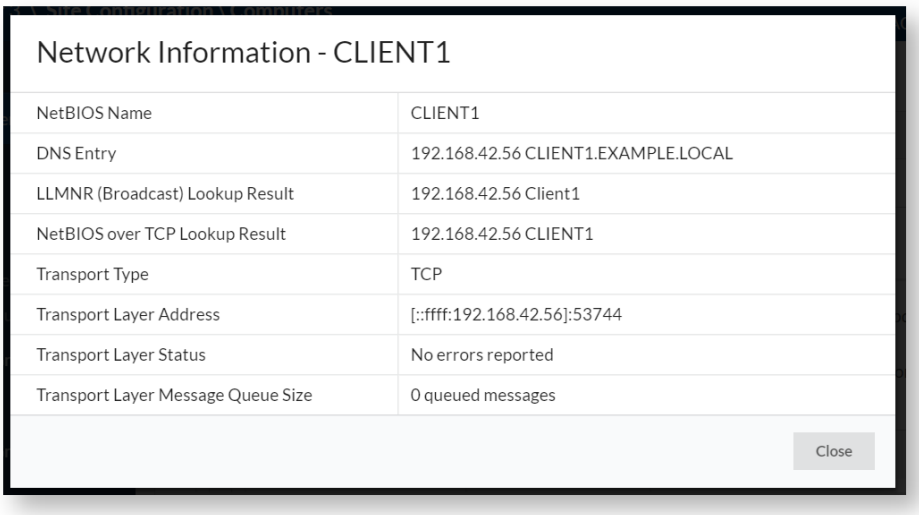
Resync Logs

A confirmation modal will be shown before starting the resync.

The selected Agents will be disconnected and on reconnect will resync all backup logs.

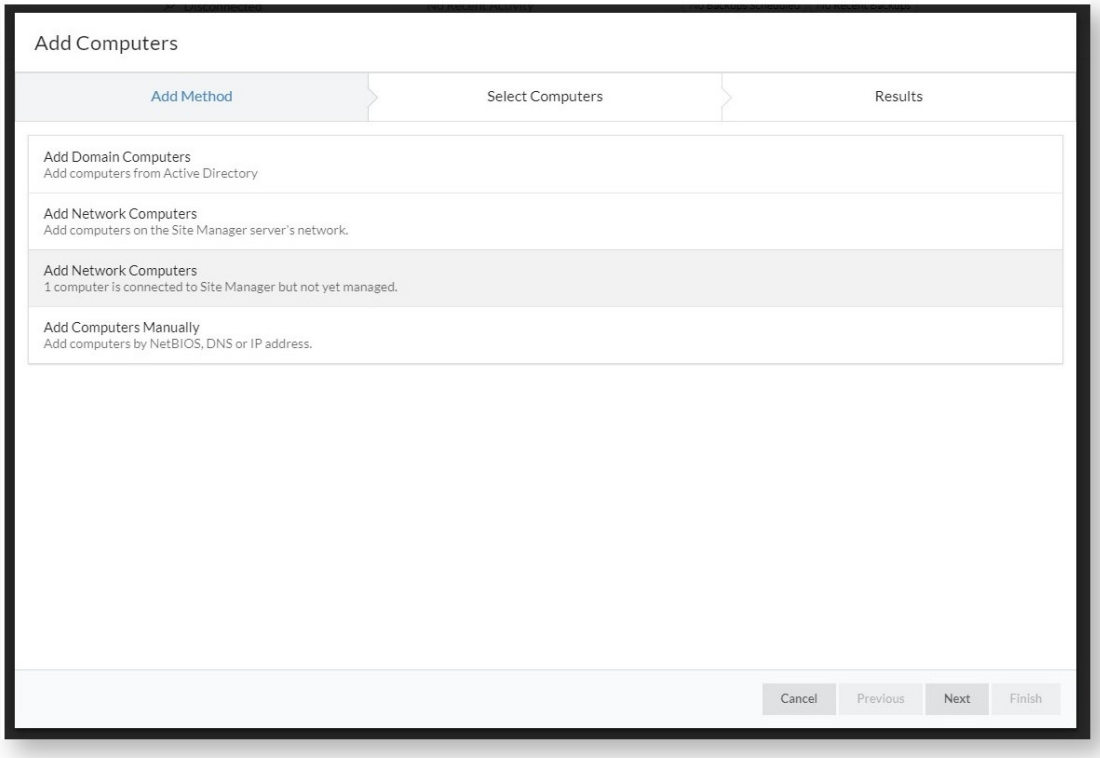
Get Network Information

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



Adding New Computers to Site Manager

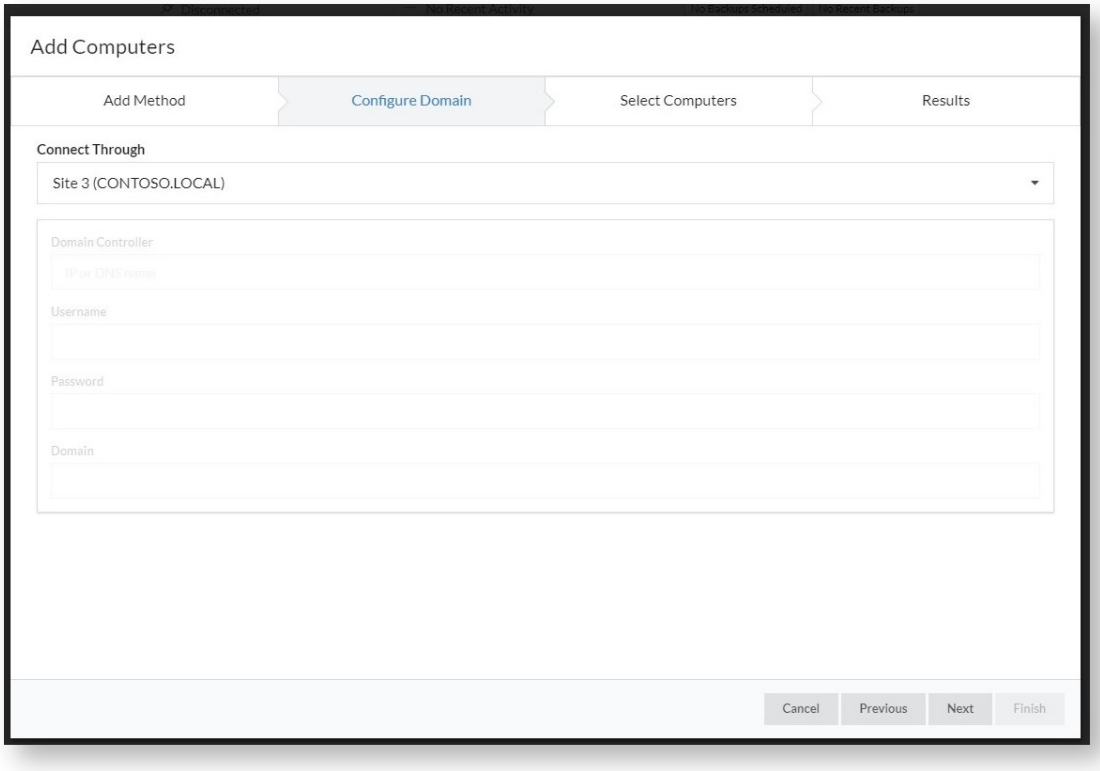
Computers are added to Site Manager using the Add Computers Wizard which can be accessed from the computers page.



Site Manager uses NetBIOS names to uniquely identify computers (though connections are over TCP/IP). This means that a NetBIOS name must be provided before a computer can be added to Site Manager. However, Site Manager provides multiple ways to lookup a computer's NetBIOS name for user convenience.

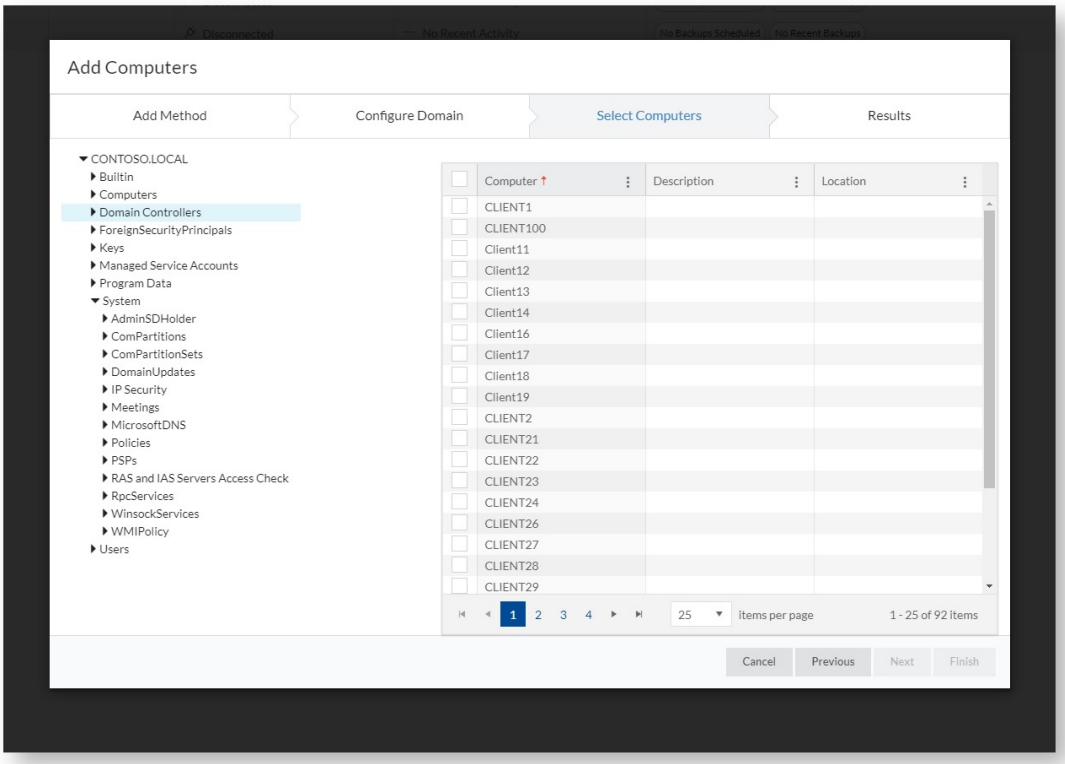
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Domain Computers

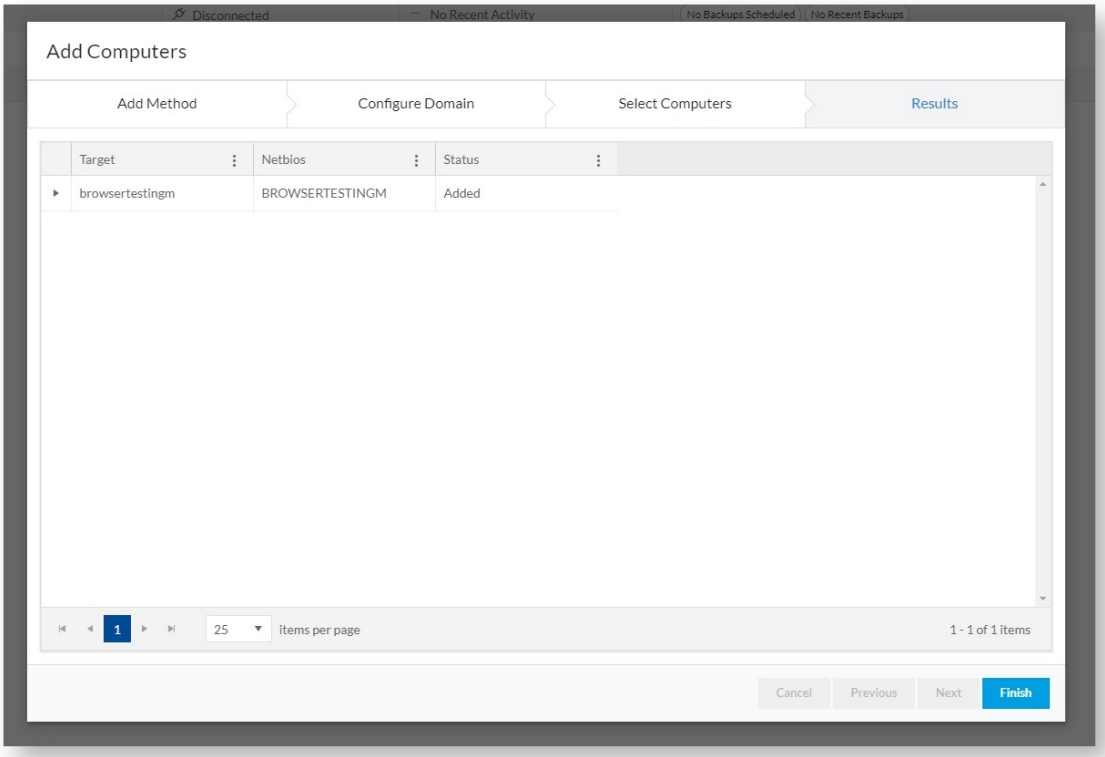


Site Manager can search Active Directory to find domain computers. To set up a connection with Active Directory, users can choose a domain login provider or enter the connection details manually. For a manual connection, enter the name of the domain controller and the credentials of a user authorised to perform searches (the domain field is used in domain forests where the domain of user differs from the target domain). The connection will be verified before the next step of the wizard.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



The tree on the left can be used to navigate the domain and computers contained within the selected organisational unit are displayed in the table. Selected computers will be added to Site Manager.



Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

The final page displays the computers which have been added to Site Manager.

Network Computers

Site Manager can search for computers on the network it is connected to. Users can select computers from the search results to be added to Site Manager.

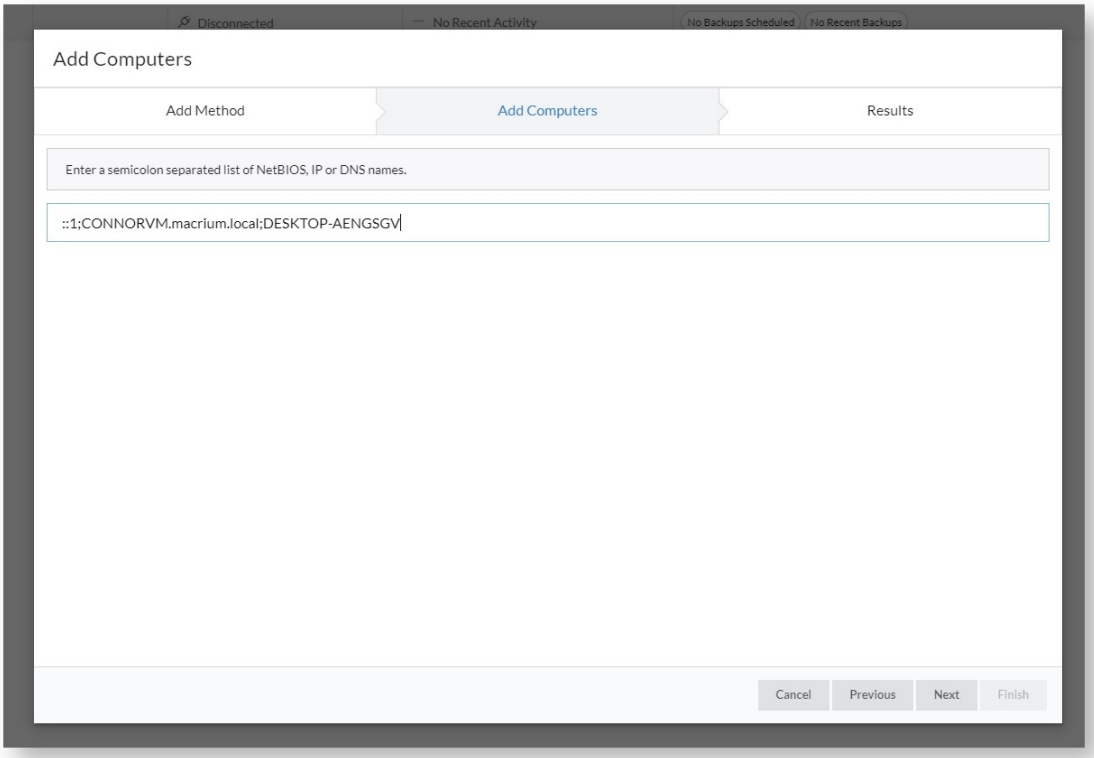
Add Computers Trying to Connect to Site Manager

Agents which have been configured to communicate with a given Site Manager server will have already setup a communication channel. The computer still needs to be added for Site Manager to manage it.

This option will list all computers which has an agent configured to seek the Site Manager server. Users can select computers to be added from the table.

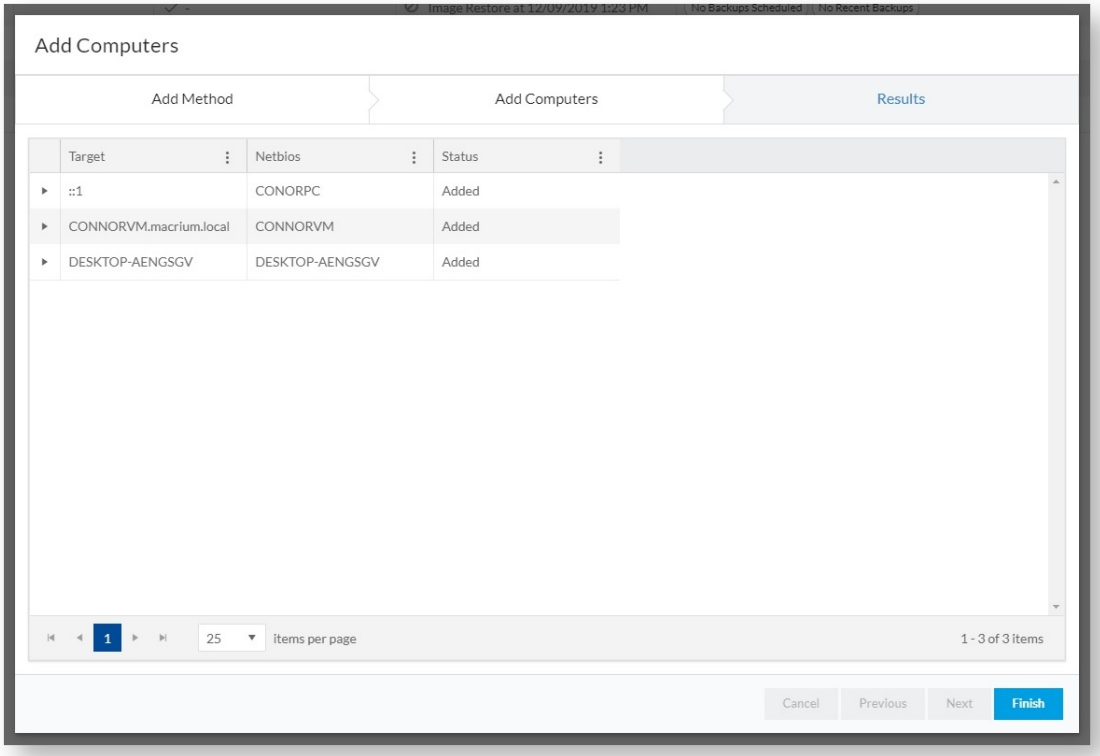
If there are no computers seeking a connection with Site Manager then this option is disabled.

Adding Computers Manaully



Computer can be added manually if the user knows the NetBIOS or DNS name or the IP address (IPv4 or IPv6) of the target computer. DNS names and IP addresses will be resolved to a NetBIOS name by Site Manager. Multiple computers can be added if they are separated by semicolons (;); whitespace is ignored.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



The table reports the success of name resolution; agents with resolved NetBIOS names are added to Site Manager. Unsuccessful IP lookups will also be reported. Note that NetBIOS and DNS names are not checked to allow offline computers to be added.

Installing the Site Manager Agent

Adding a computer to Site Manager will add the computer in the **Disconnected** state unless the computer has had the Site Manager Agent installed and configured to connect to this Site Manager Server.

This can be done remotely via the Site Manager user interface or manually by installing the Site Manager Agent MSI installer.

Installing the Agent via Remote Install

If Site Manager is on a domain or the appropriate steps have been follow, the Agent software can be remotely installed on the client to be managed. See Troubleshooting Agent Communications for a detailed guide to network and firewall requirements for this process.

Steps to Remote Install

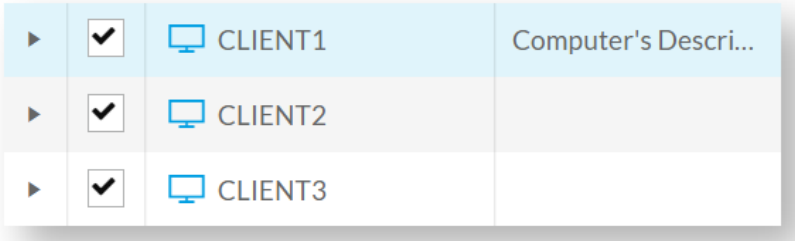
Installation Credentials

Administrator level access to the computer is required to install an Agent. If available, the credentials used to log in to Site Manager will be used. If Site Manager is configured to allow anonymous access, the installation process will prompt for credentials before attempting install.

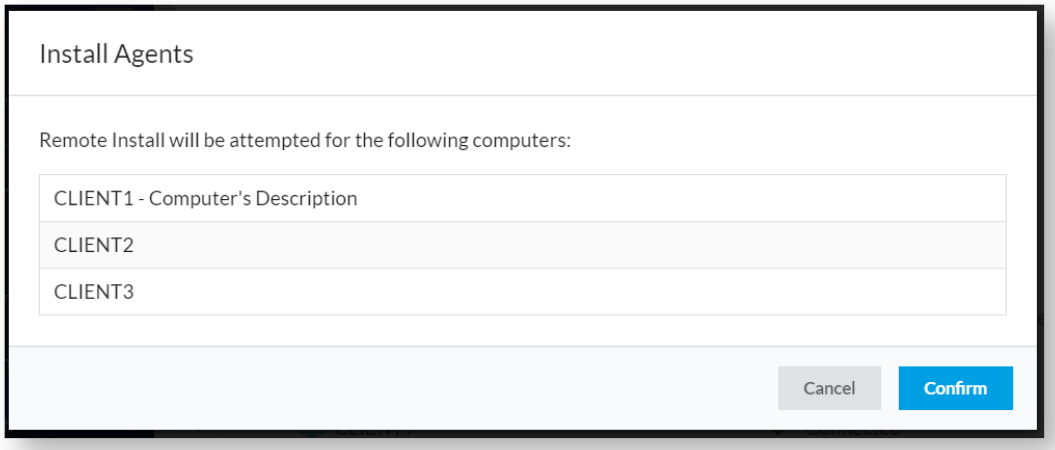
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Additional credentials may be configured in the **Settings** page.

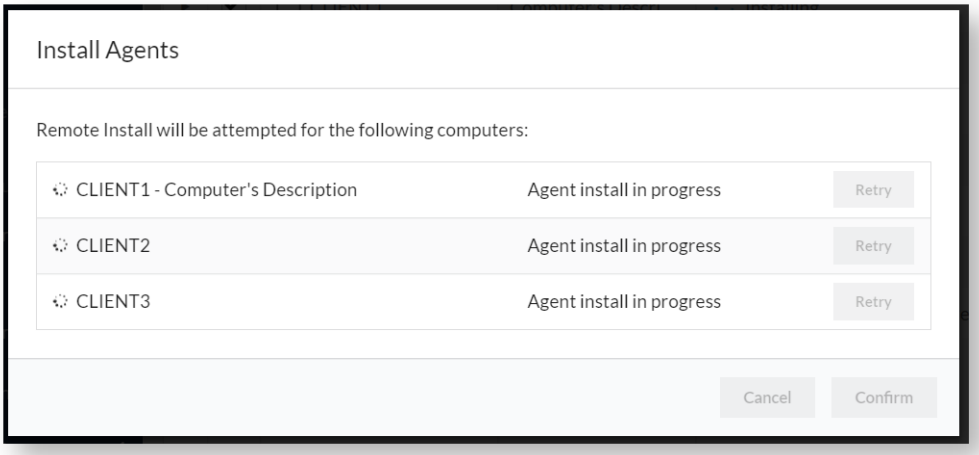
- Select the computers to perform a remote install on.



- Press the **Install Agent** button in the toolbar.
- Select 'Confirm' in the dialog that pops up to attempt to install or cancel to exit.

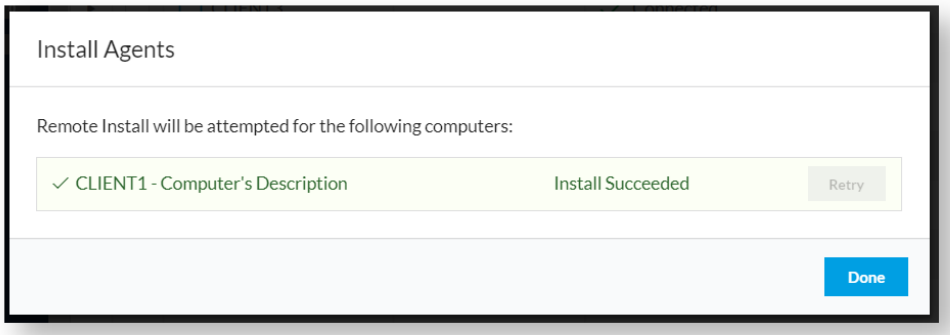


- Site Manager will attempt the install and show the status of each computer.



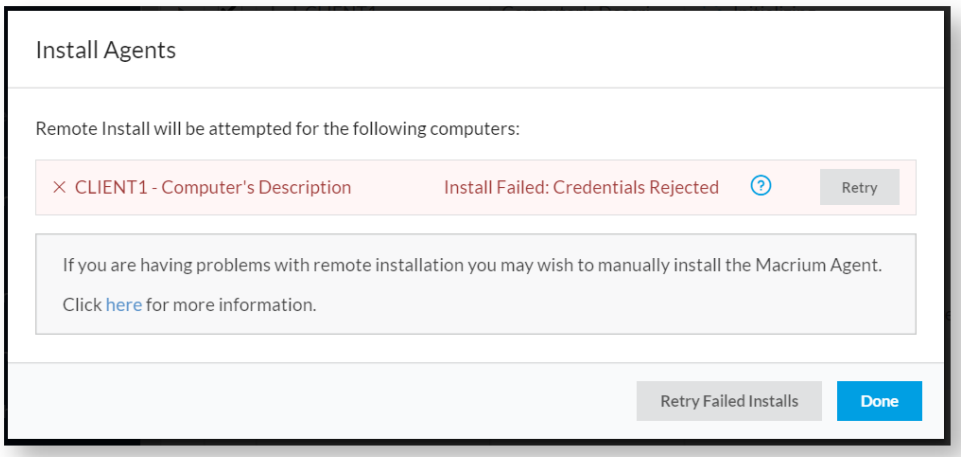
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

- Once each install has finished, the status will be displayed. If all computers succeeded then only 'Done' will be available



Problems with Remote Installation

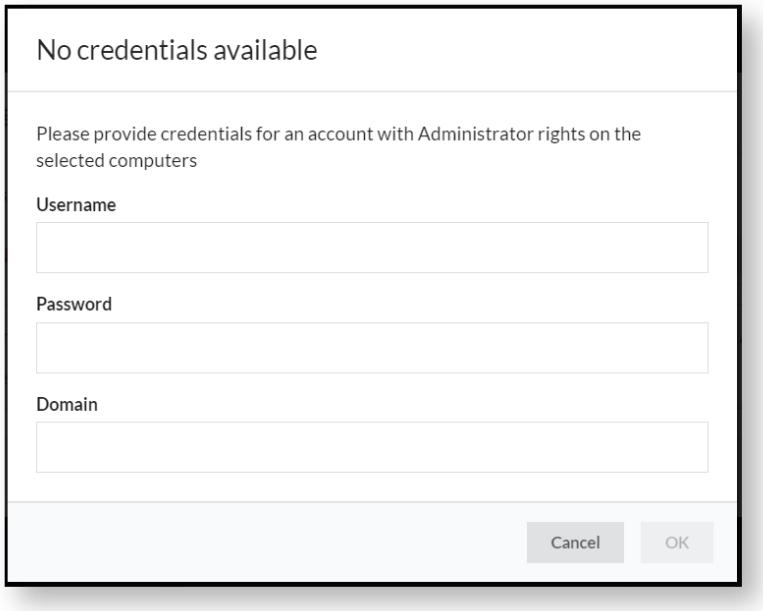
If there are any issues in installing the agent on any computer, this will be shown in the results:



All failed installs can be retried simultaneously via the **Retry Failed Installs** button or on an individual computer basis by using the **Retry** buttons in the table next to the install status. Each failed computer has a help icon that can be clicked to provide detailed information about the failure.

If retrying the installation on a computer (or computers) which failed the install due to credential errors, Site Manager will prompt for new credentials:

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



Once new credentials have been entered and **OK** pressed, reinstallation will be attempted using the new credentials.

Other possible errors are:

Install Error	Description	Recommended Action
No Credentials Available	The installation cannot proceed because there are no cached credentials to try. This only occurs when attempting the install when the Management Console is set to allow anonymous login and the password prompt is cancelled on attempting the install	Retry the install and enter credentials when prompted
Credentials Rejected	None of the entered or cached credentials were accepted by the computer as valid. This may occur if the computer is not part of a domain and the computer is configured to only allow unelevated access remotely.	Retry the install with different credentials or attempt a manual installation.
Remote Install Not Available	The install process connected to the WMI server successfully, but the WMI installer component is not installed. This typically occurs on Windows XP machines as later editions have this component installed automatically.	Install the Remote Installer WMI component on the remote machine and try again.
WMI Not Available	Could not find a WMI process to connect to. Either the computer is offline, not a Windows machine or WMI remote access is blocked for security reasons	

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Install Error	Description	Recommended Action
		Check the computer status and try again or manually install the agent.
Operating System too old	The computer connected but is below the Windows version required for the Agent.	Upgrade the OS on the computer or use a different computer.
Installer Error - 1234	The installer ran, but returned an error code and was not successful. The number in place of *1234* is the code from the installer	Contact Macrium support or try a manual install.
Install Failed	A general failure in installation.	Retry the install or contact Macrium support.
Computer not present on network	The computer name could not be resolved to an IP address by either DNS lookup or LLMNR broadcast.	Check that the computer is present on the network and that DNS is correctly configured
File sharing unavailable	The computer IP address could be lookup up, but an attempt to connect to the Windows administrative share failed (\\computername\admin$)	Check that the computer is present on the network and that Windows share traffic is not blocked

Installing the Agent Manually

If Remote Install is not available, the Agent can be installed manually. See Agent Manual Install for more details.

Adding Computers With Agents Preinstalled

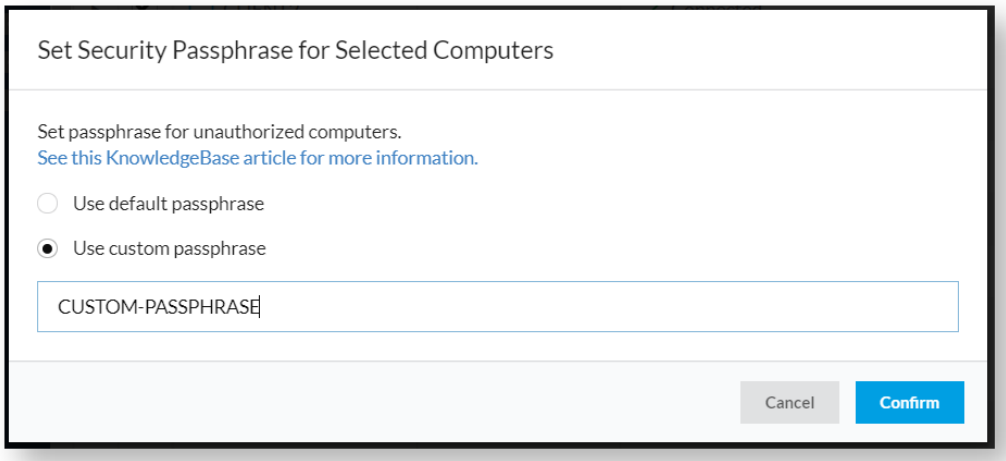
When a Site Manager Agent is installed, it is configured with the information required to access the Site Manager server. This is provided automatically when the Agent is installed via the Site Manager **Install Agent** function or manually if the Agent has been installed via MSI installer file. If the Agent is properly configured, it will enter the **Connected** state automatically when added to Site Manager. If the Agent has been configured with the incorrect details (or details for another Site Manager server), the agent must be reconfigured by either reinstalling the Agent via the **Install Agent** function or running the Agent Configuration Tool on the Agent itself.

If the Site Manager has been configured with a different security passphrase than the one configured in the Security Settings page of the Site Manager server, it will enter the **Unauthorized** state.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

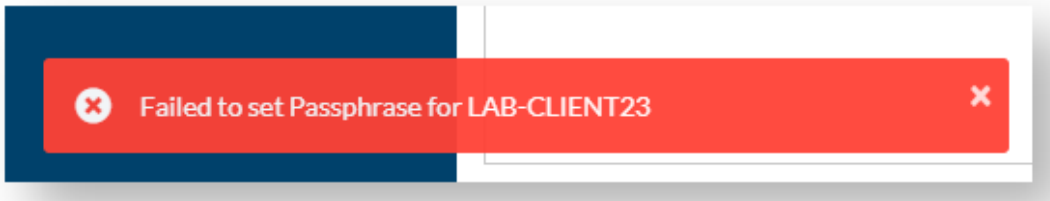
To fix this and manage the agent, you can set the correct passphrase on the Agent using the Agent Configuration Tool, reinstall the Agent (remotely or manually) which will reset the passphrase, or supply the old passphrase in Site Manager. When this is done, Site Manager will connect to the agent using the old passphrase and update the passphrase to the appropriate one for the current installation.

To set the passphrase, select the computers by checking the appropriate box in the computers list and press the **Set Passphrase** button in the "More Actions" dropdown. This will open the passphrase editing dialog:



To set a passphrase, check the **Use custom passphrase** option and enter the passphrase in the box. Press CONFIRM to apply the passphrase.

If the passphrase is correct, the computer will connect. If it is incorrect an error will be shown:

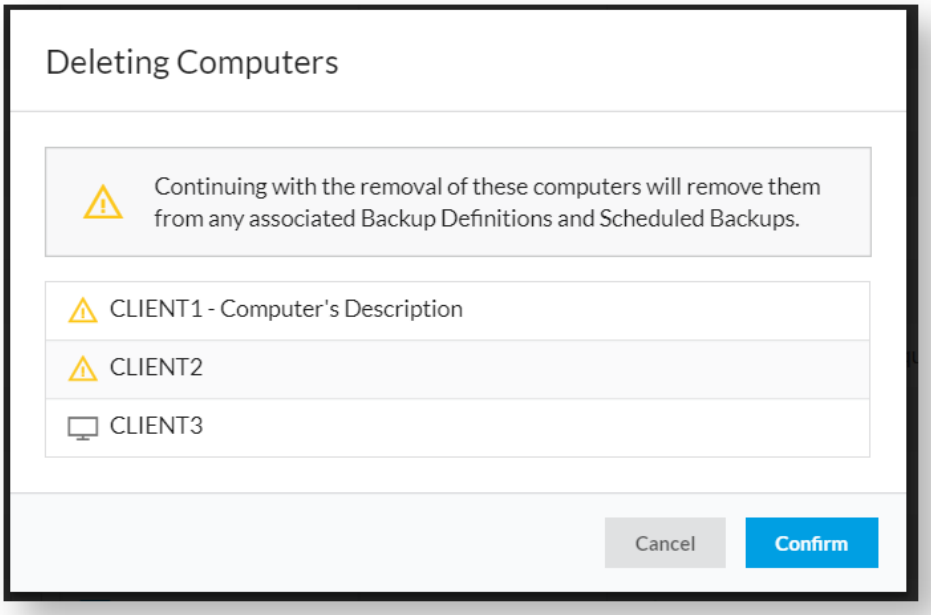


Deleting Clients from Site Manager

To delete computers from Site Manager, select the computers to delete via the checkboxes and press the **Delete** button in the toolbar:

This will bring up a confirmation dialog box, including information of any computers which are part of currently scheduled backups or Backup Definitions:

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

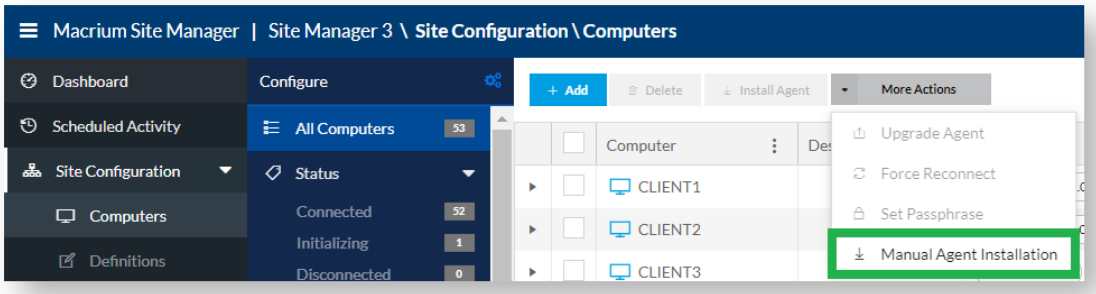


To remove these computers, press **Confirm**.

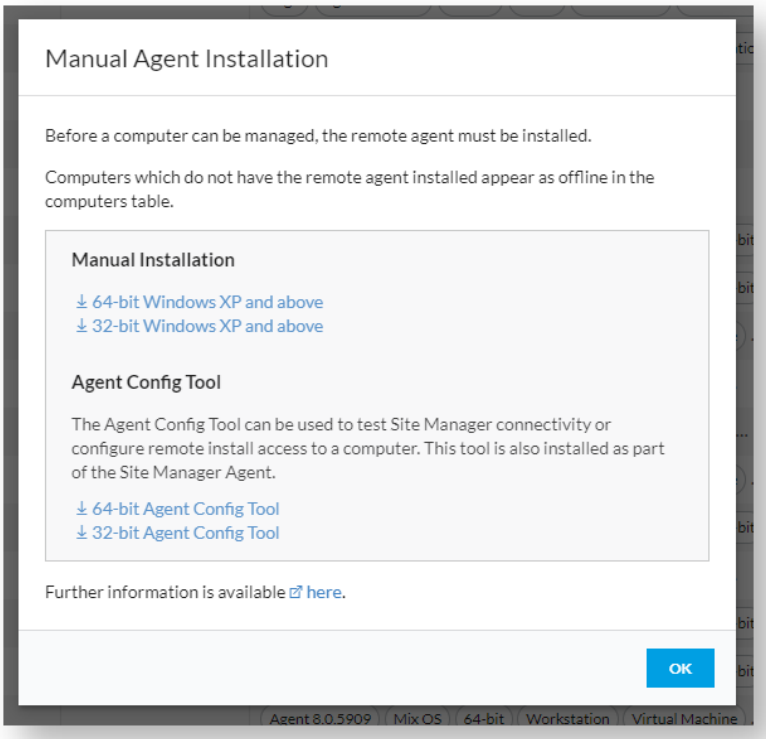
Running the Installer

If your network is not part of a Windows domain or if you are unable to remotely install the Macrium Remote Agent then you can manually install the agent on the remote computer.

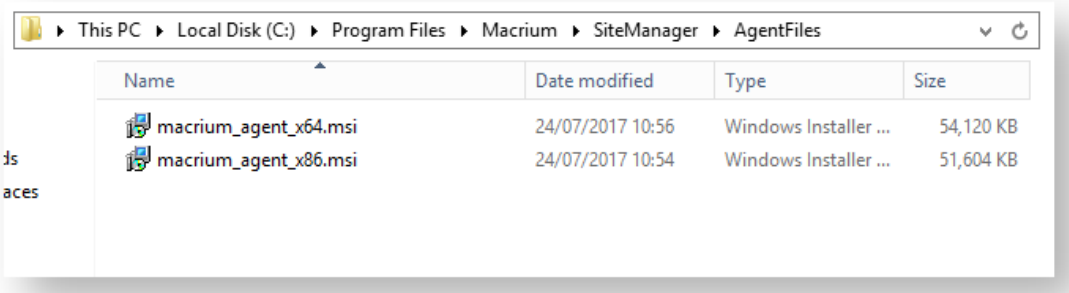
The agent MSI installer can be downloaded via the Site Manager interface on the Computers page - the option **More Actions > Manual Agent Installation** has links to the .msi files for installing agents as shown below:



Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

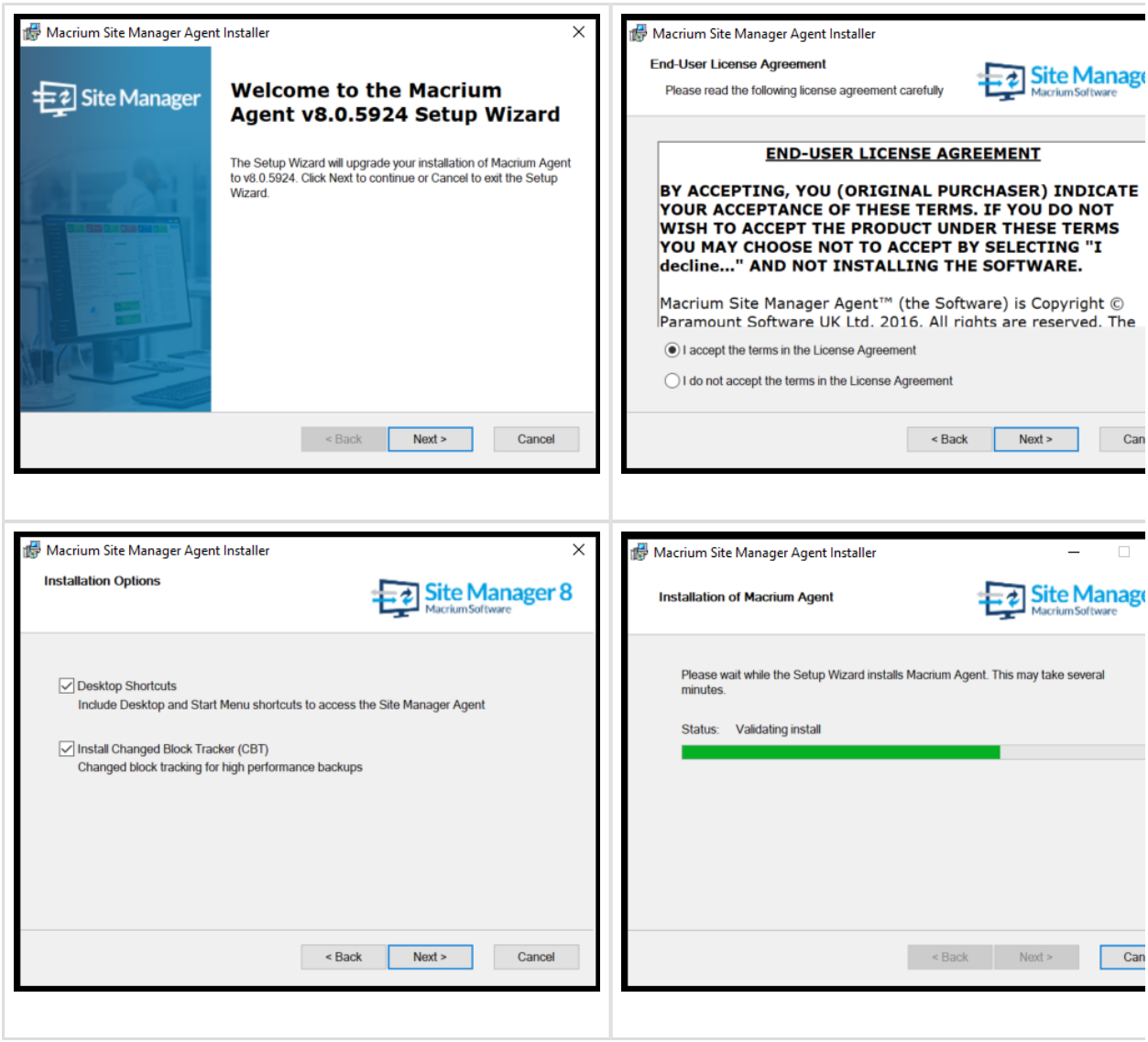


Alternatively, the agent .msi installer can be found on the Site Manager server in folder: **C:\Program Files\Macrium\SiteManager\AgentFiles**



Copy either **'macrium_agent_x64.msi' (64 Bit)** or **'macrium_agent_x86.msi' (32 Bit)** to the client PC and run by **double clicking in Windows Explorer.**

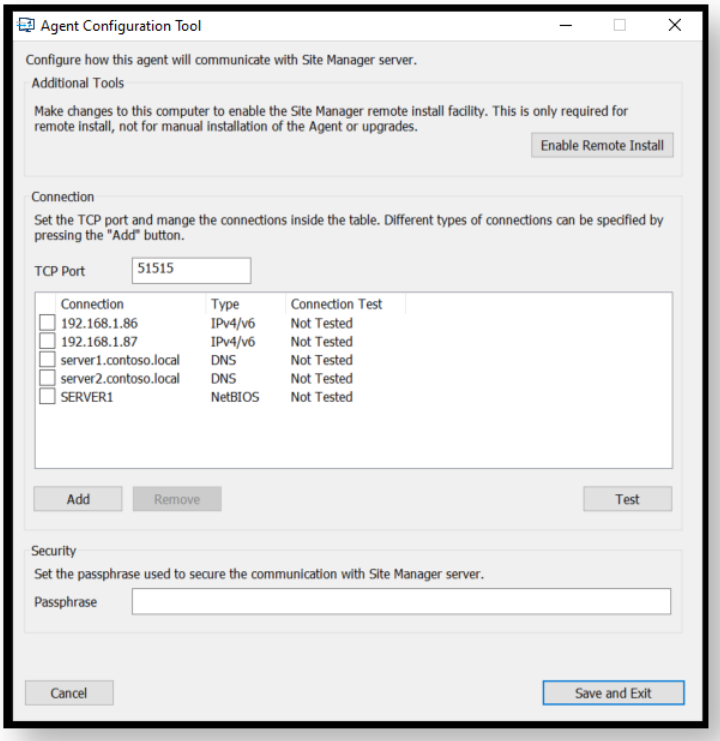
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



The **Desktop Shortcuts** option controls whether the installer will create desktop or start menu shortcuts. The **Install Changed Block Tracker (CBT)** option will install the CBT driver, which is used by the Macrium Reflect backup engine to increase the backup performance of incremental backups. This option will be disabled if the computer's OS cannot support this driver.

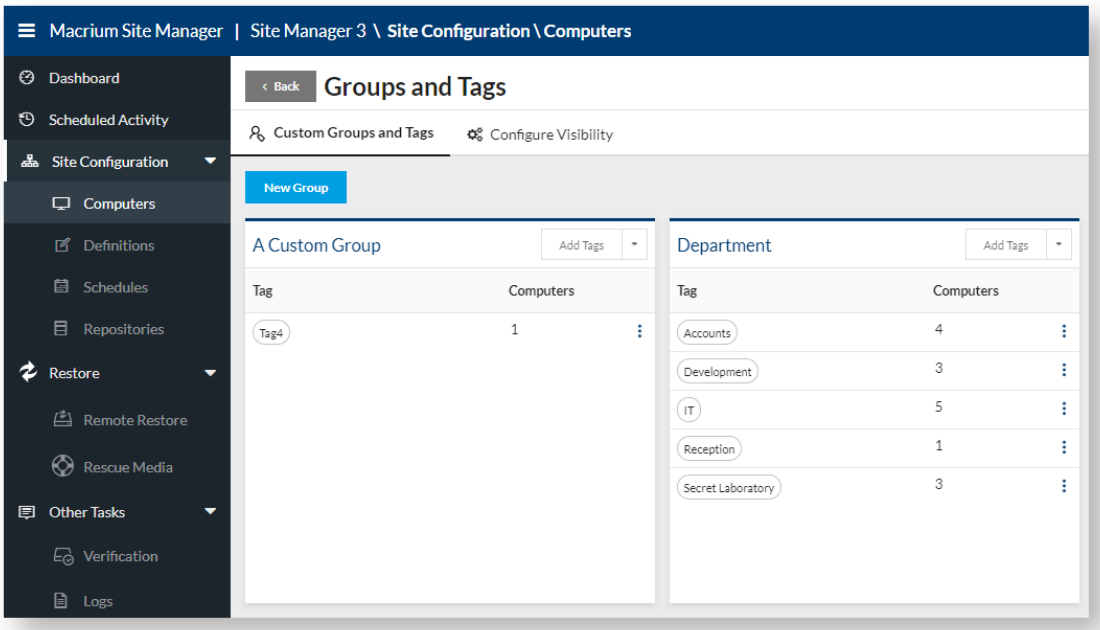
Once the install has completed, the Agent Configuration Tool will automatically run to configure the Agent's connection to the Site Manager server. See Troubleshooting Agent Communications for more details.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



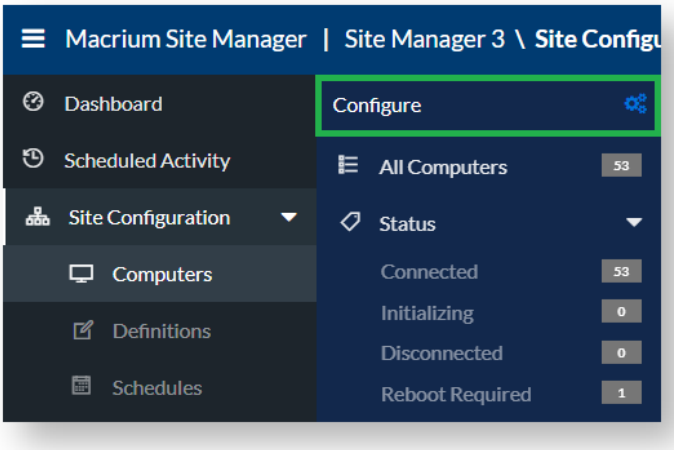
The connection to the Agent can be automatically configured in the MSI installer by using the MSI command line switches described in Deploying Site Manager Agents Using SCCM

Groups and Tags



Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

This page can be accessed by clicking on **Configure** on the **Computers** page**.**



A **Group** can contain multiple **Tags**. Those Tags can be assigned to different Computers to organize them in various ways.

There are two types of Tags:

- **Automatic Groups and Tags**: Computers have Tags assigned to them dynamically (e.g., Status, Backup Definitions).
- **Custom Groups and Tags**: Tags created by the user.

In this page, you can create, edit and delete groups and tags, assign tags to computers and configure their visibility on the side menu or/and on the tags column on computers page.

Automatic Groups and Tags

There are tags that are automatically assigned to computers:

Group Name	Description
Computer Information	General computer information such as 32- or 64-bit, UEFI, Virtual machine status
Operating System	The version of Windows running on the Agent
Status	The Site Manager connection status of the Agent: • Connected • Connected (with Errors) • Initializing • Disconnected • Migrating • Installing

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Group Name	Description
	• Upgrading • Unauthorized • Unlicensed • Patch Failed • Reboot Required • Upgrade Required
Agent Health	Any backup health checks the Agent has failed: • No Backups Scheduled • Last Backup Failed • No Recent Backups
Domain	The Active Directory Domain the Agent is joined to
Domain OU	The Organizational Unit of the computer's account in Active Directory
Backup Definitions	The Backup Definitions this computer is a part of - there will be one tag per Backup Definition
License Status	Whether the computer is unlicensed, licensed via an Agent license or via a standalone Macrium Reflect 8 license. There is an additional status **Awaiting Connection** for computers which have never connected to Site Manager and therefore do not have any license status
Agent Version	The version of Site Manager Agent installed on the computer
Reflect Version	The version of standalone Reflect (if any) installed on the computer
Reflect Edition	The edition of standalone Reflect (if any) installed on the computer (Workstation, Server, Server Plus etc)
Domain Groups	One tag will be added here for each security or distribution group that a computer's AD account is a member of
	If there is an Agent user script disabling backups on this computer, the computer will have a **Scheduled Backups Disabled** tag

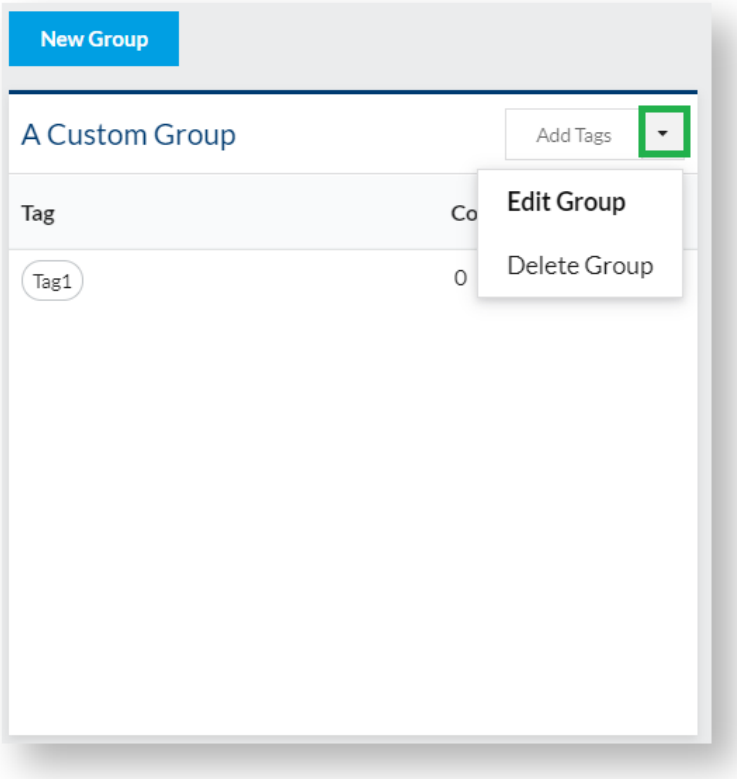
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Group Name	Description
Agent Operating Mode	
Activity	If there is an active backup or restore on a computer, it will have a **Operation in Progress** tag

Note - automatic groups are only shown if there is one or more computers which have a tag in that group present

Custom Groups

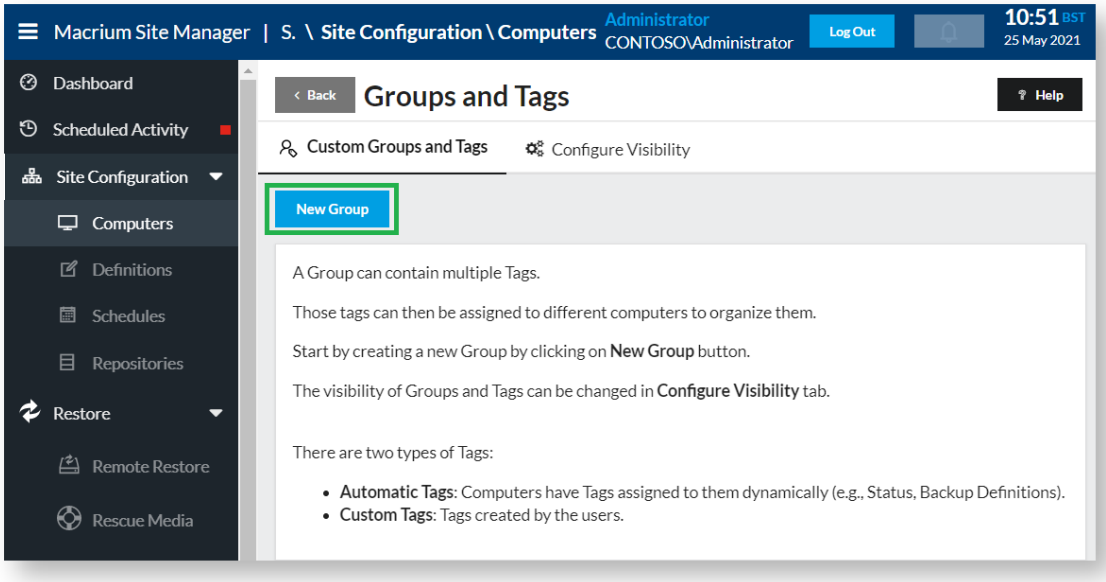
From this view, a group can be added, edited and removed as well as add tags to it.



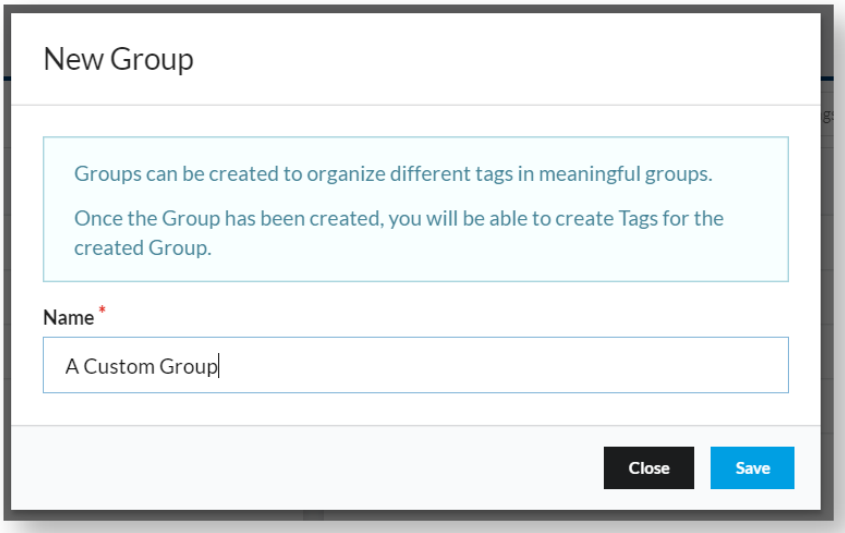
Add a Group

To add a new group, click on the "New Group" button.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

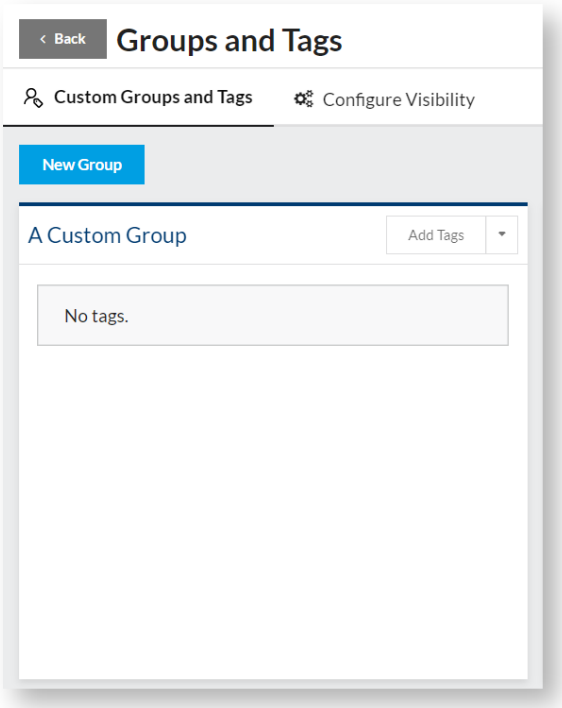


A dialog will prompt for the group's name.



Click "Save" to create the group.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

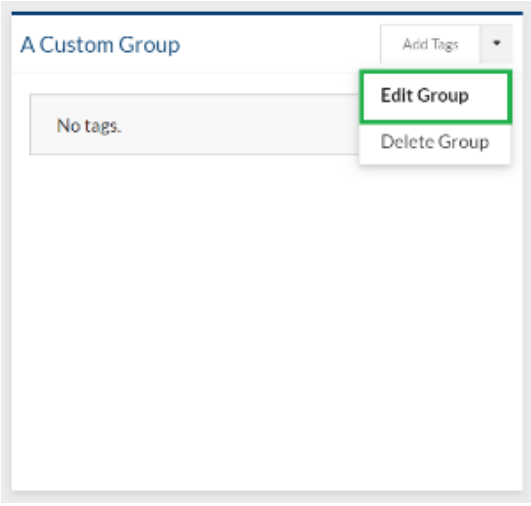


The group's name needs to be unique.

Once the group has been created successfully, tags can be added to it. Click here to know more.

Edit a Group

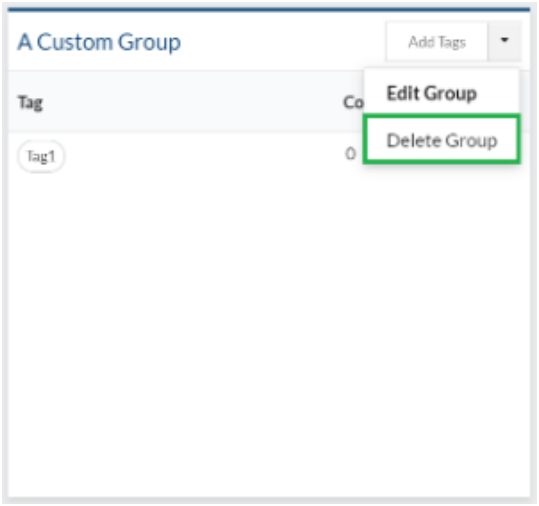
To edit a group, click on "Edit Group" and it will prompt for a new group name.



Delete a Group

To delete a group, click on "Delete Group". A confirmation dialog will open to confirm or cancel the action.

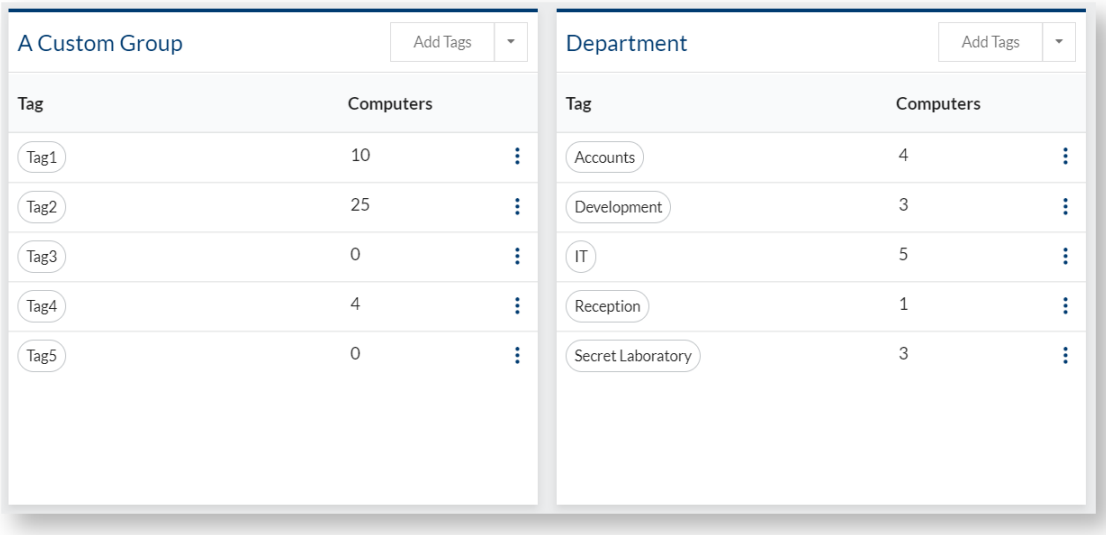
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



The group will be deleted as well as all the tags related to the group. Tags associated with this group will be removed from the computers.

Custom Tags

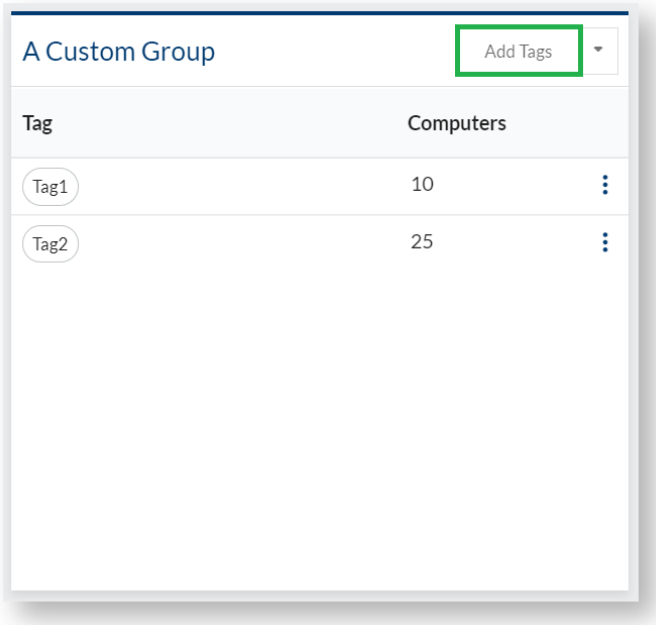
Custom tags can be added to different groups.



Add Tags

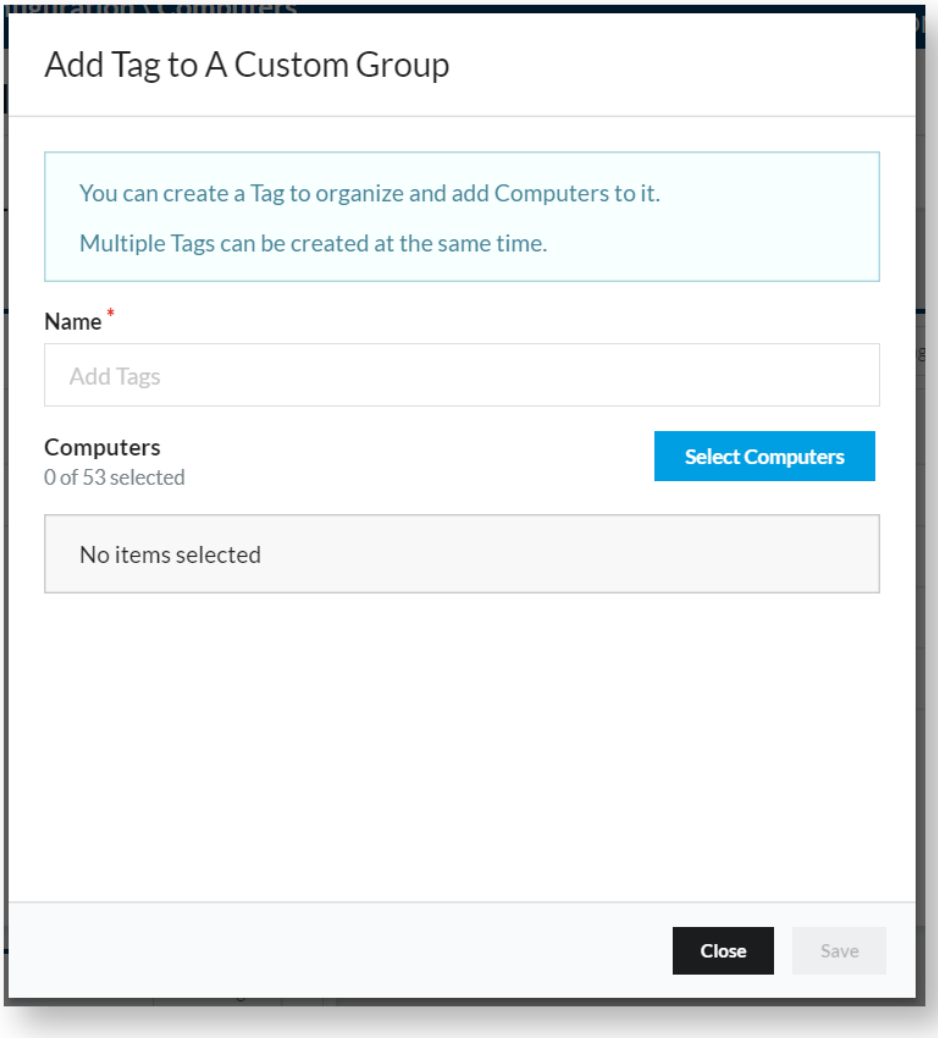
To add tags to a group, look for the group you want to add tags to and click on "Add Tags".

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



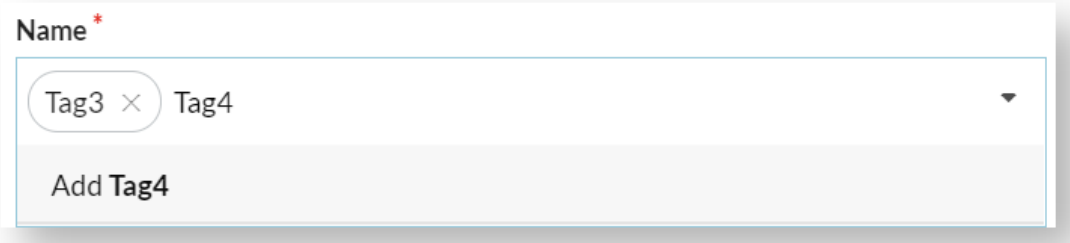
A dialog will prompt for the tag's name and the computers that will be assigned with it.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



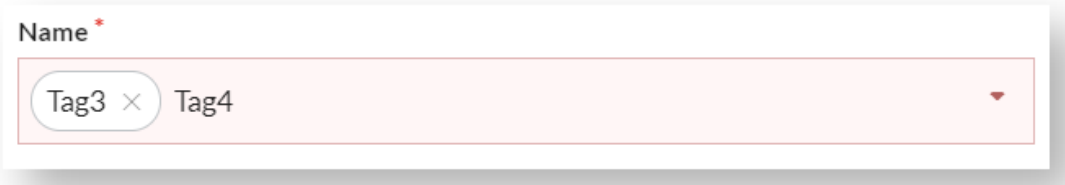
Tags

Multiple tags can be added at the same time. Press "Enter" or click on the "Add" option.

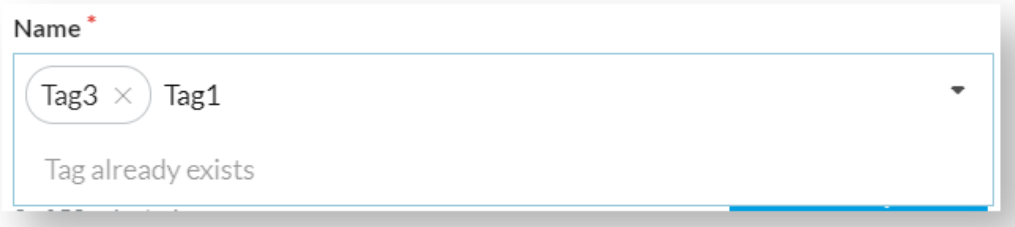


If the tag hasn't been added to the input, it will show as an error. Click on the input and follow the instruction above.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



If a tag already exists in the group, the tag cannot get added.

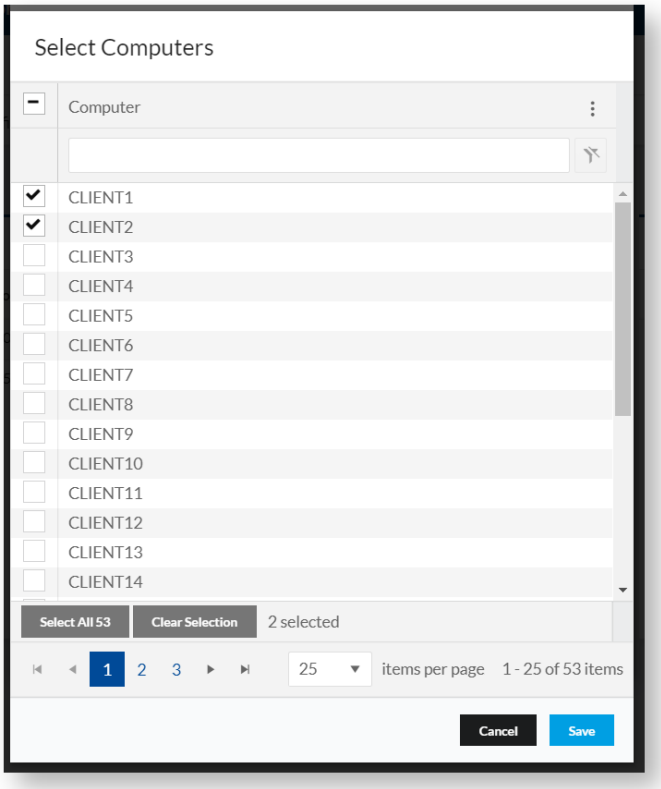


To delete a tag so it doesn't get added, click on the *x* icon.

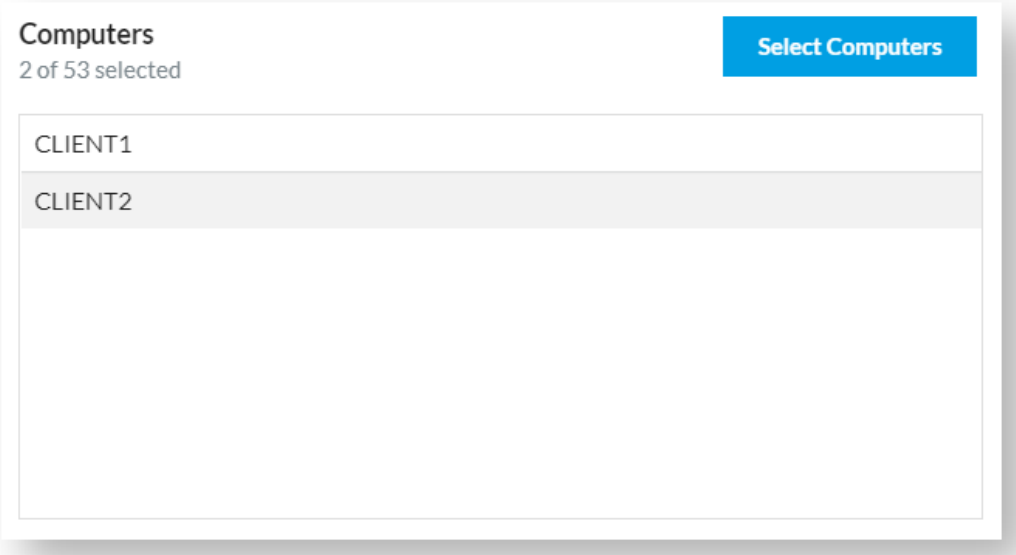
Select Computers

The next step is to select the computers that will have the tags assigned to them. Click on "Select Computers" to open the selection dialog and select the computers.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



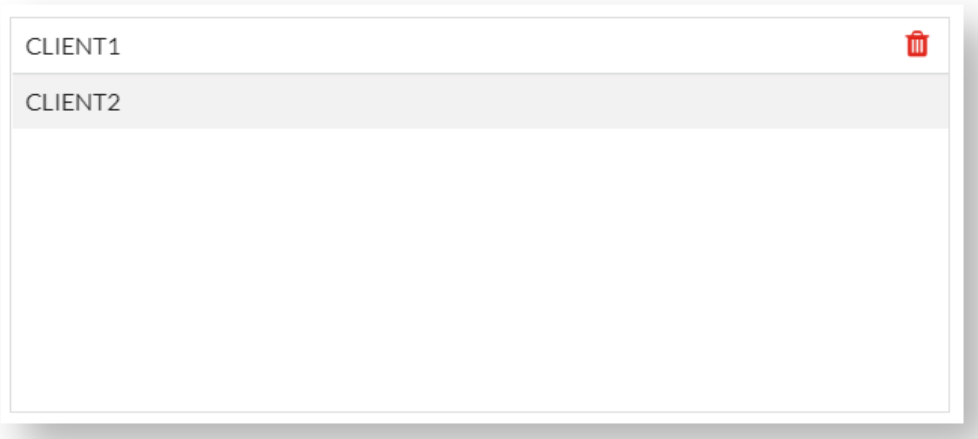
Click on "Save" to confirm and the selected computers will be shown:



To edit the select computers, click on "Select Computers" again.

If you hover over a computer row, the computer can be quickly deleted.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

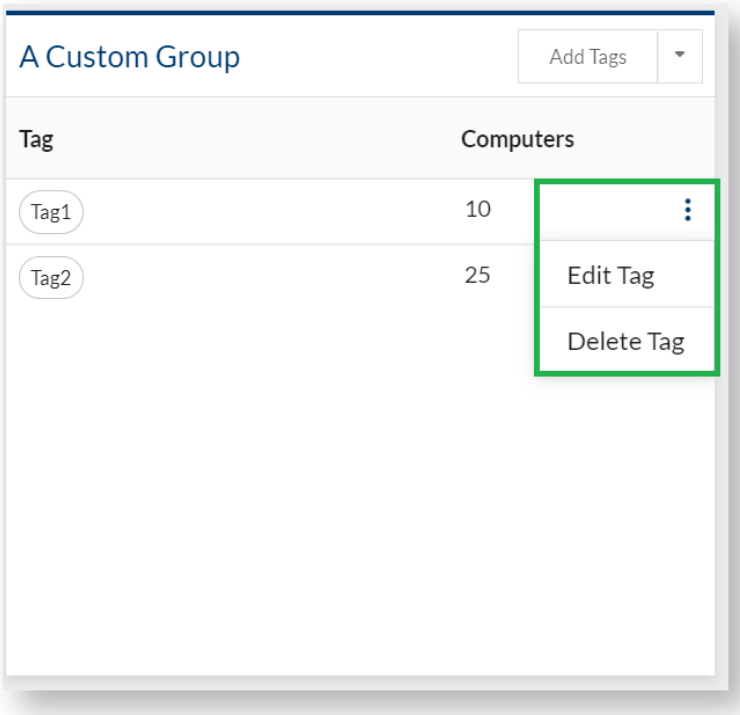


Click "Save" to confirm to create the tags and assign them to the selected computers.

> The tags names need to be unique within the same group.

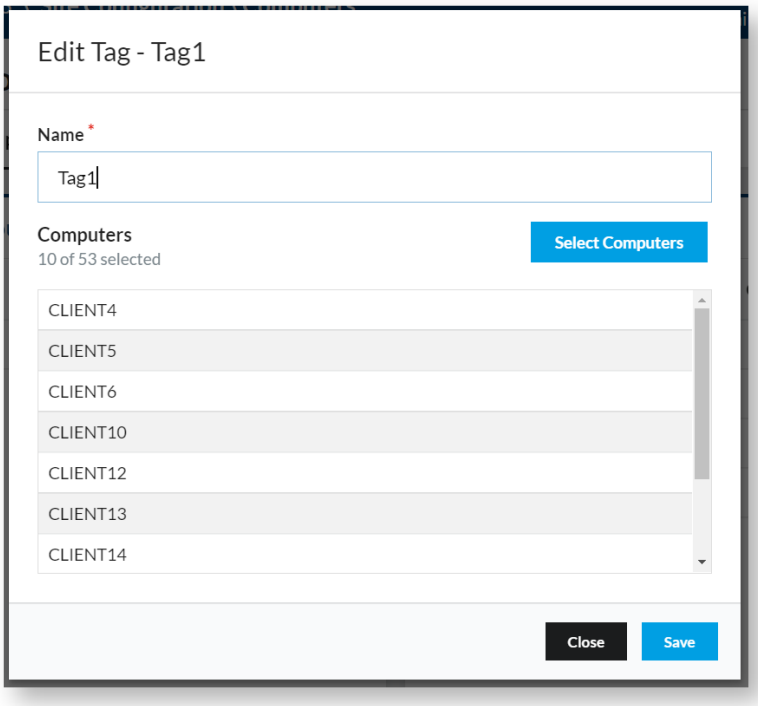
Edit Tag

To edit a tag click on the ⋮ icon to open the tags options and click on "Edit Tag" to open the edit form.



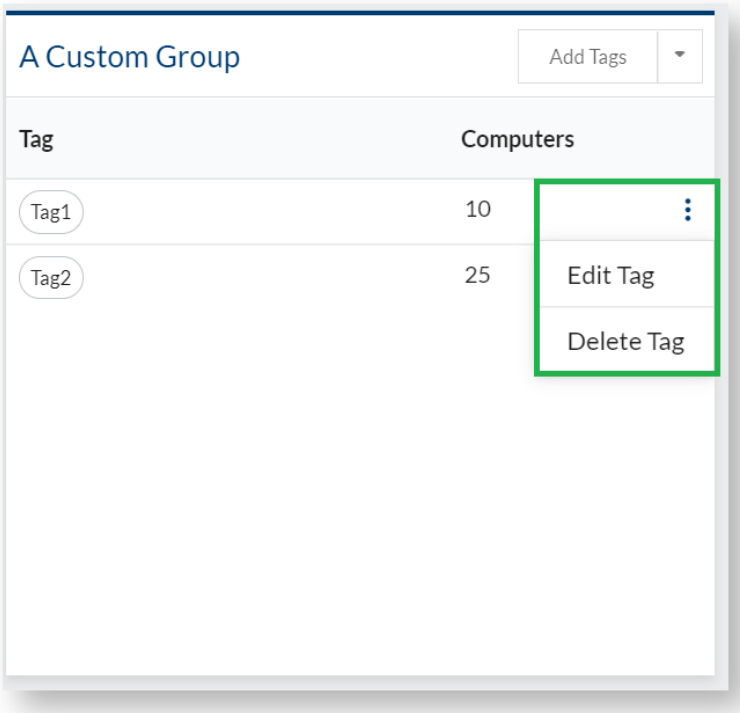
From this view, the tag's name can be edited and the selected computers can be changed.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



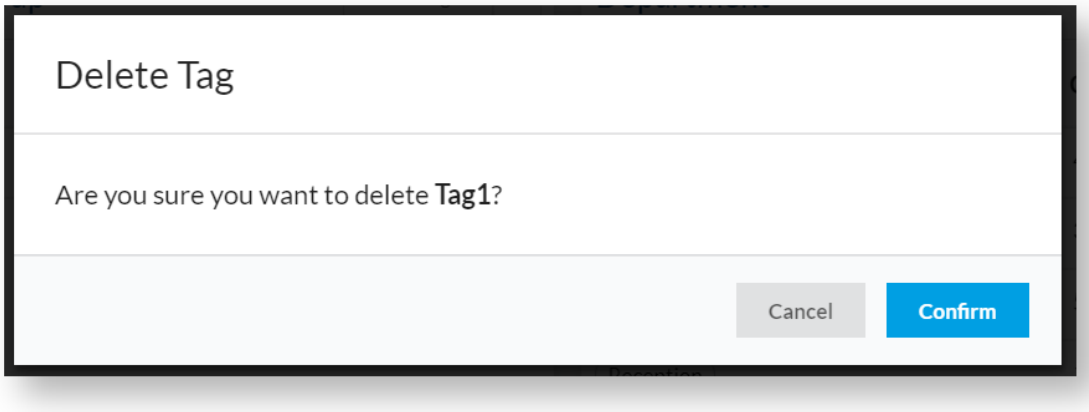
Delete Tag

To delete a tag click on the ⋮ icon to open the tags options and click on "Delete Tag".



A confirmation box will appear to confirm or cancel the deletion.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



The tag will be removed from the group and from the computers previously associated with it.

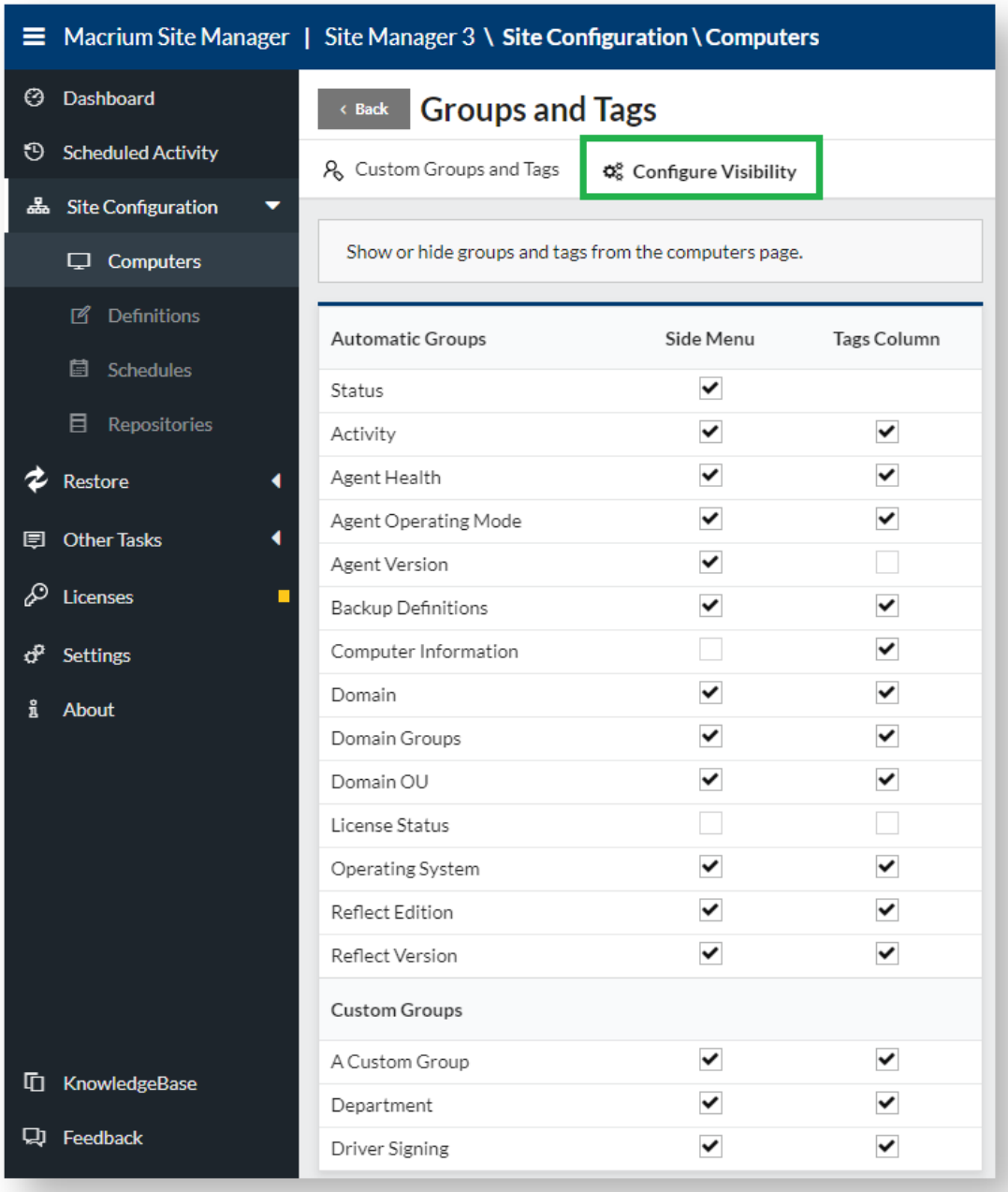
Groups Visibility

To configure the visibility of the groups on the computers page, click on the "Configure Visibility" tab.

It will show a table with all the *Automatic Groups* and all the *Custom Groups*.

The "Status" group is the only exception: it's always hidden in the Tags Column.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

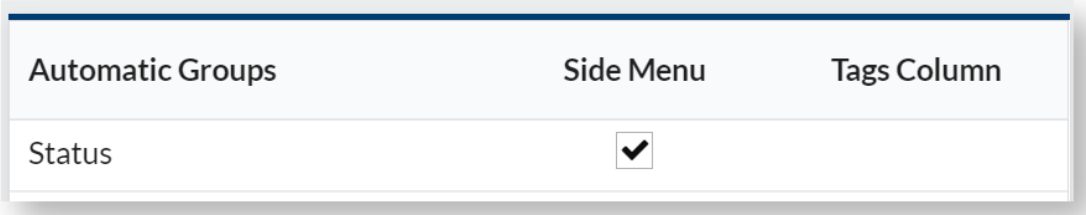


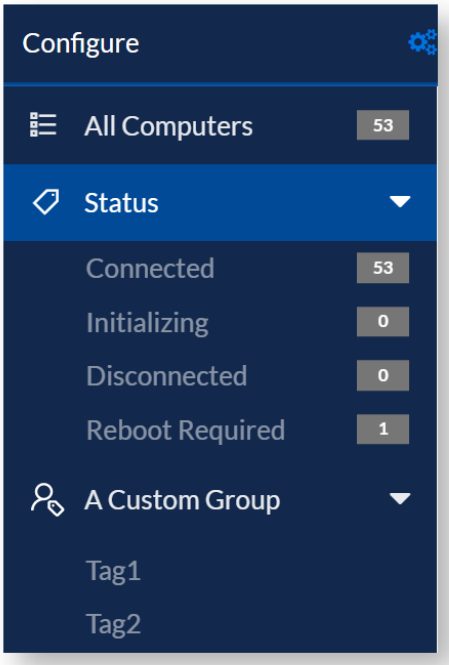
The groups can be hidden/visible on different places: Side Menu and Tags Column.

Side Menu

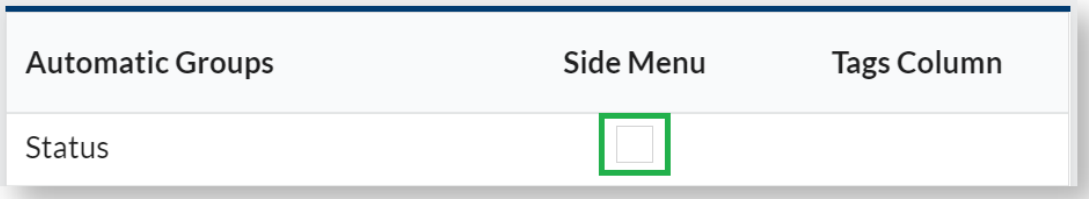
By default, the group will be visible in the side menu on the computers page.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

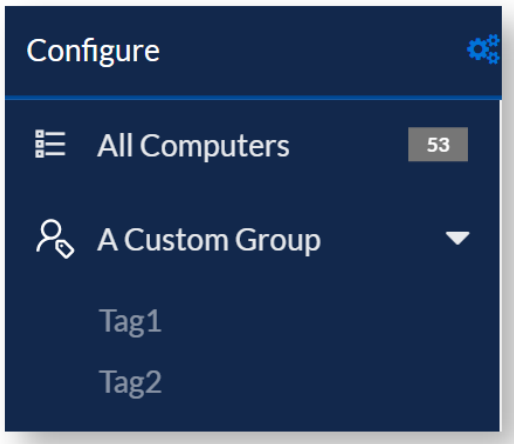




But it can be hidden by unchecking the option and clicking "Save" at the bottom of the page.

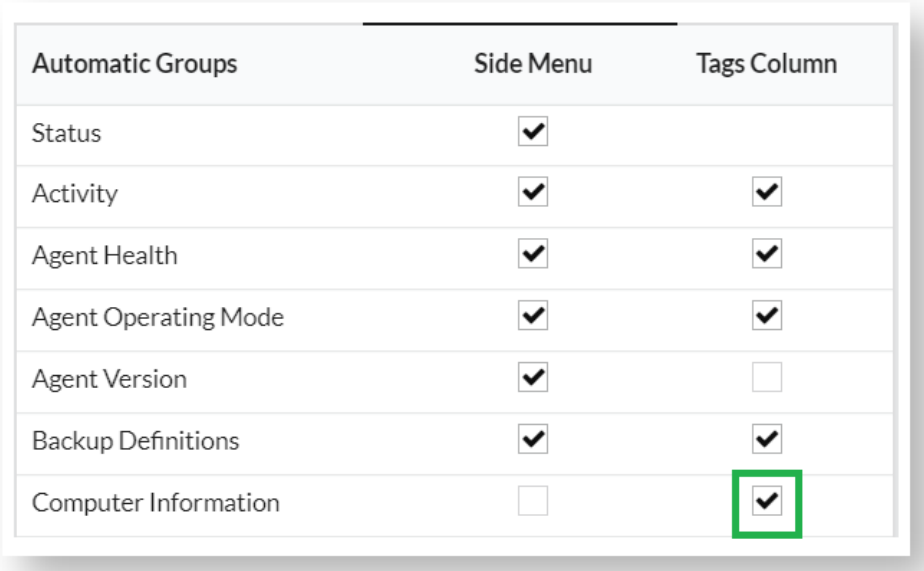


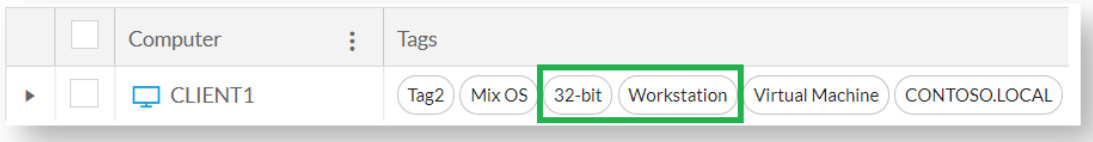
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



Tags Column

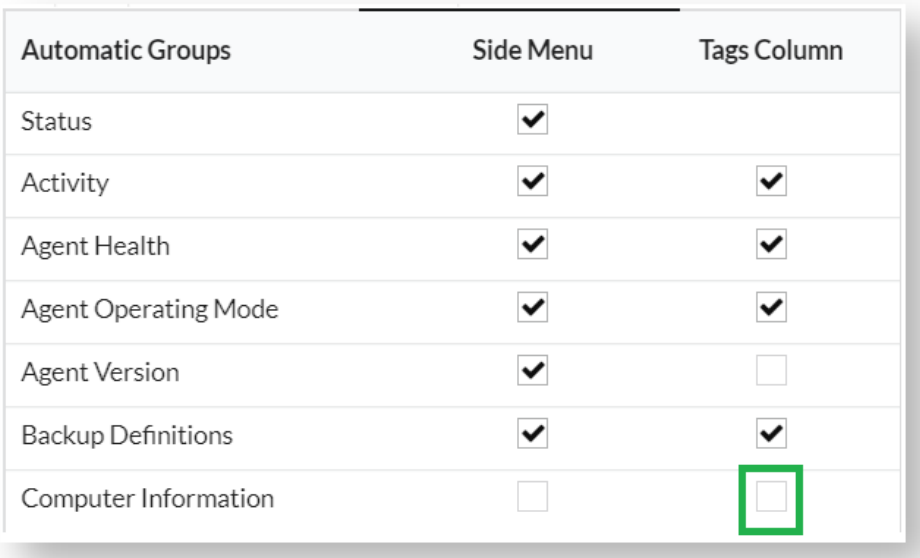
By default, all the tags will show on the Tags column on the computers page.

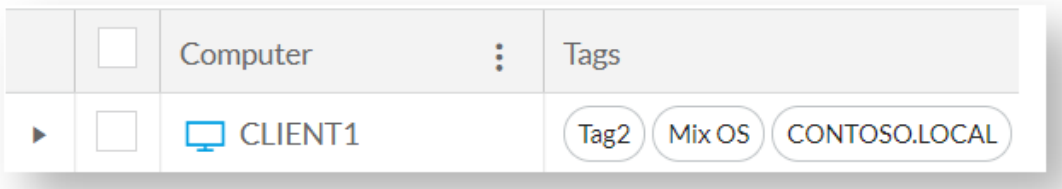




But it can be hidden by unselecting the option and clicking "Save" at the bottom of the page.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.





Setup - Backup Definitions

A **Backup Definition** contains the data needed to perform a backup on a set of computers. Each definition contains settings for the following information:

- A list of computers which should be backed up.
- A set of rules describing which partitions, disks or files to backup on each computer
- A set of options and settings controlling how the backup files should be created and stored.

Backup Definitions contain all the information on *how* and *what* to backup. A Backup Definition can be run manually to perform a single backup of each computer or used to schedule regular backups into a Repository

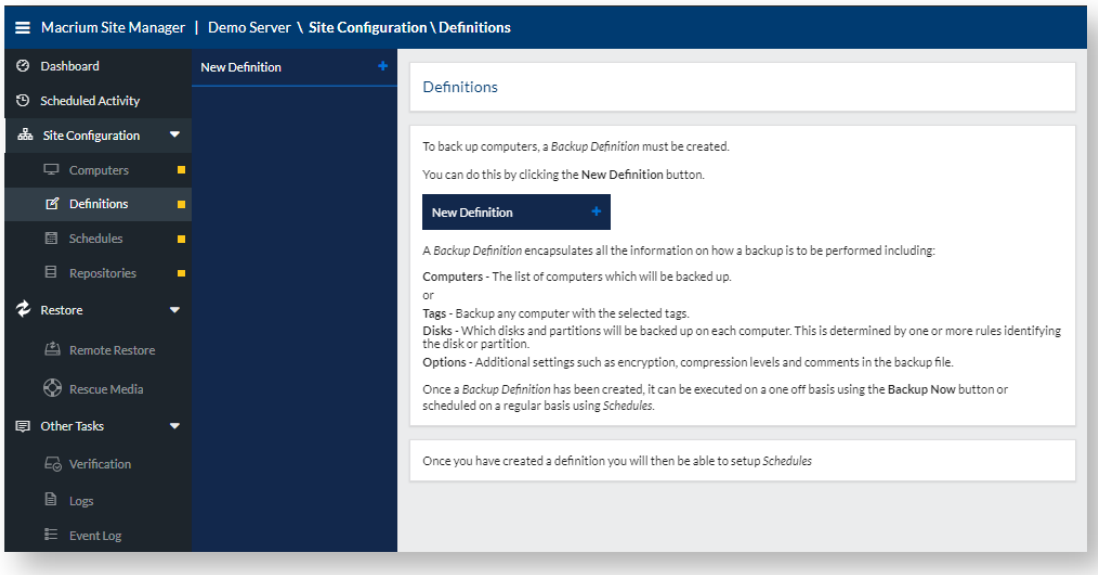
- Creating a Backup Definition
  - Step 1 - Definition Type
  - Step 2 - Computers Selection
  - Step 3 - Disk Image - Disk Selection Rules
  - Step 3 - File and Folder - File and Folder Selection
  - Step 4 - Options
- Backup Definition Operations

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

- Deleting a Backup Definition
- Copying a Backup Definition
- Editing a Backup Definition
- Running a Backup Definition Manually
- Running Backups Automatically on a Schedule

Creating a Backup Definition

The '**Backup Definition**' section option in Site Manager contains the list of existing Backup Definitions. If there are no Backup Definitions created, a quick help page is shown instead:

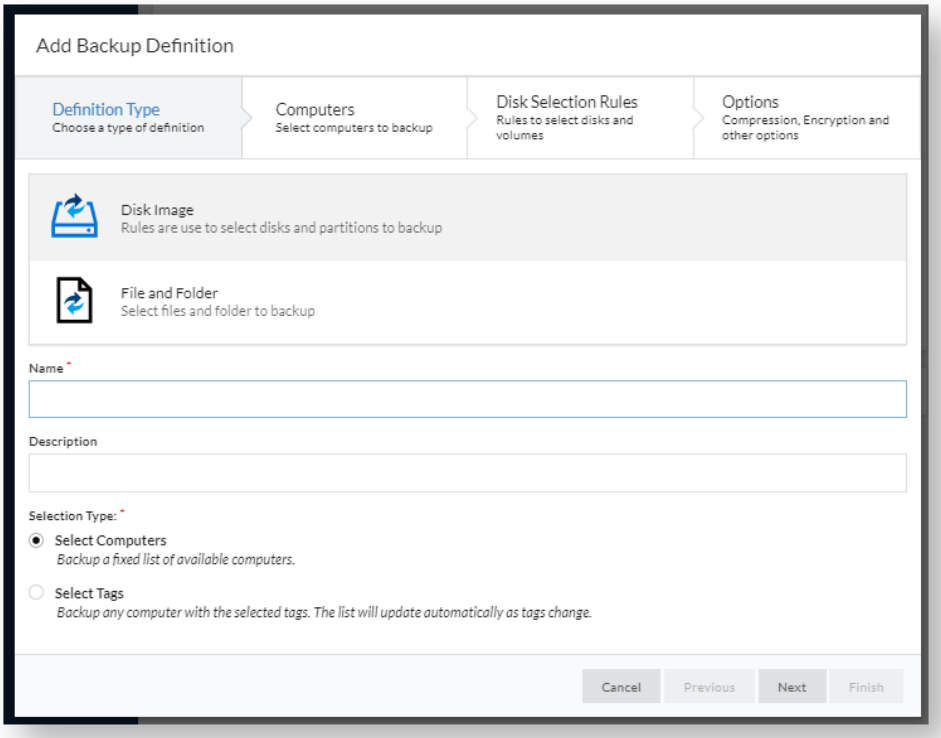


Clicking on '**New Definition**' will open the Backup Definition wizard.

The steps of the wizard are:

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Step 1 - Definition Type



The first step is to select the type of Backup Definition. The types available are:

Definition Type	Description
Disk Image	This definition type creates image backups of full disks or partitions. It is configured by setting a set of rules which control which partitions or disks are included. This is the most efficient backup type for large amounts of data and provided the correct partitions have been backed up, these image files can be used to restore a fully bootable Windows OS.
File and Folder	File and Folder backups only back up files on specific paths from a disk. This is a faster, more convenient backup type when only critical data from a disk needs to be backed up. e.g. c:\accounts*.*

Once the backup type has been selected, a name for the Backup Definition must be entered. This is for display purposes only. An optional description may also be entered.

The **Selection Type** controls how computers are selected for backup in the next step of the wizard. The available options are:

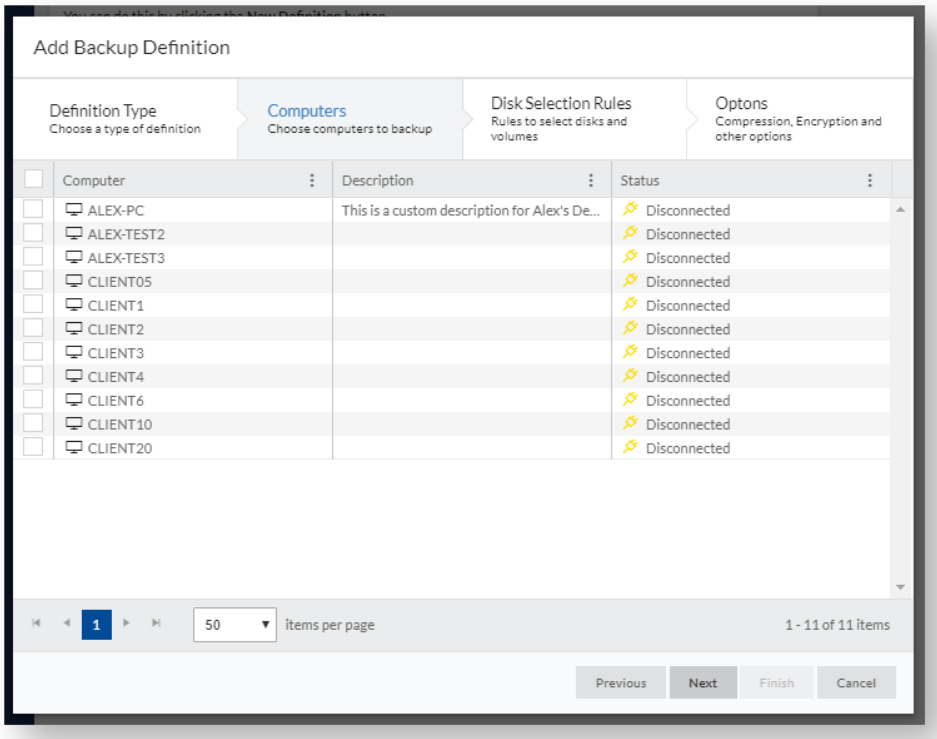
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Selection Type	Description
Select Computers	Select computers from a list. Computers will remain part of this backup definition until removed manually
Select Tags	Select a set of tags to associate with this backup group. Any changes to the membership of these tags will change the backup definition automatically

Step 2 - Computers Selection

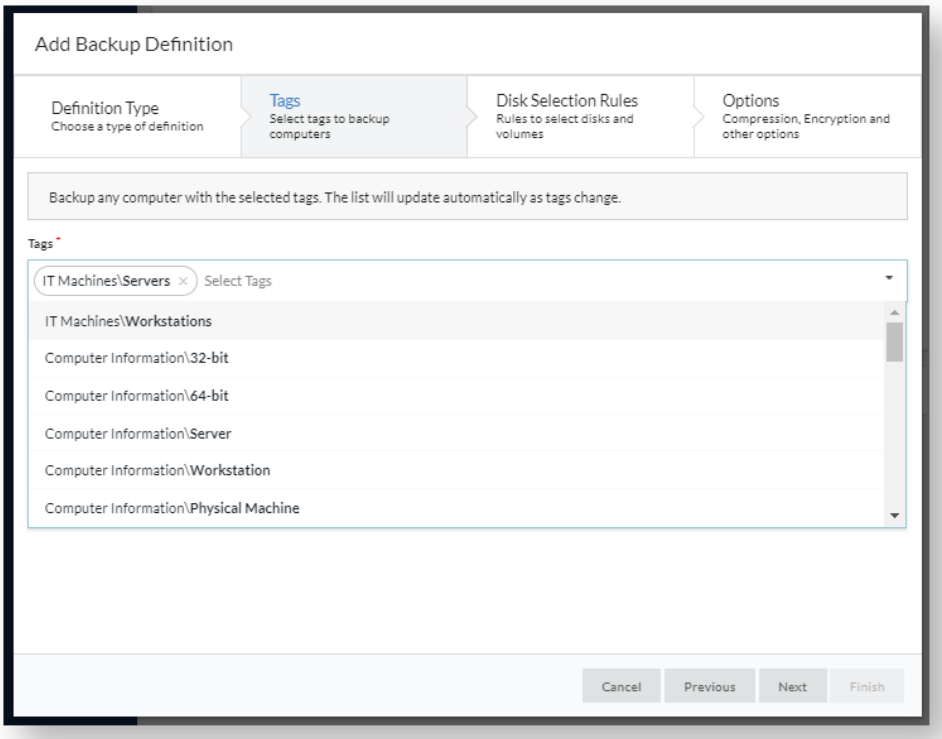
This stage lists available computers to be part of the Backup Definition. If **Select Computers** was chosen in the previous step, a computers list will be displayed:

Columns can be filtered and sorted in the computer list to aid in finding the right computers. If there are large numbers of computers they will be split into multiple pages.



If **Select Tags** was chosen in the previous step, the tags selection will be displayed:

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



This interface allows multiple tags to be selected. Not all tag groups are valid for use as a Backup Definition tags. Only the following groups can be used:

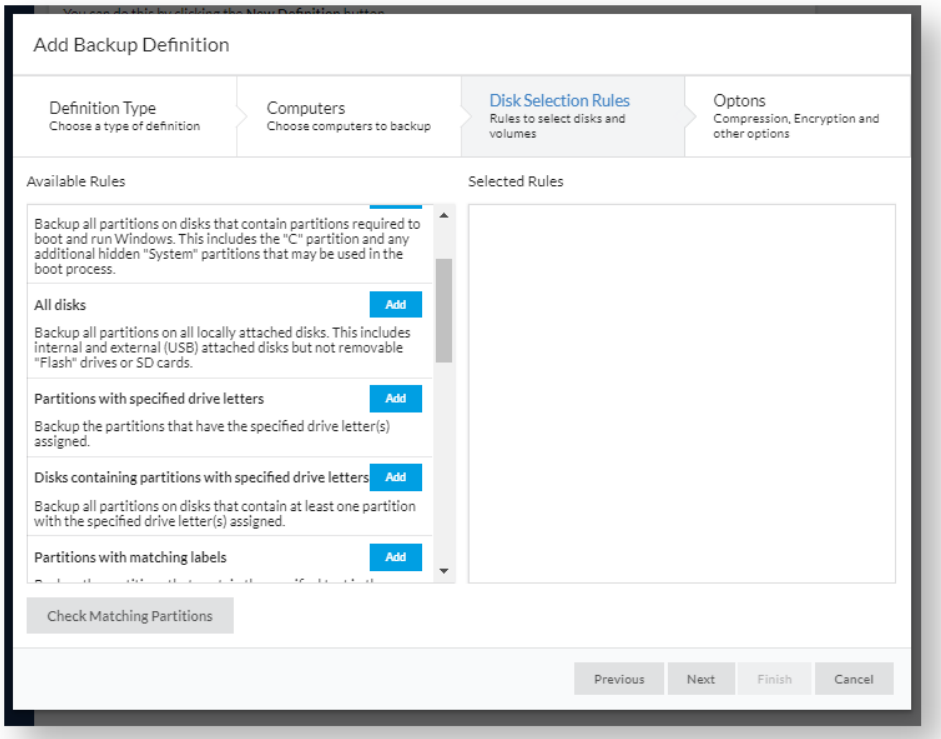
- Any user created tag
- Computer Information (Architecture, virtual machine status)
- Windows Version
- Domain
- Domain OU (Organizational Unit)
- Domain Groups (Security and Distribution Groups)

Once the computers or tags required have been selected, press **Next** to advance to the next step. This step will vary depending on the definition type selected in stage 1.

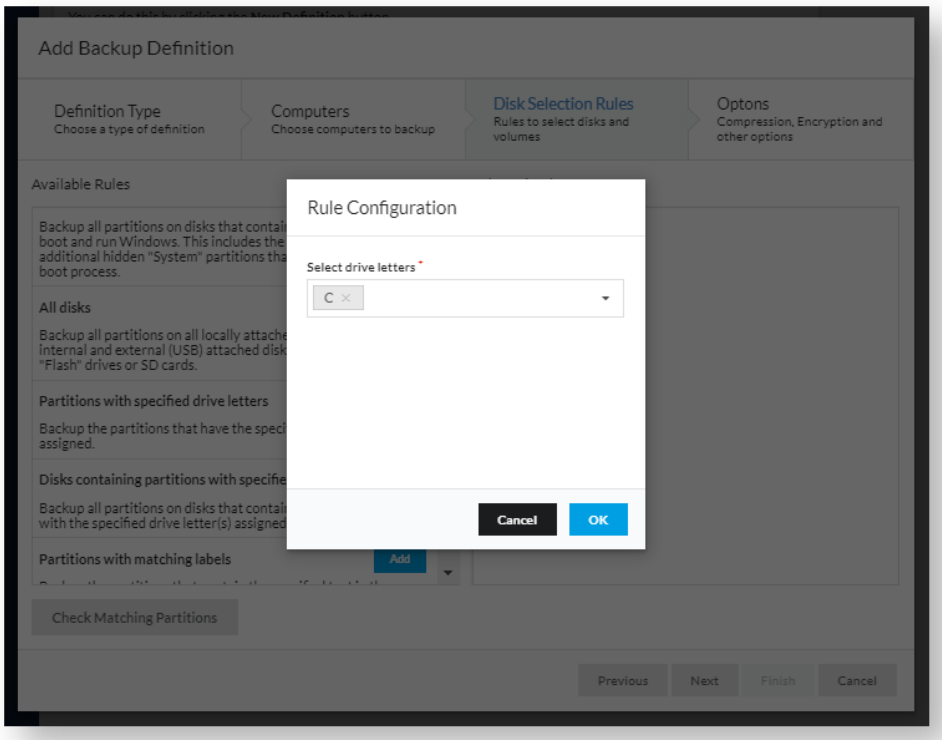
Step 3 - Disk Image - Disk Selection Rules

For **Disk Image** backups, the next stage is to select rules which control which partitions and disks will be imaged as part of the backup.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



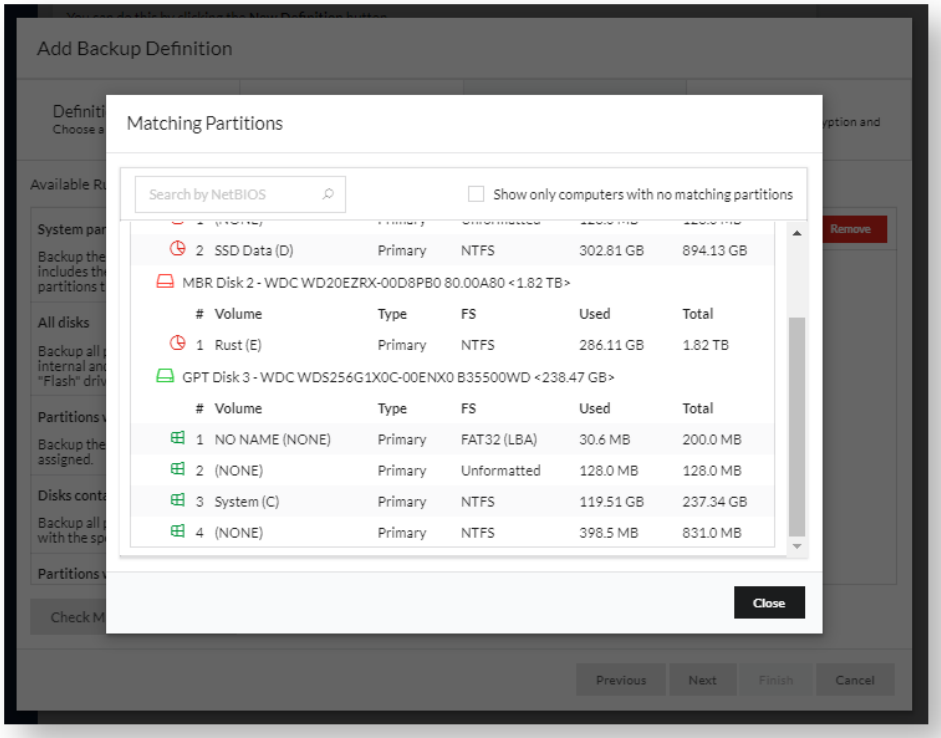
A set of rules are available on the left hand side of the screen. To use a rule, press the **Add** button on the rule to move it to the right have side of the list. Some rules have additional configuration such as a volume label or drive letter to match. In this case, a dialog box will pop up when adding the rule as seen below:



Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Once rules have been added, they are listed in the right hand pane of the interface. If a rule has additional configuration, it can be reconfigured by pressing the pencil icon on the right of the rule name. A rule may be removed by clicking it to select and clicking the **Remove** button.

To assist in configuration, pressing the **Check Matching Partitions** button will show the partitions on the computers in the definition which match the rule:



The disk matching information can be filtered by computer or to show only computers with no matches. This can help identify any gaps in rules.

For simple operation, there is an '**All Disks**' rule which will match everything on all computers.

Exclude Rules

There are exclusion rules as well as inclusion rules - the exclusion rules make it easier to backup all data except those meeting the criteria. For example, if there are multiple computers in the definition, each with a number of partitions and drive letters which need to be backed up without backing up the Windows partitions, this can be achieved using an exclusion rule. Exclusion rules work in the following way:

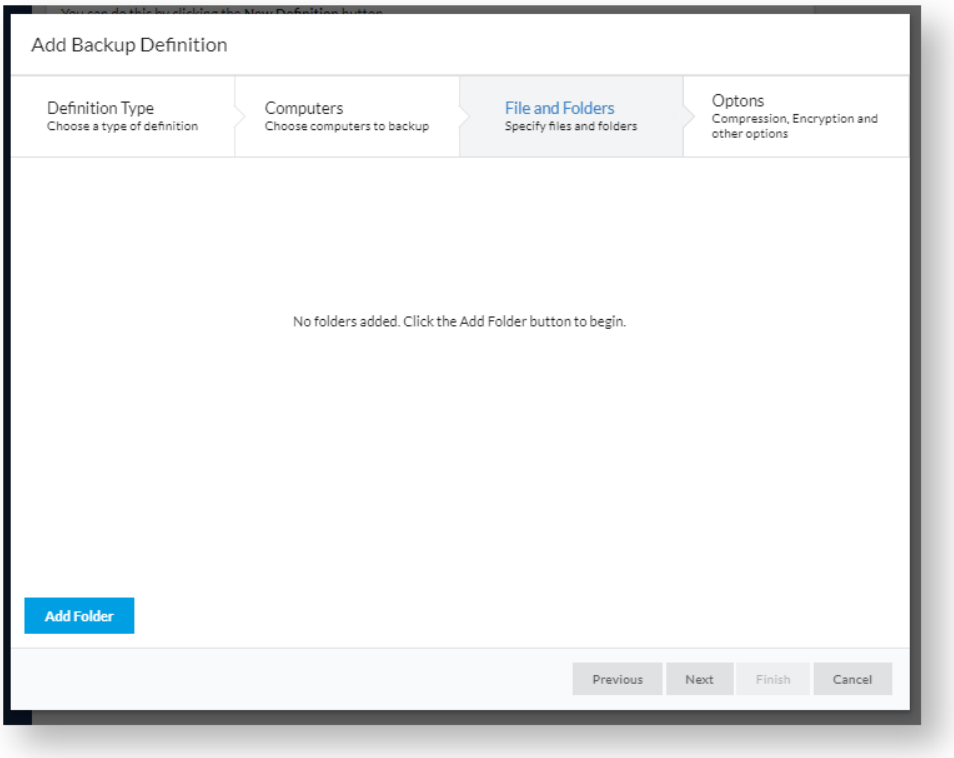
- Exclude rules override include rules - a definition with an include rule for system drives plus an exclude rule for the C: partition will backup system partitions except for the C: partition.
- If there are only exclude rules, all partitions are included except for those specified by the exclude rule - a definition with just an exclude rule for C: and D: partitions will backup all other partitions.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Once rules are configured, press next to move to the next step.

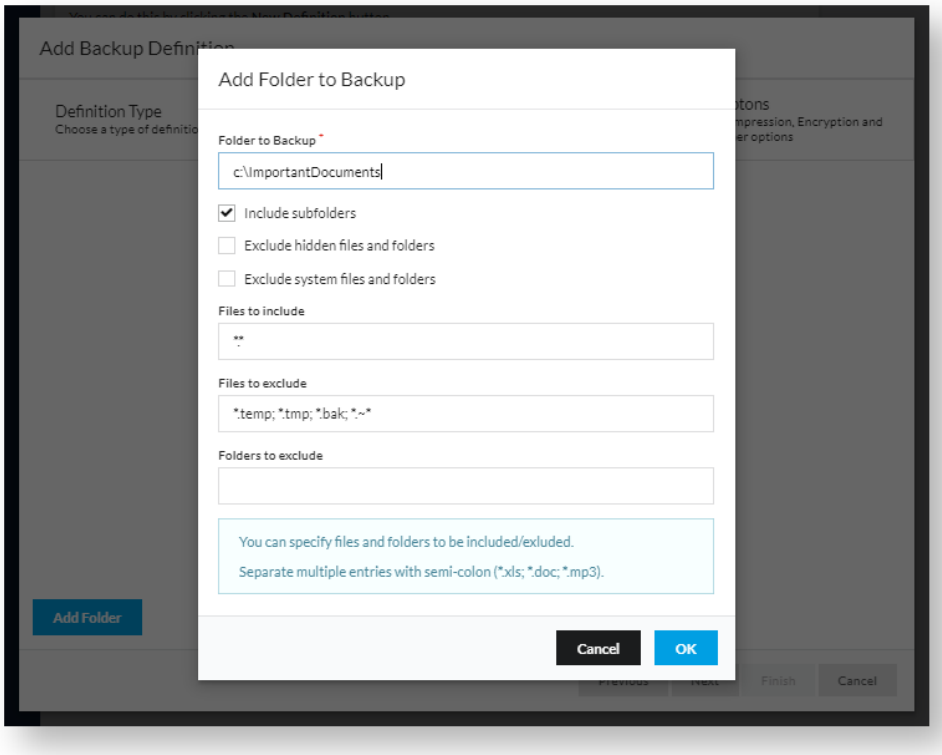
Step 3 - File and Folder - File and Folder Selection

For **File and Folder** backups, the next stage is to select the folder rules which will be used to identify the files to backup.



At least one folder must be added, using the **Add Folder** button.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

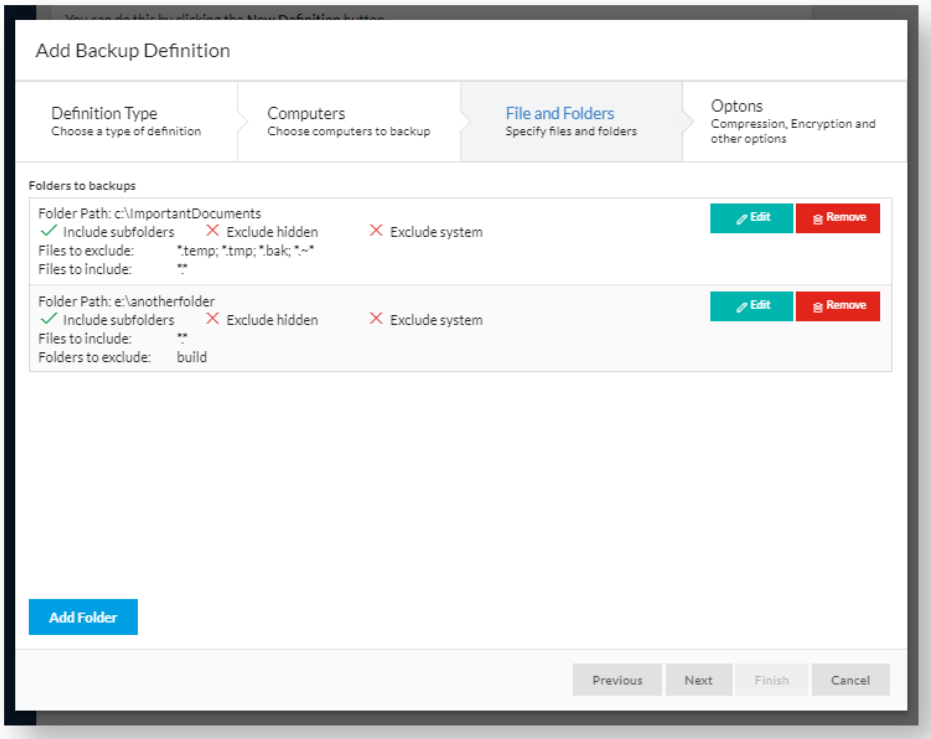


The Add Folder dialog has the following options:

Option	Description
Folder to Backup	The folder path on the Agent computer which will be included in the backup.
Include subfolders	If checked, this option will cause any matching files in subfolders of the target folder to be included in the backup
Exclude hidden files and folders	If checked, any files or folders with the 'hidden' file system attribute will be ignored
Exclude system files and folders	If checked, any files or folders with the 'system' file system attribute will be ignored
Files to include	A file mask for names of files to include within the selected folder/subfolder. e.g. ***.docx** will include only document files
Files to exclude	As **files to include**, but these files will be excluded. Takes precedence over the include list
Folders to exclude	As **files to exclude**, except it is used for subfolder names. Only relevant when **Include subfolders** is used

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

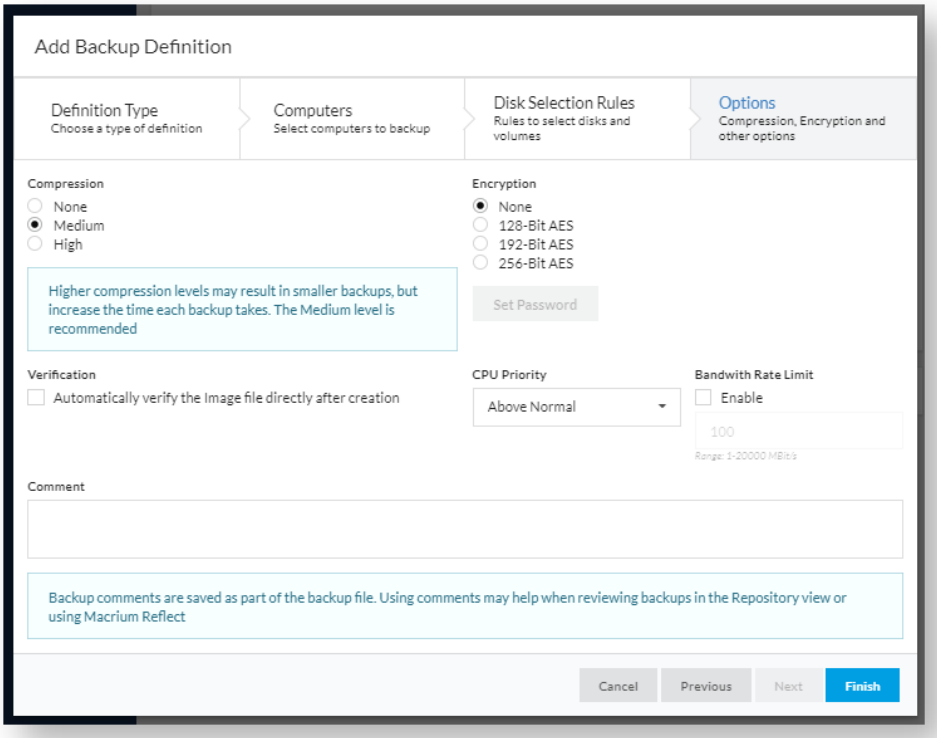
Multiple rules can be added to one definition - files matching any rule will be backed up. Rules can be removed and edited using appropriate buttons:



Once rules are configured, press next to move to the next step.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Step 4 - Options



In step 3, options for how the backup files are created are set.

Backup Option	**Description**
Compression	The level of compression to use in any backup files created when using this Backup Definition. The default level is '**Medium**'.
Encryption	The type of encryption to use on any backup files created from this Backup Definition. If AES encryption is used, a password must be entered using the '**Set Password**' button.
Verification	If this option is selected, backup files will be reread and verified immediately after creation.
Comment	If a comment is entered here it will be saved as part of any backup files created and be visible to any restore tools.
CPU Priority	The CPU priority to run the backup process as. Lower priorities may result in the backup taking longer if there is contention for CPU resources. The default priority is **High**

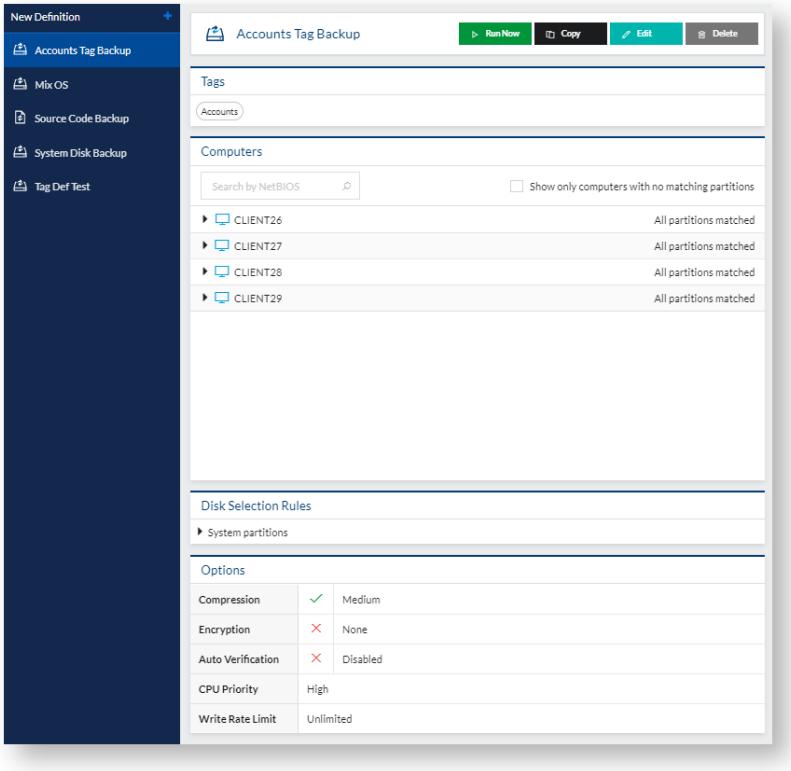
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Backup Option	Description
Bandwidth Rate Limit	If enabled, a rate limit can be set for writing to the repository. This will limit the write rate to a specified number of MBit (megabits) per second. This can be used to help manage bandwidth when performing large numbers of backups. In the backup progress, a higher transfer rate than the rate limit may be displayed. This is because the transfer limit counts the amount of data read from the source disk and saved into the backup file without including compression. After backup is completed, the read and write rate are shown in the backup log.

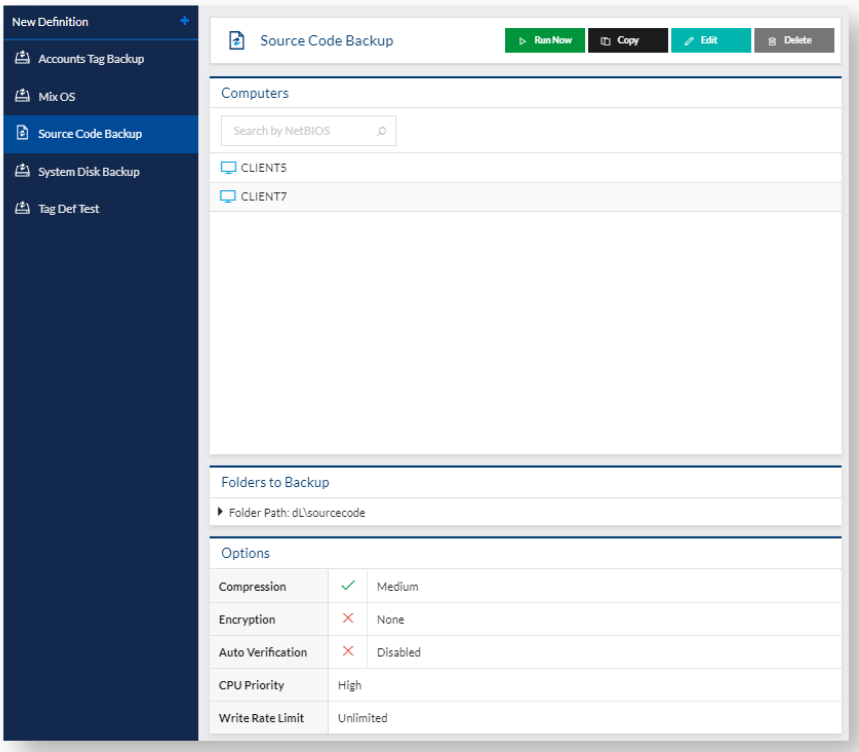
Once the options are set appropriately, press finish to complete the wizard and save the Backup Definition. If there are any errors or issues with saving the Backup Definition, the wizard will not close and an error message will be displayed. If appropriate any affected fields will be highlighted in red.

Backup Definition Operations

Once Backup Definitions have been created, they are shown in a list as below:



Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



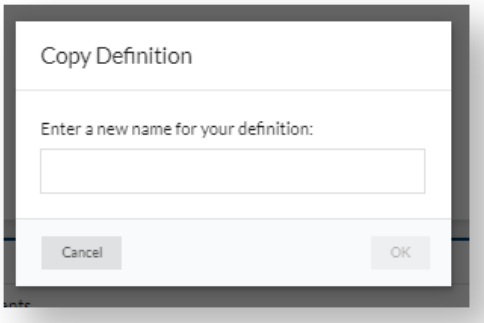
The selected Backup Definition can be changed by clicking on the list of names in the left-hand column. Once a Backup Definition has been selected, the configuration of that Definition is shown. Several operations can be performed on this Definition.

Deleting a Backup Definition

Clicking the '**Delete**' button to the right of the definition name will delete the selected Backup Definition.

Copying a Backup Definition

Clicking the '**Copy**' button to the right of the definition name will copy the selected Backup Definition to a new Definition which can then be edited. This is useful for creating multiple Definitions with only minor differences. The new Definition must be given a new name:



Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

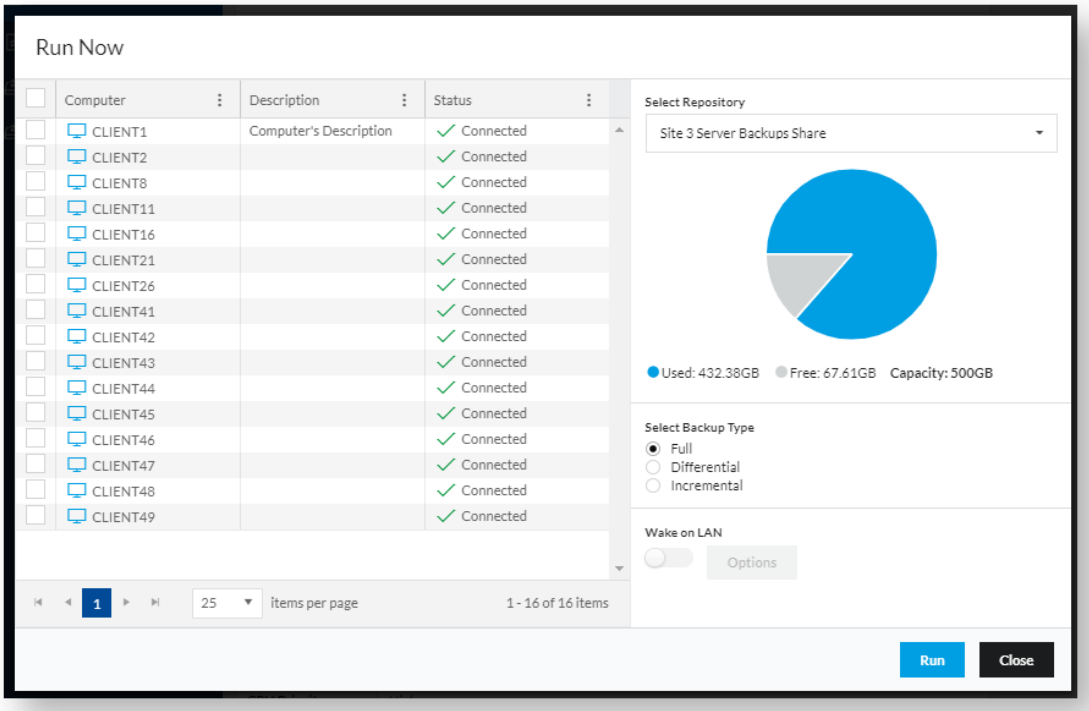
Editing a Backup Definition

Editing a Backup Definition is possible by clicking any of the **Edit** buttons in the page. Each button will open the Backup Definition wizard at the appropriate wizard step. This is the same process used in creating a Backup Definition except the wizard will be pre-populated with data from the selected Definition. When editing a Backup Definition the '**Finish**' button may be pressed at any stage and not just the final one.

Running a Backup Definition Manually

To run a Backup Definition on a one-off basis, the **Run Now** button can be clicked. This opens a dialog which allows to to select:

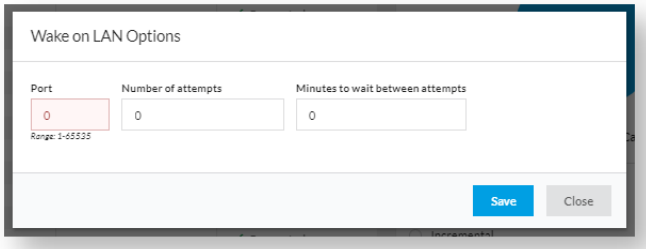
- The computers to backup
- The Repository to backup to
- The type of backup (Full, Differential, Incremental)



If the **Wake on LAN** option is selected, disconnected computers may be selected as well as connected ones. The Site Manager server will attempt to wake any disconnected computers up as part of the the backup process.

The Wake on LAN options allows detailed Wake-on-LAN options to be set:

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



Selecting **Run** will run the backup with the selected options. Run Now backups can be seen in the forecast in the **Dashboard** page.

Backup Types

If a Differential or Incremental backup is selected without a corresponding Full backup in the Repository to base the Differential or Incremental backup on, the computer will perform a Full backup instead.

Running Backups Automatically on a Schedule

To perform automated backups according to a schedule, The Backup Definition can be scheduled to run in a Repository according to a Schedule. More information is available here.

Setup - Schedules

- Overview
- Default Schedules
- Creating a Schedule
  - Step 1 - Triggers
  - Step 2 - Retention Rules
  - Step 3 - Options
  - Finalizing the Schedule
- Editing and Deleting Schedules
- Copying Schedules

Overview

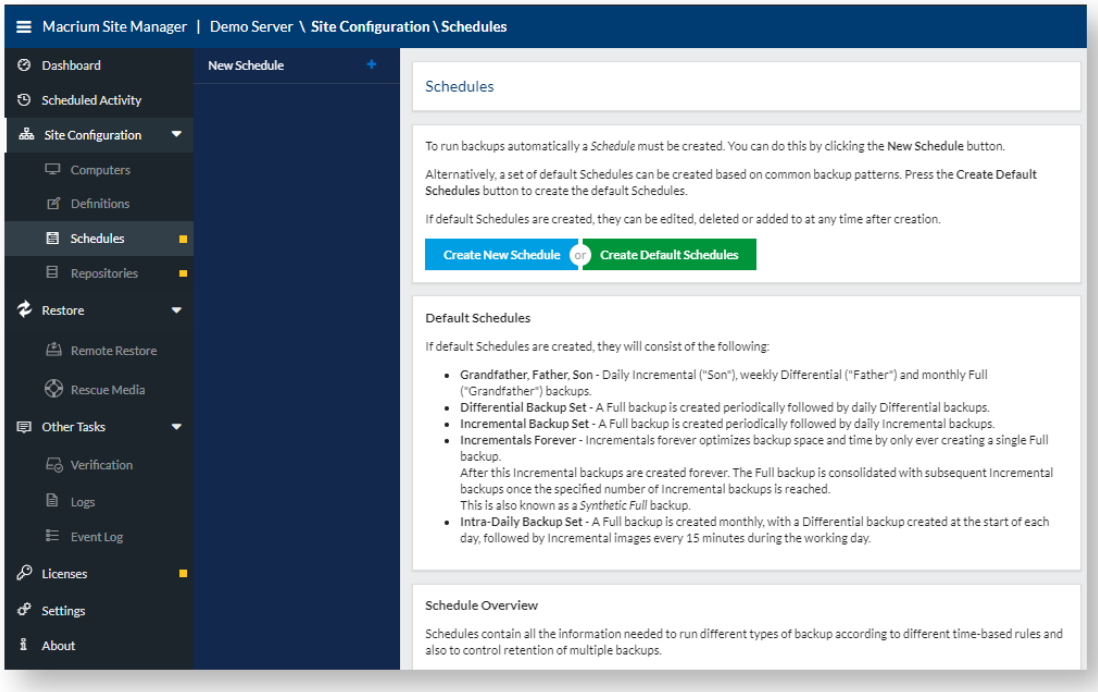
A **Schedule** contains information on when backups are to be performed and how long each backup is to be kept. The data in a Schedule includes:

- Triggers which define when backups should be taken and what type of backup (Full, Differential, Incremental)
- Retention rules describing how long or how many backups should be kept before old backups are removed.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

- Options for advanced behaviors of how retention rules should be applied

To work with Schedules, visit the Schedules page of the Management Console by clicking the '**Schedules**' link under the '**Setup**' heading. On the initial visit to the Schedules page, or if all Schedules are deleted, the page will show some general help and information on Schedules:



Default Schedules

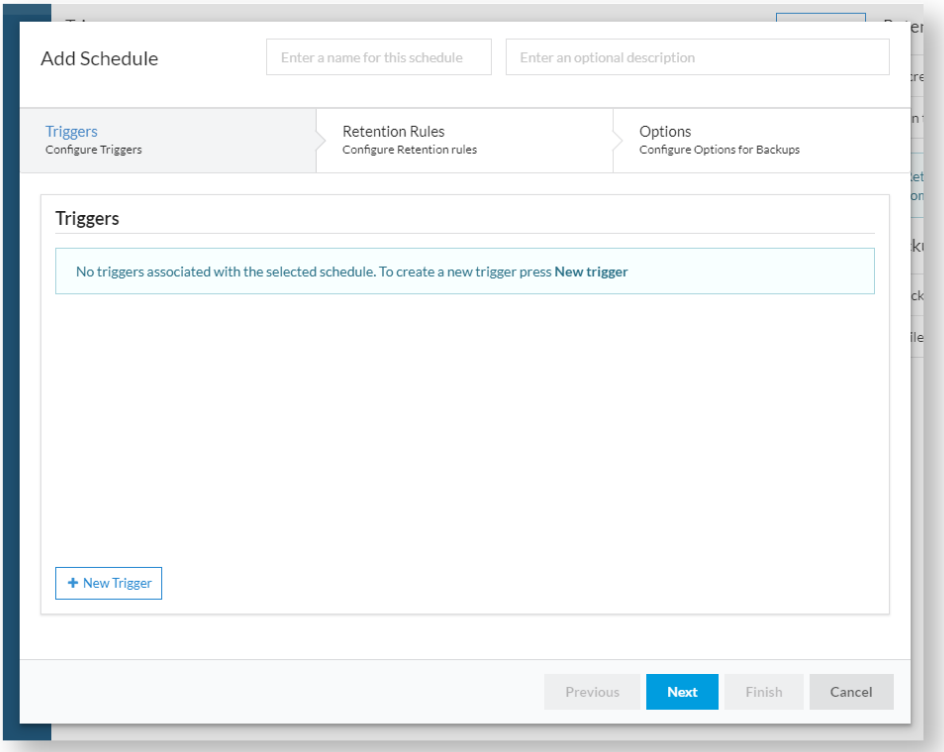
On the initial guidance page for Schedules, there is an option to create a set of default Schedules. These defaults can be edited and modified once created to provide the exact scheduling required. The defaults created are:

- **Grandfather, Father, Son** - Daily Incremental ("Son"), weekly Differential ("Father"), and monthly Full ("Grandfather") backups.
- **Differential Backup Set** - A Full backup is created periodically followed by daily Differential backups.
- **Incremental Backup Set** - A Full backup is created periodically followed by daily Incremental backups.
- **Incrementals Forever** - Incrementals forever optimizes backup space and time by only ever creating a single Full backup.
  After this Incremental backups are created ad infinitum. The Full backup is consolidated with subsequent Incremental backups once the specified number of Incremental backups is reached.
  This is also known as a Synthetic Full backup.
- **Intra-Daily Backup Set** - Monthly Full backups, daily Differential backups and Incremental backups every 15 minutes during working hours. Differentials are retained for 4 weeks., Full images for 6 months.

Creating a Schedule

To create a new Schedule, click the '**New Schedule**' button in the upper left of the interface. This opens the Schedule creation wizard:

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

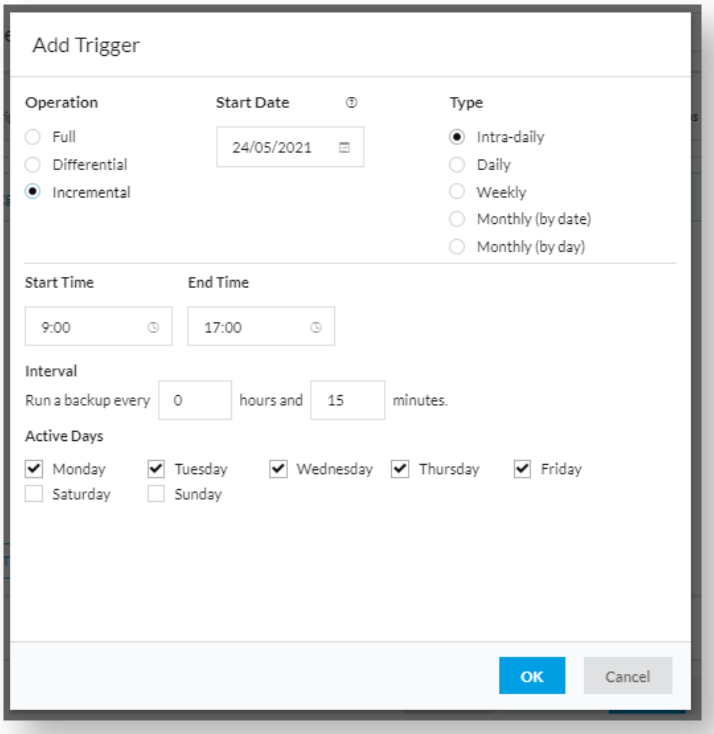


Each Schedule must have a name set in the box at the top. An additional description may be included.

Step 1 - Triggers

The first stage of the wizard is to define the triggers for when backups are to be run. To create a new trigger, press the '**New Trigger**' button. This opens a dialog box as seen below:

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



The Add Trigger dialog has a number of options for creating the trigger. These are:

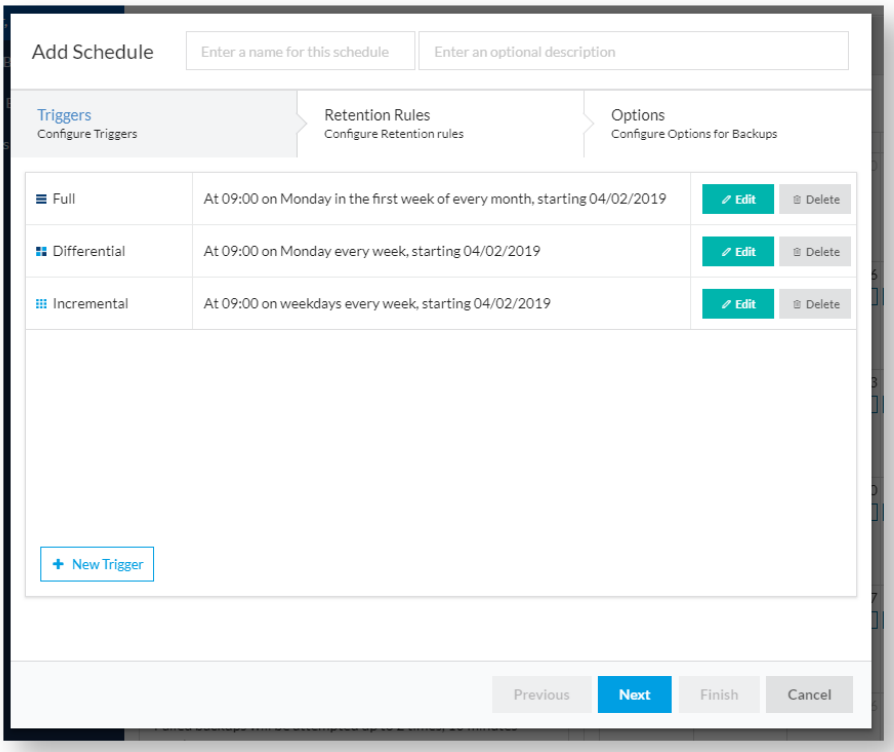
Option	Description
Operation	Which type of backup to perform when this trigger initiates a backup. May be Full, Differential or Incremental. If a trigger fires for an Incremental or Differential backup, but no Full backup exists in the repository to base the Differential or Incremental backup on, the backup is automatically converted to a Full backup.
Start Time	The time of day the backup operation will occur. If a backup is delayed because another backup is running, the backup will run as soon as able.
Start Date	The date when the trigger starts. The trigger will not initiate a backup before this date. This is useful to ensure that complex rules start at the right time. For example, making sure a trigger for an Incremental backup on Tuesdays doesn't occur before a Full backup trigger on Fridays.
Trigger Type	The type of trigger - the options are listed below in the 'Trigger Details' section.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Option	Description
	When triggers occur at the same time, only one backup is taken, with the more thorough backup taking precedence (Full over Differential, Differential over Incremental). For example: given a weekly Full backup trigger which occurs at 10:00 PM and a daily Incremental backup trigger at the same time, the Full backup will take precedence and run. This allows for simpler trigger creation - for example a weekly and daily trigger which overlap rather than two weekly triggers, one for one day and the other for all other days of the week.
Trigger Details	The panel changes depending on the trigger type. • **Intra-Daily** - backup every **n** minutes between the start and stop times. May be restricted to certain days of the week. • **Daily** - Interval (every **n**th day) • **Weekly** - Interval (every **n**th week) and Active Days (Monday, Weekends etc) • **Monthly (by Date)** - Active Days (the day number(s) in the month - 1st to 31st) and Active Months (which months of the year the trigger is active during) • **Monthly (by Day)** - Week of the month (which week number, 1st to 4th or last the active days entry applies to), Active Days (the day(s) of the week the trigger will fire on) and Active Months (which months of the year the trigger is active during)

Once the trigger data is correct, press '**OK**' to save the trigger. The trigger will then be displayed in the trigger list:

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



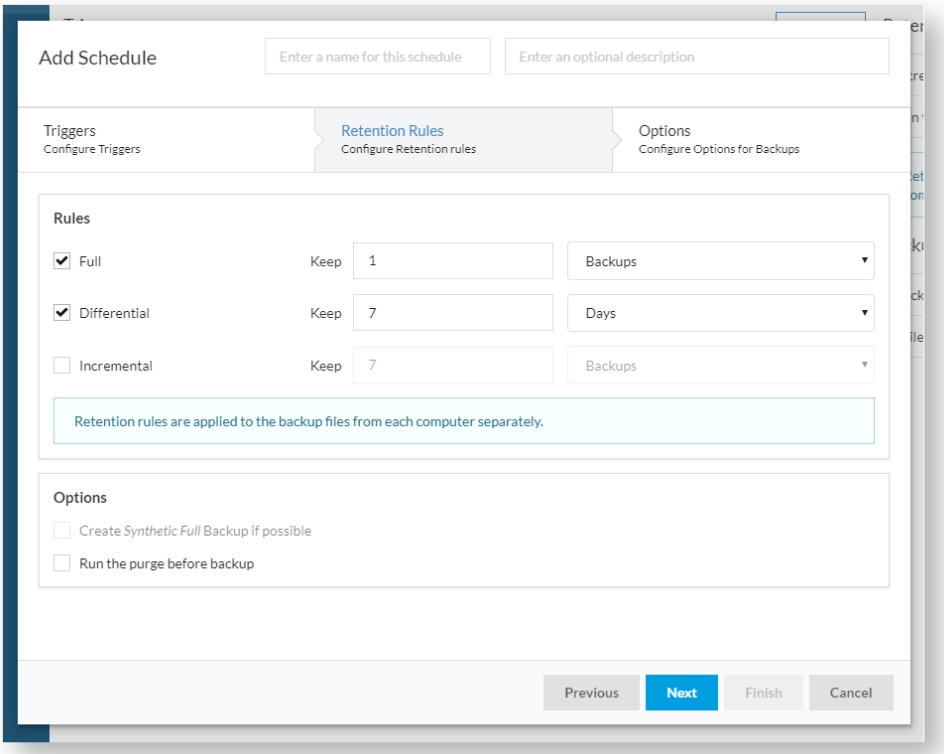
Each trigger listed has an '**Edit**' button to re-open the trigger creation dialog to edit the trigger and a '**Delete**' button to remove the trigger.

Once triggers have been created, press the '**Next**' button to continue to step 2. There must be at least one trigger to proceed.

Step 2 - Retention Rules

Retention rules govern how long backups are kept in the repository before being deleted to conserve space. The retention rules step appears as follows:

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



The '**Rules**' section contains the retention rules for each backup type. If the checkbox next to each rule is checked, if there are any backups older than the time period or count of backups specified in the dropdown boxes.

If the **Retention Rule** for a given backup type is unchecked, those backups are kept forever unless manually deleted from the repository.

Retention rules are applied on a per-computer basis. If a retention rule is configured to keep 10 Full backups, the rule will keep 10 Full backups per computer in the backup plan.

The '**Options**' section contains options for additional and fine control over the way retention rules are applied. Options available are:

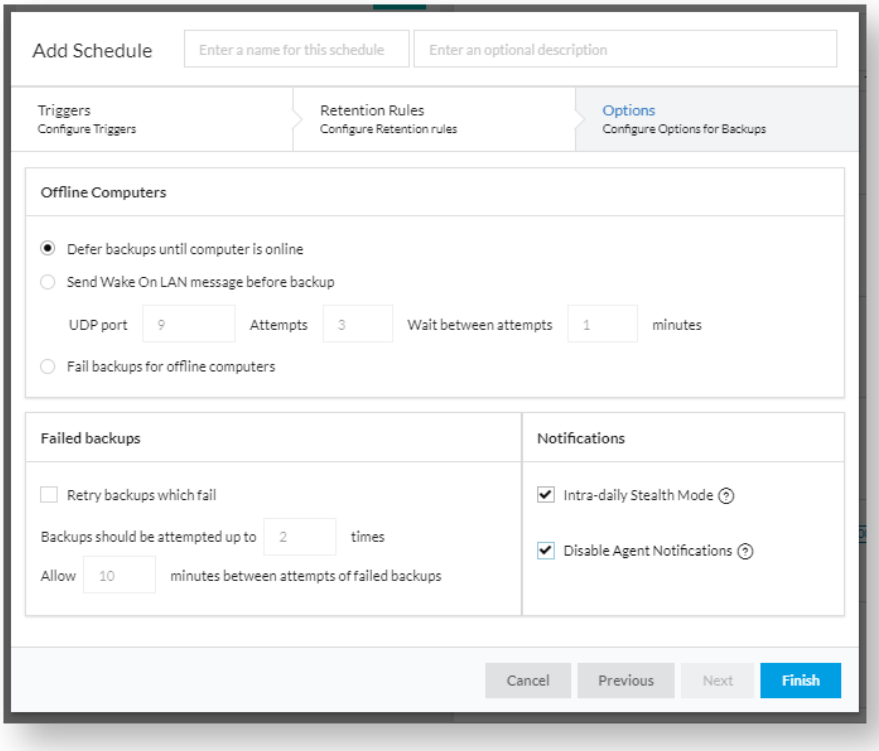
Option	Description
Create a Synthetic Full Backup if possible	If this options is checked, Instead of deleting Incremental backup files once they have reached the limit of retention, they are merged into the Full backup they are based on, creating a new Full backup containing all the data up to the merge point

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Option	Description
	This option only applies to backup plans such as 'Incrementals Forever' where a single Full backup is followed by frequent Incremental backups. The retention rule for Incremental backups must be enabled and set to 'Backups' mode for this option to become available.
Run the purge before backup	This option applies retention rules and deletes any files according to retention rules before the backup starts. This keeps repository space usage lower but may result in fewer retained backups when new backups fail

Step 3 - Options

Options control how backups are scheduled and what actions are taken on failure. The interface appears as below:



The available options are:

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

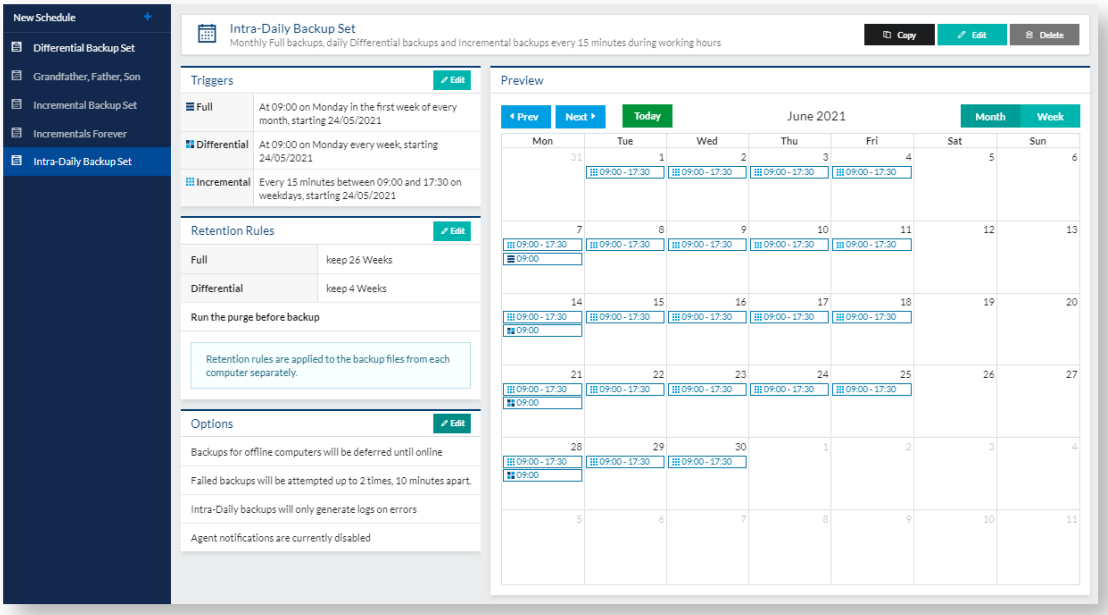
Option	Description
Defer backups until computer is online	If this option is selected, scheduled backups cannot be performed because a computer is offline will be performed when the computer comes back online. If the option is unchecked, scheduled backups will fail if the computer is offline
Send Wake On LAN message before backup	If this option is selected, Site Manager will attempt to use Wake On LAN to wake offline computers before starting a backup. If Wake On LAN attempts fail, it will behave as the "Fail backups for offline computers" option Additionally, UDP port, number of wake attempts and time between attempts can be set.
Fail backups for offline computers	If this option is selected, backups will be failed if the computer is offline and the computer will not perform a backup until the next trigger time or next retry time as set below.
Retry backups which fail	If a backup attempt fails, it can be retried up to the number of times specified here
Allow X minutes between attempts of failed backups	The time between each attempt which Site Manager will wait. May be set to between 2 and 120 minutes. Backups of other computers may occur between the retries.
Intra-daily Stealth Mode	When Intra-daily stealth mode is enabled, backups that are triggered by Intra-daily triggers will only create backup logs if there is an error or if new files/folders have been found (For File and Folder Backups). Instead of logs, the logs view will show a daily summary for each computer backed up
Disable Agent Notifications	When enabled, pop-ups are suppressed on the Agent computer, so that the backup is completely silent to a user of that computer. If the user has manually launched the monitor app on the Agent computer, they will receive notifications until log off.

Finalizing the Schedule

Once the options have been set appropriately, press '**Finish**' to save the Schedule.

Once the Schedule is saved, the Management Console will display the Schedule list with the newly created Schedule selected:

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



Editing and Deleting Schedules

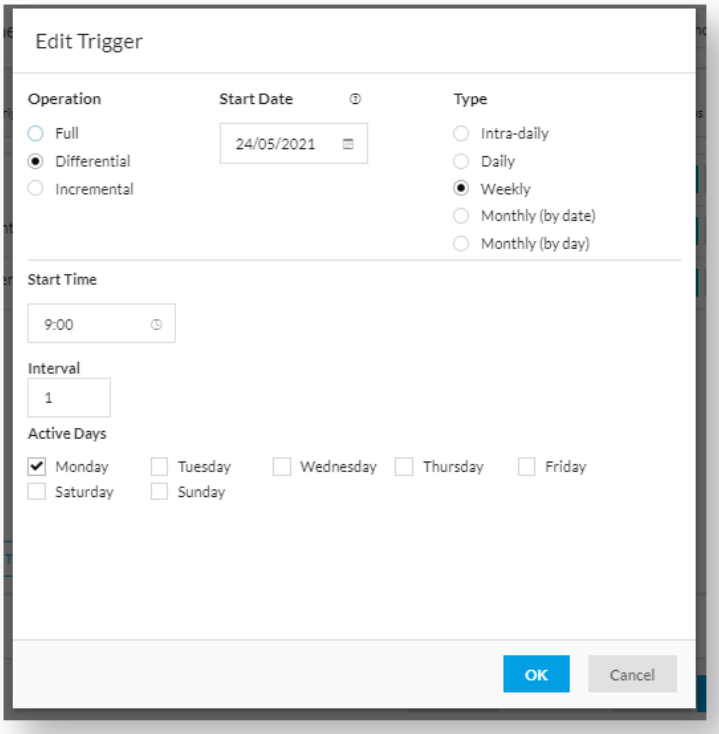
Once a Schedule has been created, it can be edited by selecting the '**Edit**' button in the top right. This will reopen the Schedule wizard and allow the Schedule to be edited. In addition, the retention rules panel has an edit button which can be pressed to open the Schedule for editing and jump to the retention rules section.

Deleting Schedules

Deleting a Schedule may fail if that Schedule is being used to schedule backups in a Repository. In this case, deleting the Schedule with require those scheduled backups to be removed or changed to use a different Schedule first.

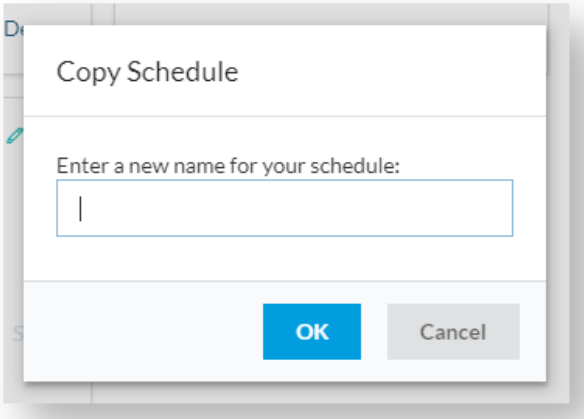
The triggers may be edited directly by using the pencil icon on each trigger's display in the view. They can also be deleted with the delete icon and new triggers can be created with the '**New Trigger**' button. Creating and editing triggers this way launches the dialog box for triggers and not the whole Schedule wizard:

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



Copying Schedules

An existing Schedule can be copied to a new Schedule to make creating Schedules which are almost the same simpler. Pressing the '**Copy**' button on the top right of the interface will prompt for a name for the copy of the selected Schedule.



Selecting OK will copy the Schedule.

Setup - Repositories

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

- Introduction
- Adding a Repository
  - Network Share Repository
  - Amazon AWS Storage Gateway
  - Azure Storage Account
  - Local Repository
  - Adding a new Repository - Final Steps
- Viewing Repository Information

Introduction

Repositories are required in order to use the central backup scheduling and queuing facilities in Site Manager. Once a repository has been set up, a Backup Definition can be configured to back up to the Repository according to a Schedule.

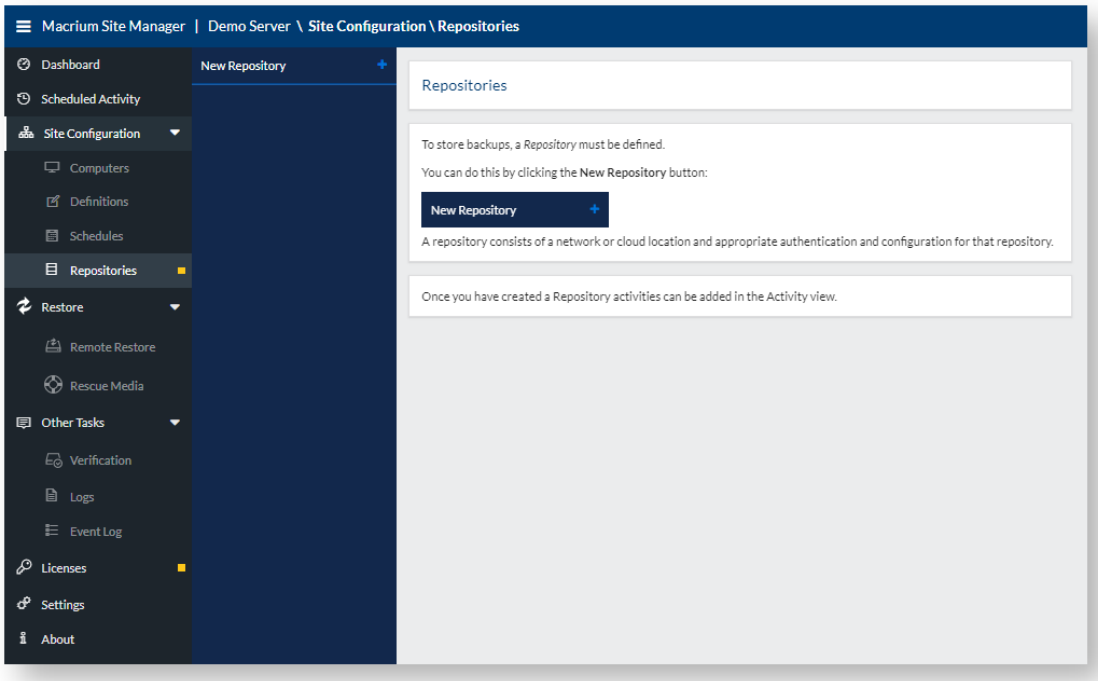
A repository is a storage location with a standardized folder layout and some tracking information. Each repository contains backup information such as, storage location, network access information, credentials required to access the resource and other basic storage management.

The following types of Repository backend are available:

- **Network Share** - Any Windows or SMB network share may be used as Repository storage
- **Amazon AWS Storage Gateway** - if an AWS Storage Gateway is available, it can be used as a Repository backend.
- **Azure Storage Account** - if Azure storage is exposed as an SMB share in Azure, it can be used as a Repository directly.
- **Local Repository** - Storage which is directly attached to a managed computer can be used as a Repository

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

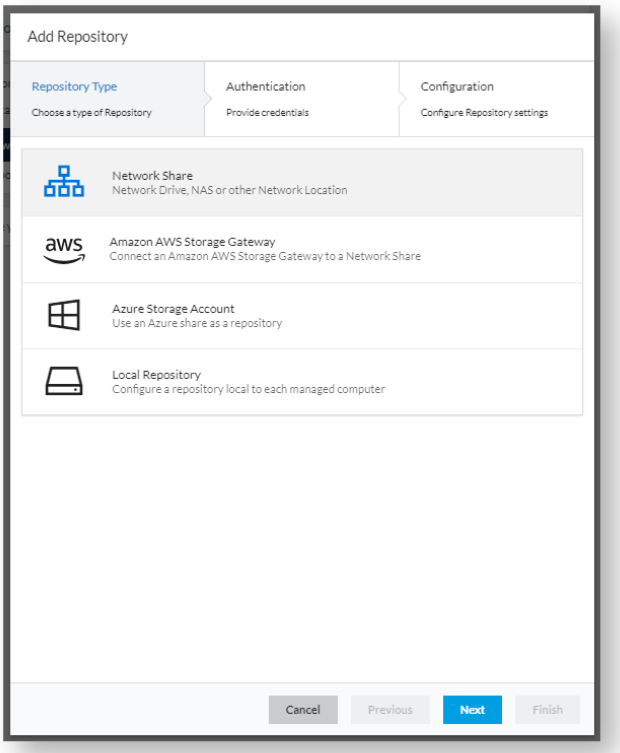
Adding a Repository



Repositories are managed by selecting the '**Repositories**' link from the main interface under the **'Setup'** main category. Initially the **Repository** interface will have no saved repositories and show some quick help notes.

To create a new Repository, click the '**New Repository**' link in the upper left, as seen in the image above. This will display the 'Add Repository' wizard shown below:

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



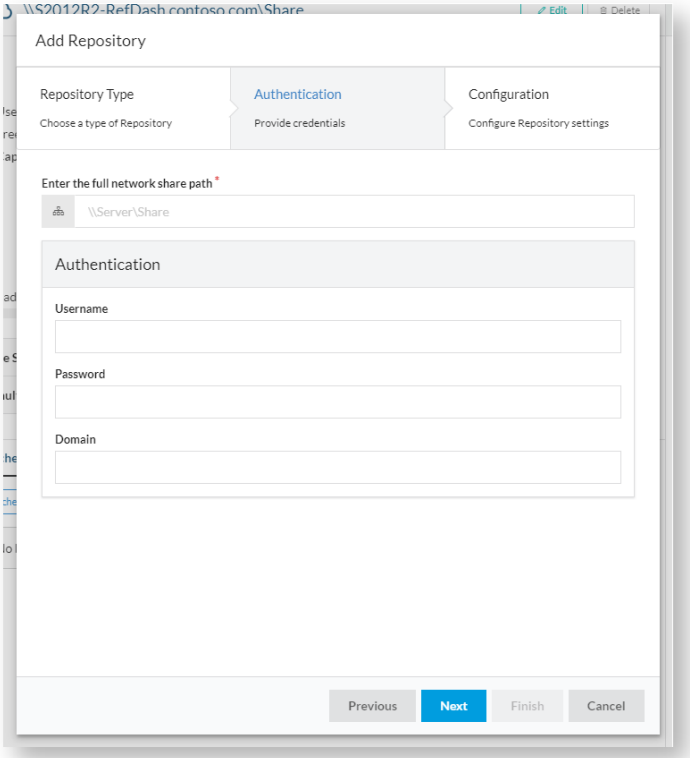
The initial repository wizard page allows the type of Repository to be selected. Once the appropriate type has been selected, click '**Next**' to move to the next step.

Depending on the Repository type chosen, the next stage will be different. See the appropriate section for details.

Network Share Repository

For a **Network Share** type repository, the next stage of the wizard is shown below:

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



This stage of the wizard allows you to configure the network path and access credentials for the Repository. The available options are as follows:

Option	Description
Path	This option will let you select the path to the network share in Windows UNC format. Example: \\SERVERNAME\Share
Authentication	Here you will input the authentication credentials that are needed to access the repository. The user requires to have **Read and Write** access to the repository so that the backup may be created and retention rules can be applied. **If the field is left blank anonymous access will be used.** When performing a backup, this authentication information is transmitted to Agent computers so that they can directly access the share. To avoid problems at the client end, it is recommended that the Domain part of the authentication is always filled in. If the share is on a computer or NAS which is not joined to a domain, the host name of the computer or NAS should be used instead.

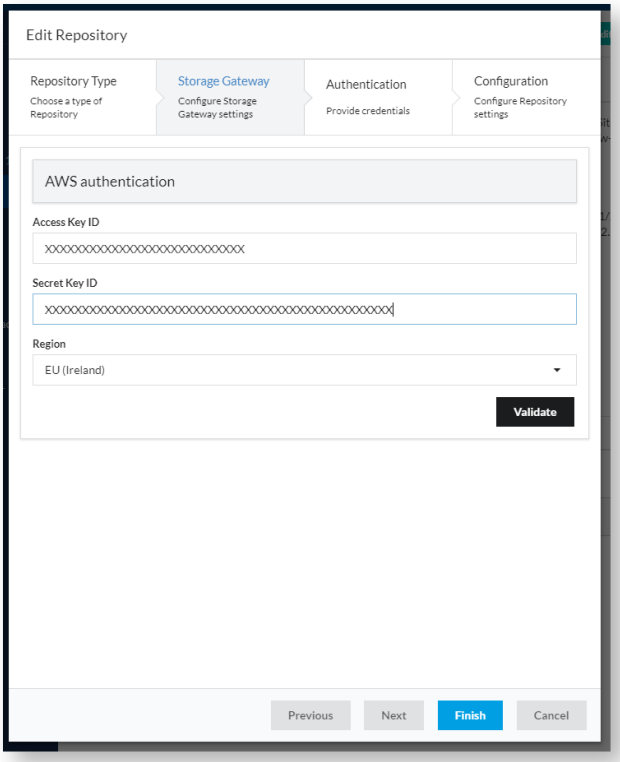
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Option	Description
	The Site Manager server will resolve IP addresses for the share and send these IP addresses to the Agent when backing up. This allows computers which cannot resolve the SMB server name to an IP address to connect and perform backups

Once this step has been completed, the next step is the final configuration page, described here.

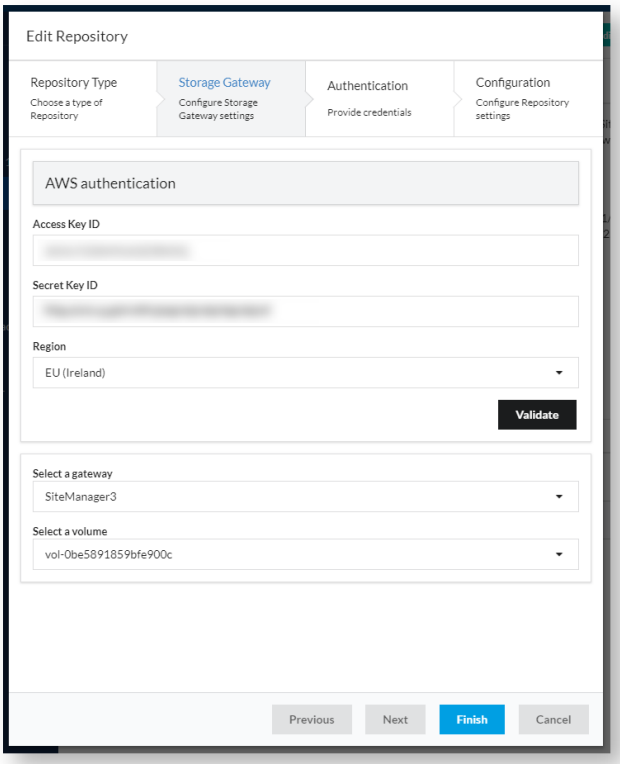
Amazon AWS Storage Gateway

See Configuring AWS Storage Gateway for information on configuring an on-premises gateway to the Amazon cloud. Once setup, the next stage is add the AWS Storage Gateway settings. After adding a new repository and selecting Amazon AWS Storage Gateway, the following wizard page is shown:

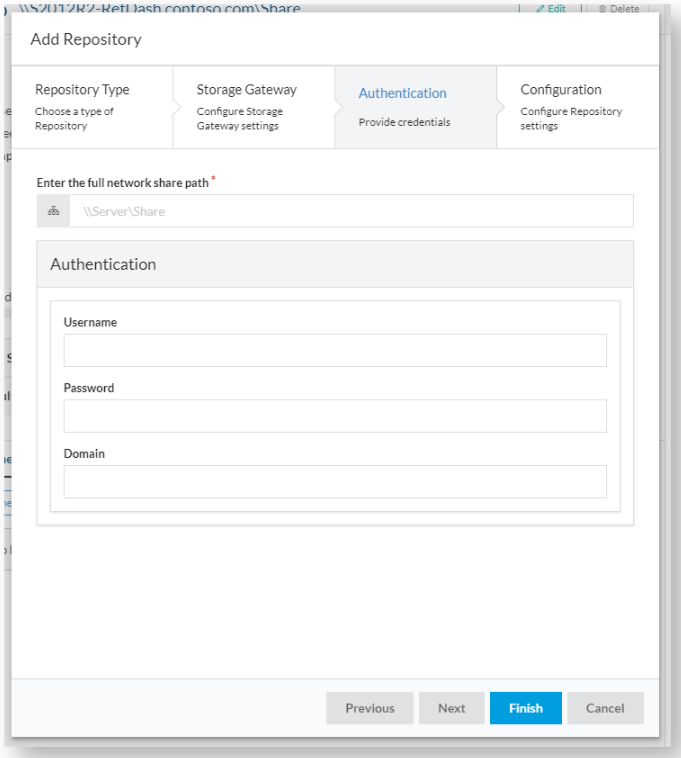


Once the Access Key ID and Secret Key ID of the Storage Gateway have been entered, press **Validate** to get a list of gateway names and volumes to select.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



Once the correct gateway name and volume have been selected, press next to move to the next step, configuring the local share and authentication options.



Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

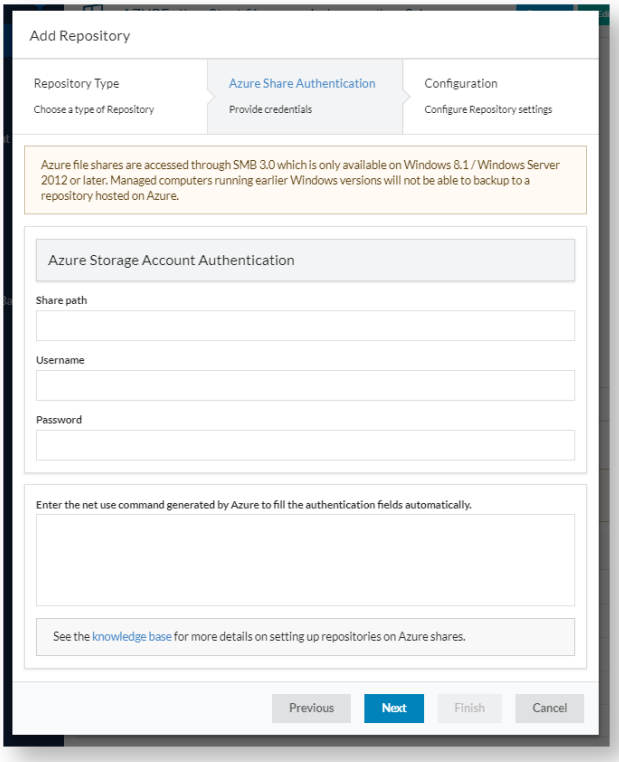
This stage of the wizard allows you to configure the network path and access credentials for the Repository. The share entered must be mapped to the AWS Storage Gateway volume selected. The available options are as follows:

Option	Description
Path	This option will let you select the path to the network share in Windows UNC format. Example: \\SERVERNAME\Share
Authentication	Here you will input the authentication credentials that are needed to access the repository.

Once this step has been completed, the next step is the final configuration page, described here.

Azure Storage Account

This repository type connects to an Azure storage account which has been configured to be accessible over the SMB protocol.



Detailing information on configuring Azure to enable share access is available here - Backup to the cloud with Azure File Shares

Azure Repository Limitations

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Azure shares use the SMB version 3.0 protocol. This requires that the computer accessing the share is running a version of Windows which supports this on both the Site Manager server and each managed computer which backs up to the Repository. Versions of Windows which support SMB 3.0 are:

- Windows 8 or later
- Windows Server 2012 or later

The wizard page has fields for the **share path**, **username** and **password** of the Azure share. These can be filled in directly, or the **net use** command generated by the Azure portal can be pasted directly into the box below to extract the share information and automatically fill in the other fields.

Once this step has been completed, the next step is the final configuration page, described here.

Local Repository

A local repository is a path which is evaluated on each individual managed computer such as a Windows file path.

This allows scenarios where some computers may be backed up to locally attached storage (USB drives, iSCSI, Windows Shares which are not visible to the Site Manager server etc) but still centrally managed.

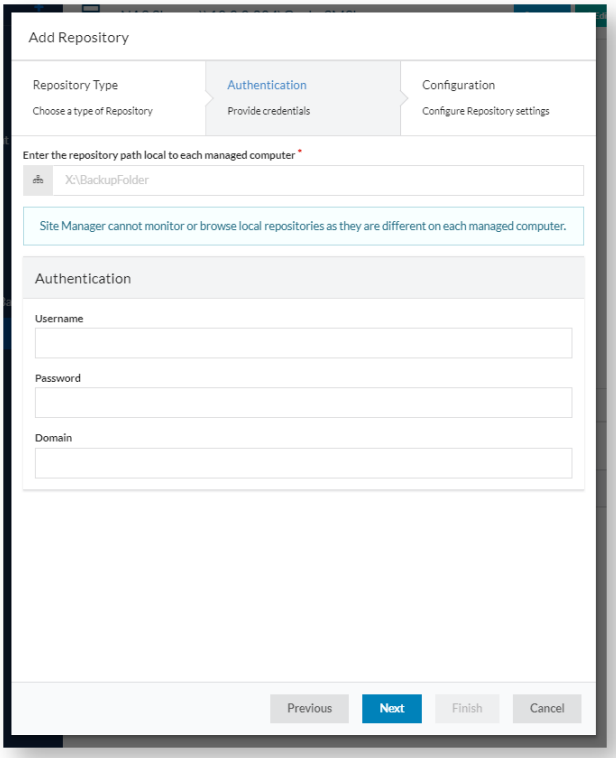
⚠ Local Repository Limitations

Because each computer evaluates the Local Repository path separately, the Site Manager server cannot provide most management features for a Local Repository.

This includes browsing, image verification, free space and status monitoring, Site Manager initiated restore and remote synchronization.

Repository browsing and restore should be done from the managed computer

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



The Local Repository configuration consists of a path to be evaluated on the managed computer - e.g. **X:** which will backup to the local X: drive on each computer, not the Site Manager server's X: drive.

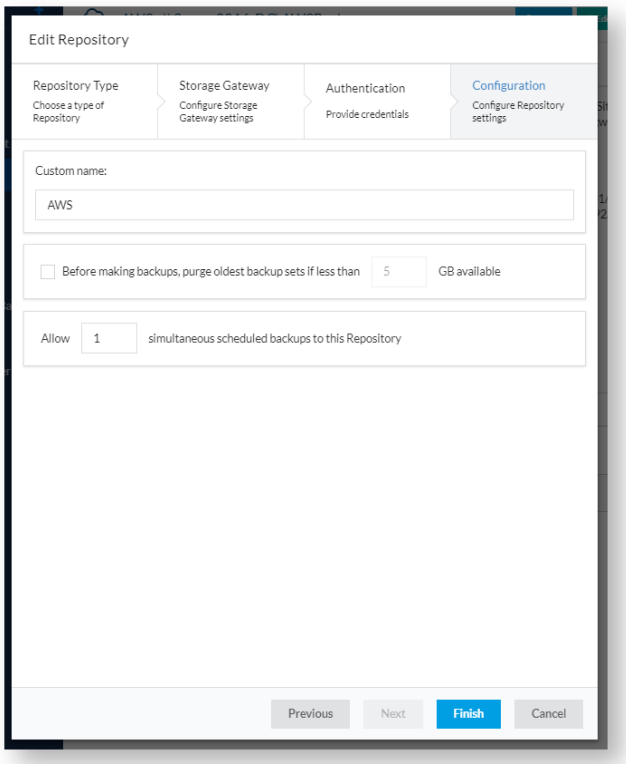
Optionally authentication information can be entered. This will be used for paths which require authentication such as Windows share paths.

Once this step has been completed, the next step is the final configuration page, described here.

Adding a new Repository - Final Steps

This page contains configuration options for how the Repository will be used by the scheduled backup system. This step is the same for all Repository types.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



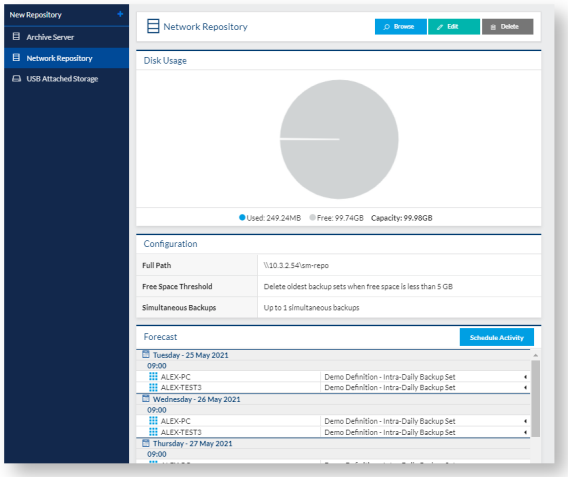
The available options are:

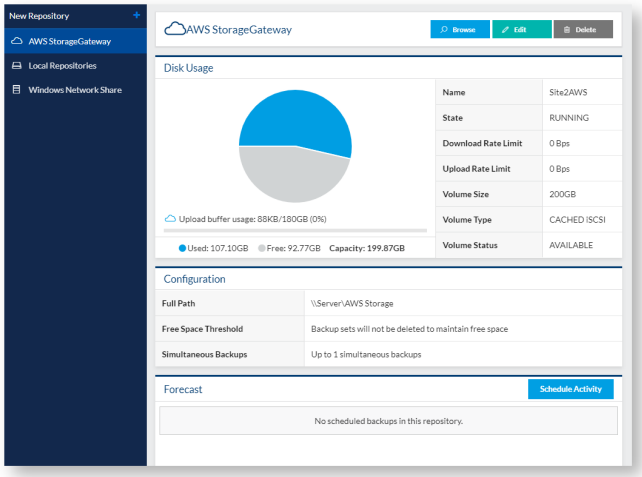
Option	Description
Custom Name	A name which will be displayed in the Site Manager interface for this repository. If left blank, it will default to the network path of the repository
Purge oldest backup set(s)	An optional value that will delete your old backups once the free space has reached a defined threshold. ⓘ This setting is independent of any retention rules configured in Backup Definitions and applies to all activity to this repository.
Simultaneous Scheduled Backups	This value sets the number of backups which can be performed to the repository simultaneously. The default value is 1, but it can be increased to a maximum of 10.

Once completed, the **Repository** can be saved by clicking the '**Finish**' button, which will return to the Repository list.

Once **Repositories** have been created, the interface shows the **Repository** list, as seen below

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.





For the **Amazon AWS Storage Gateway** Repository, the following additional data is available:

- Free space on the volume as a pie chart
- Upload buffer used/free
- Gateway information and statistics
- Volume information and statistics

Viewing Repository Information

The Repository view shows information on the Repository which has been selected in the list on the left-hand side of the screen. This information consists of:

- **Repository Status** - Disk space used and any specific information for the selected repository.
- **Forecast** - A forecast of upcoming activity configured on the Scheduled Activity page is shown.

Configuring AWS Storage Gateway

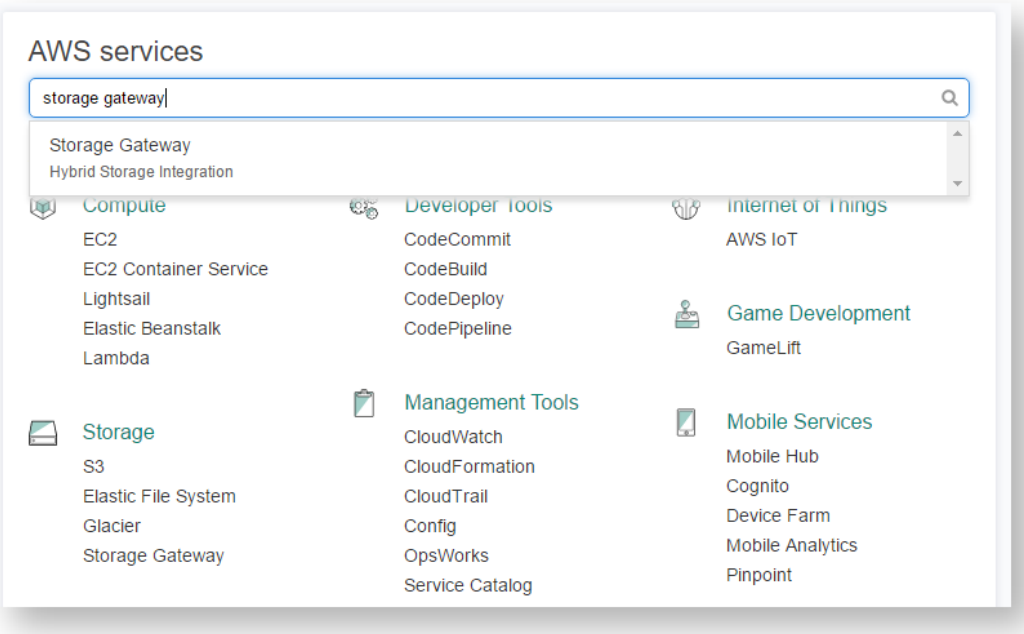
AWS Storage Gateway connects an on-premises software appliance with cloud-based storage. Macrium Site Manager can connect to a Volume Gateway via a iSCSI device mapped as a network share.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Creating Your Gateway

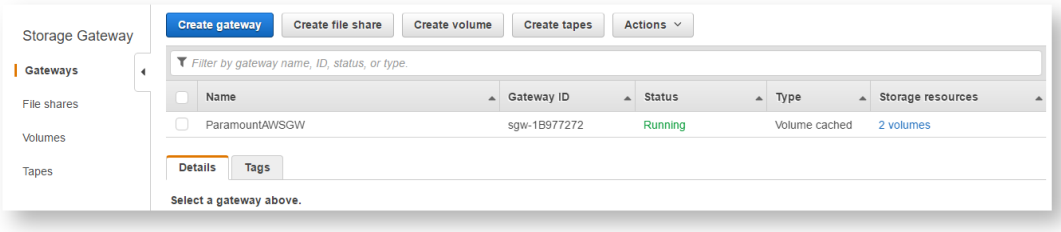
This section describes the steps to create a AWS Gateway that can be used as a Site Manager repository.

After logging on to AWS, you will need to access the AWS Storage Gateway dashboard:

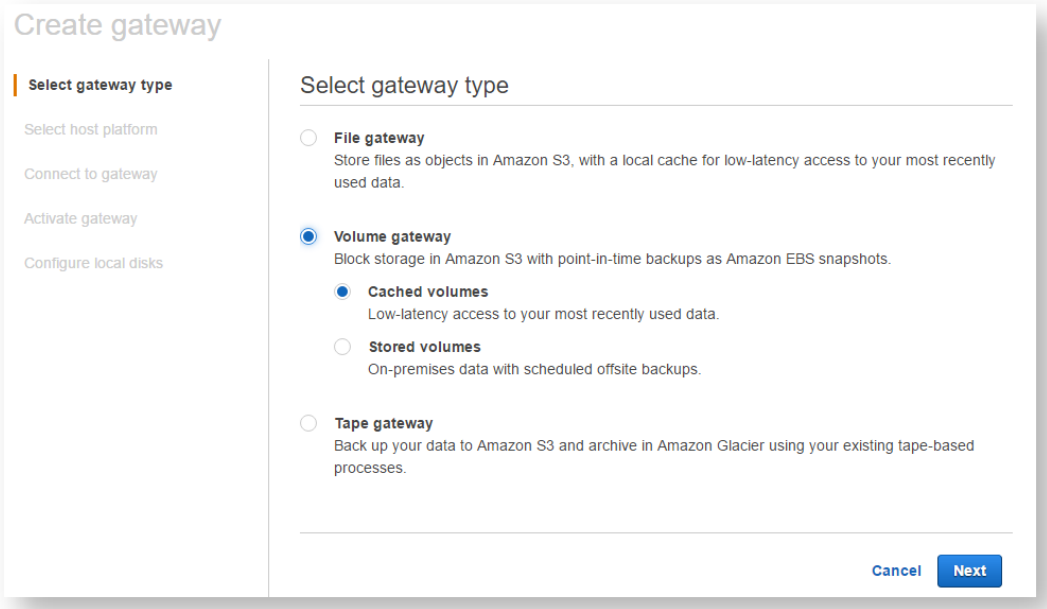


Click the "Create gateway" button to start the "Create gateway" wizard:

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

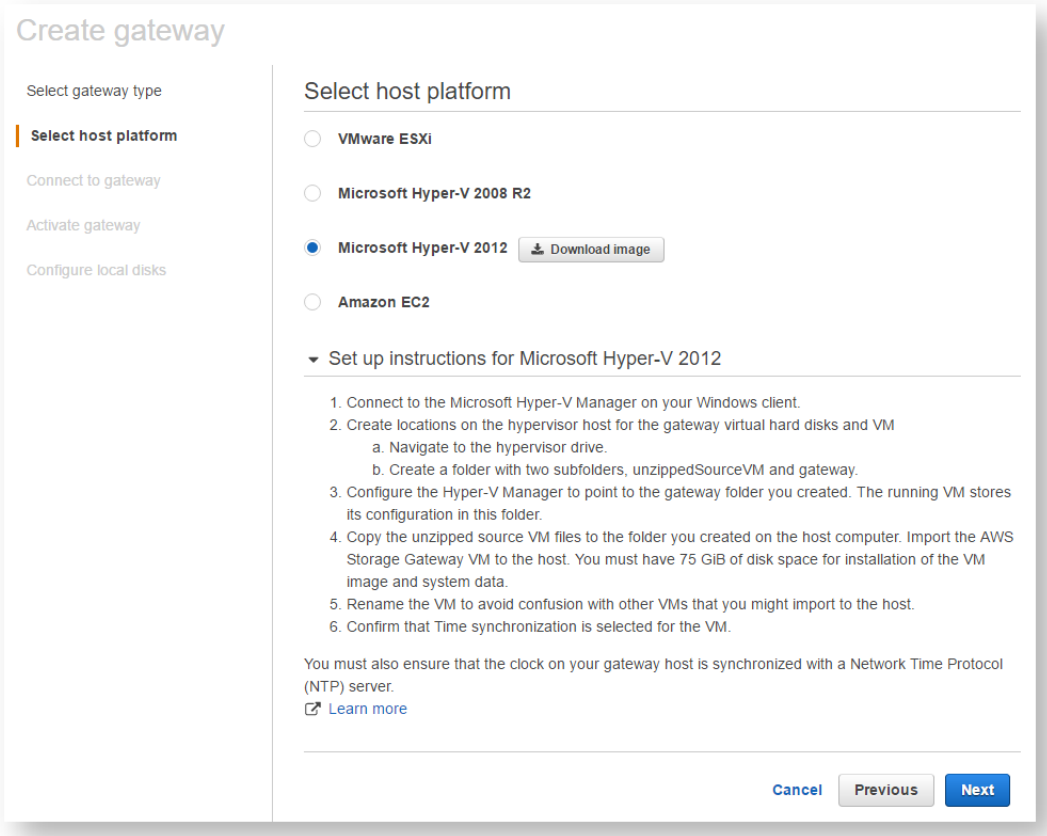


In this example we are creating a volume gateway with cached volumes:



Amazon provide a virtual machine that will host the gateway. This is downloaded and added to your VM provider. In this example we are using Microsoft Hyper-V 2012

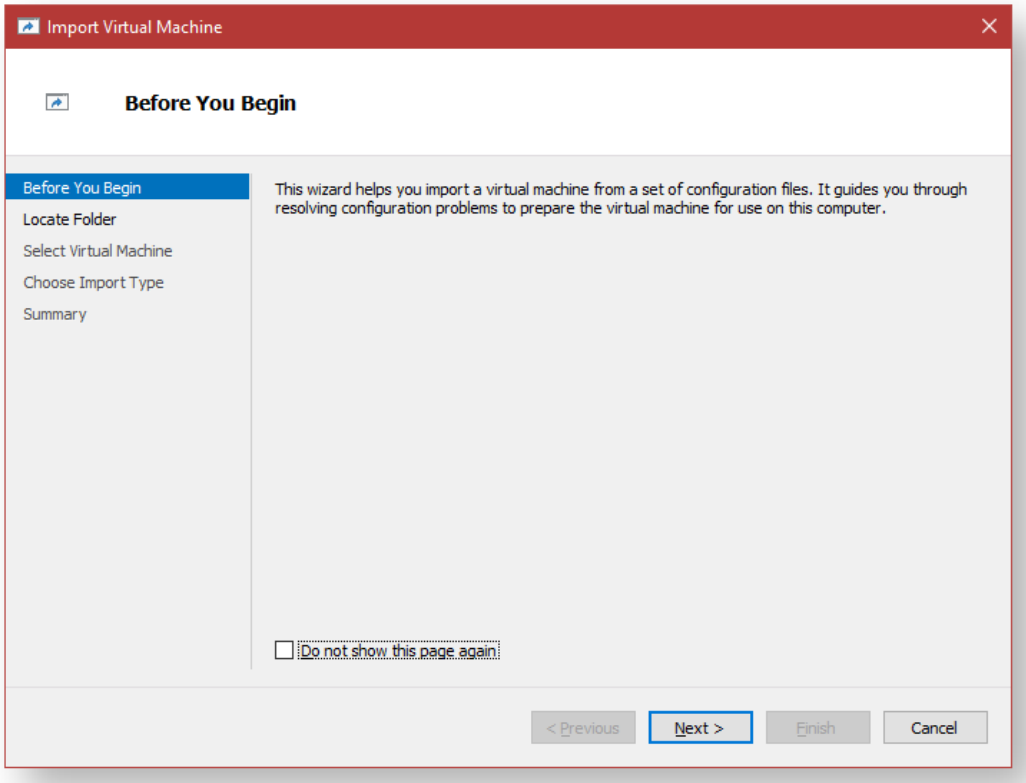
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



Configuring the Gateway VM

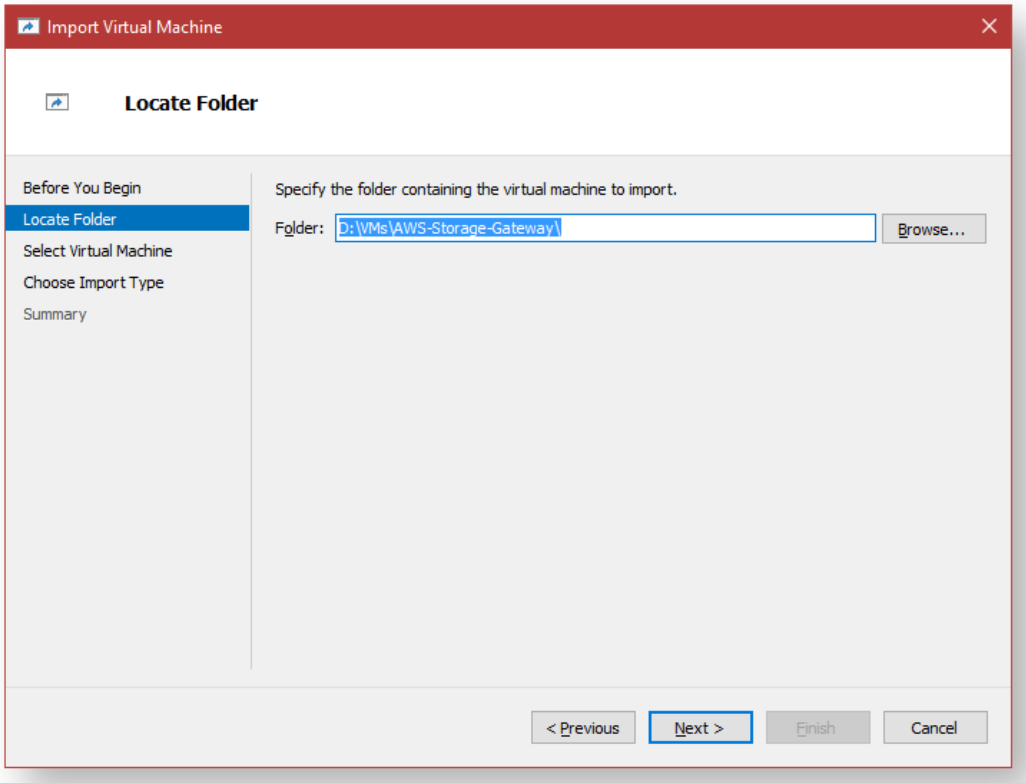
Once the VM image is downloaded, extract the contents of the zip file to disk and run the Hyper-V Manager to import the VM image.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



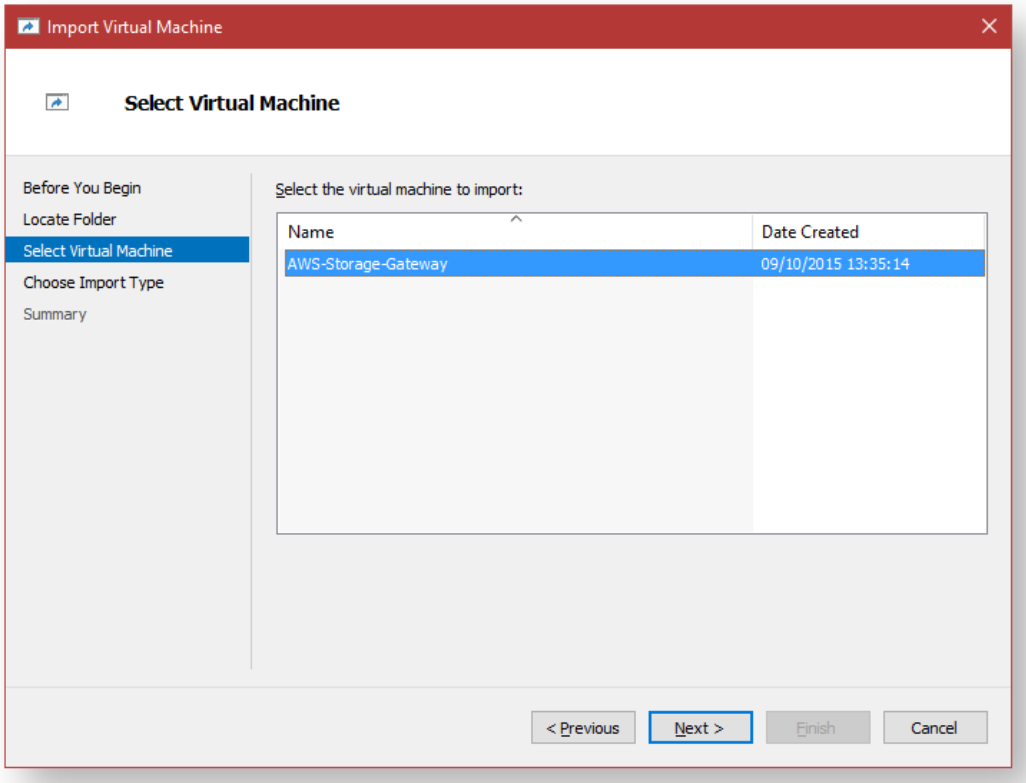
Specify the location where the zip file was extracted:

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



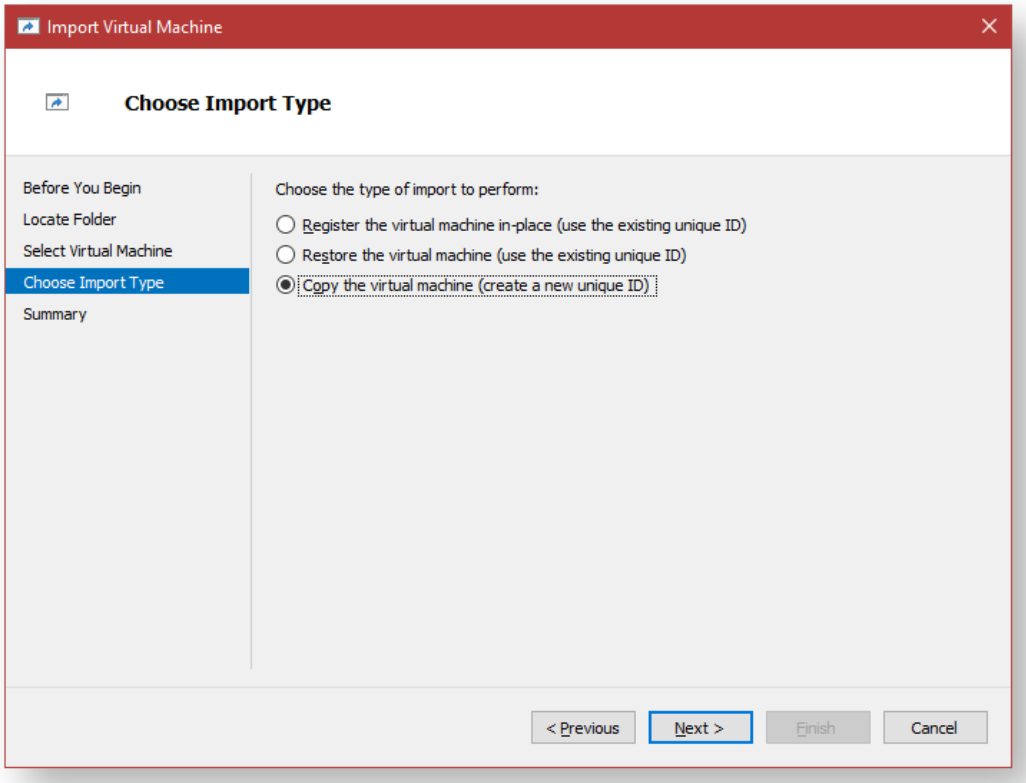
Select the "AWS-Storage-Gateway"

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



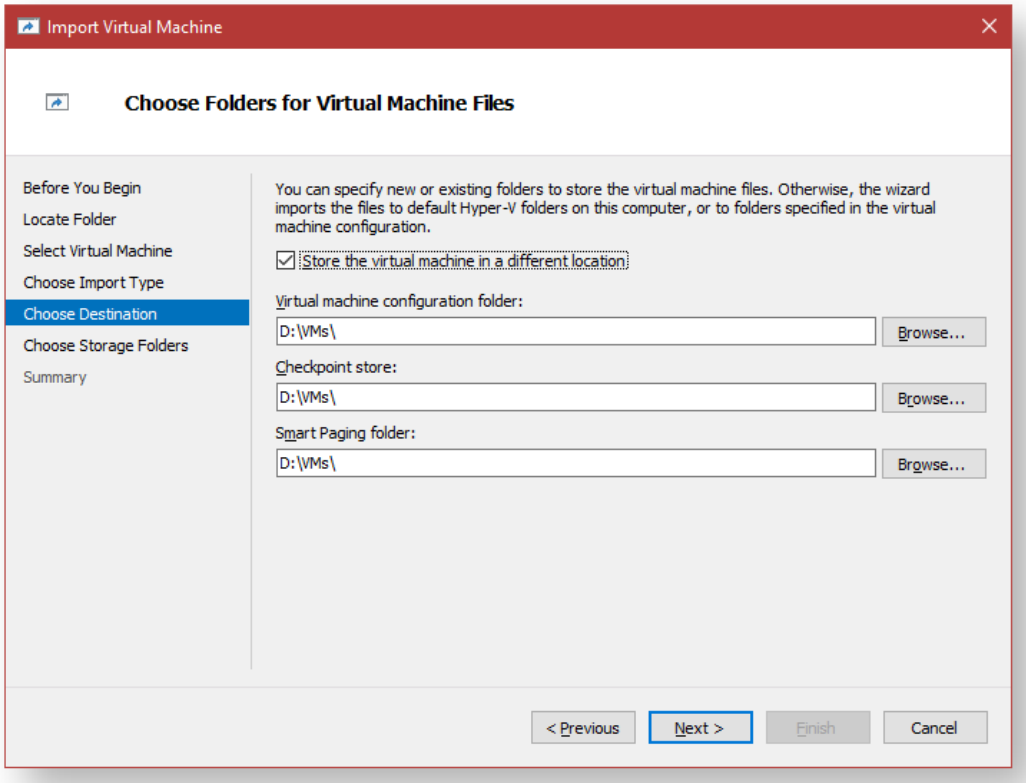
Create a copy of the VM to create a new unique ID for the VM

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



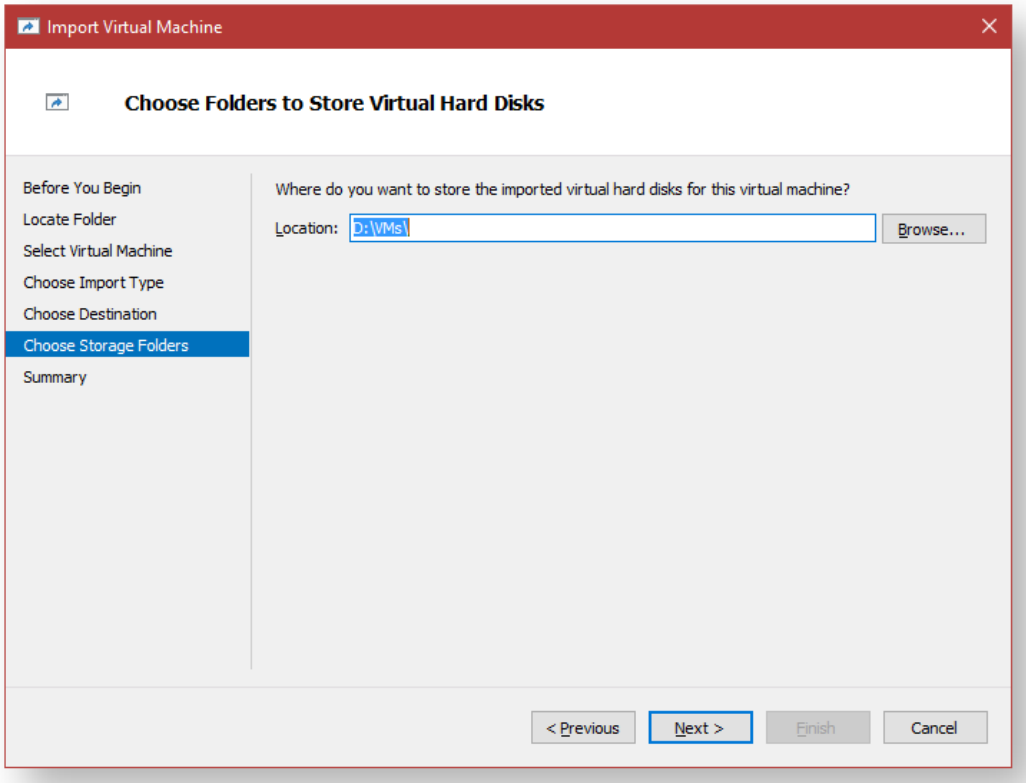
Specify the location where you want to save the VM

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



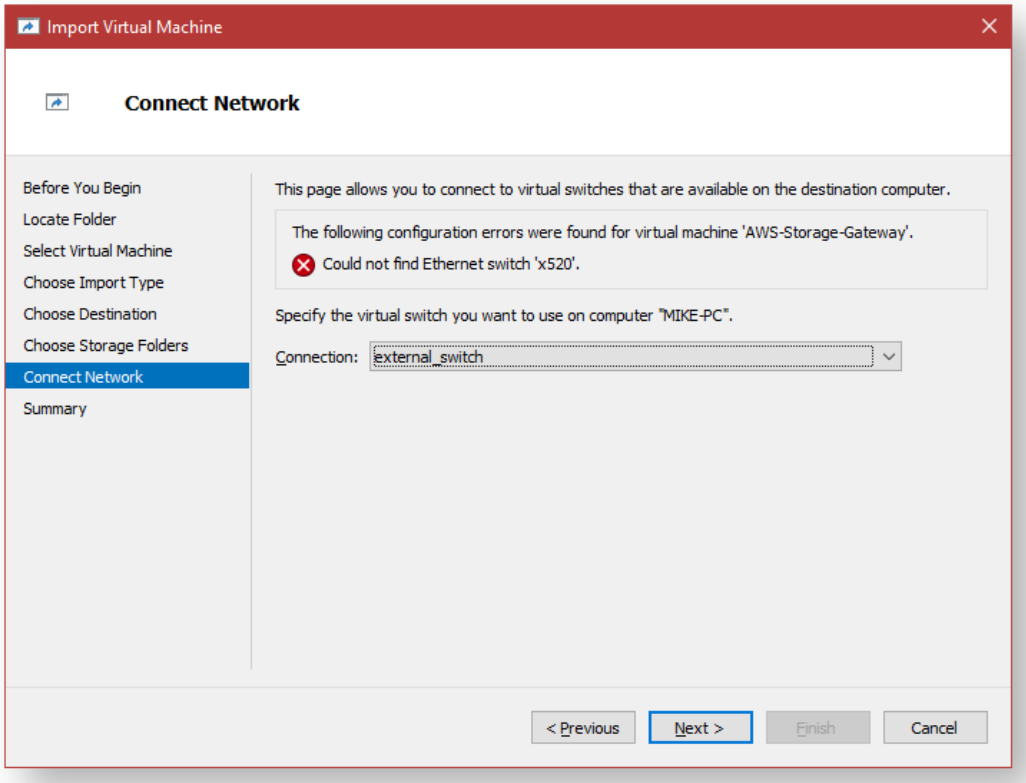
Specify the location where you want to save the VM hard disks

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



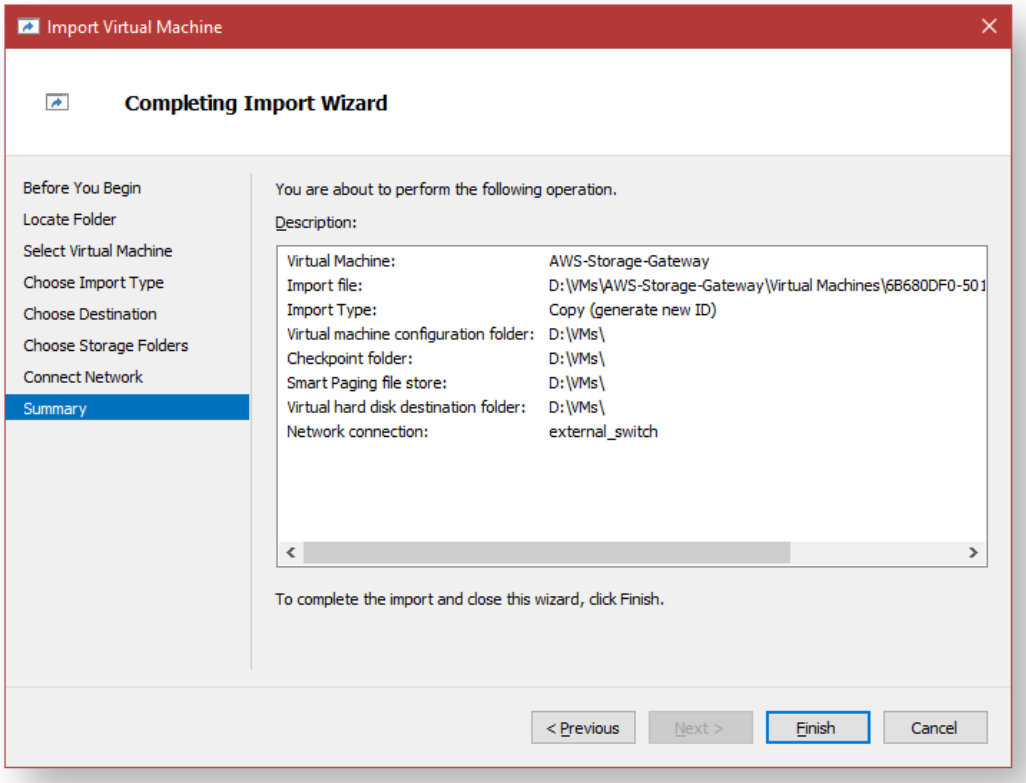
Ensure that you specify a network switch that is visible to the internet

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



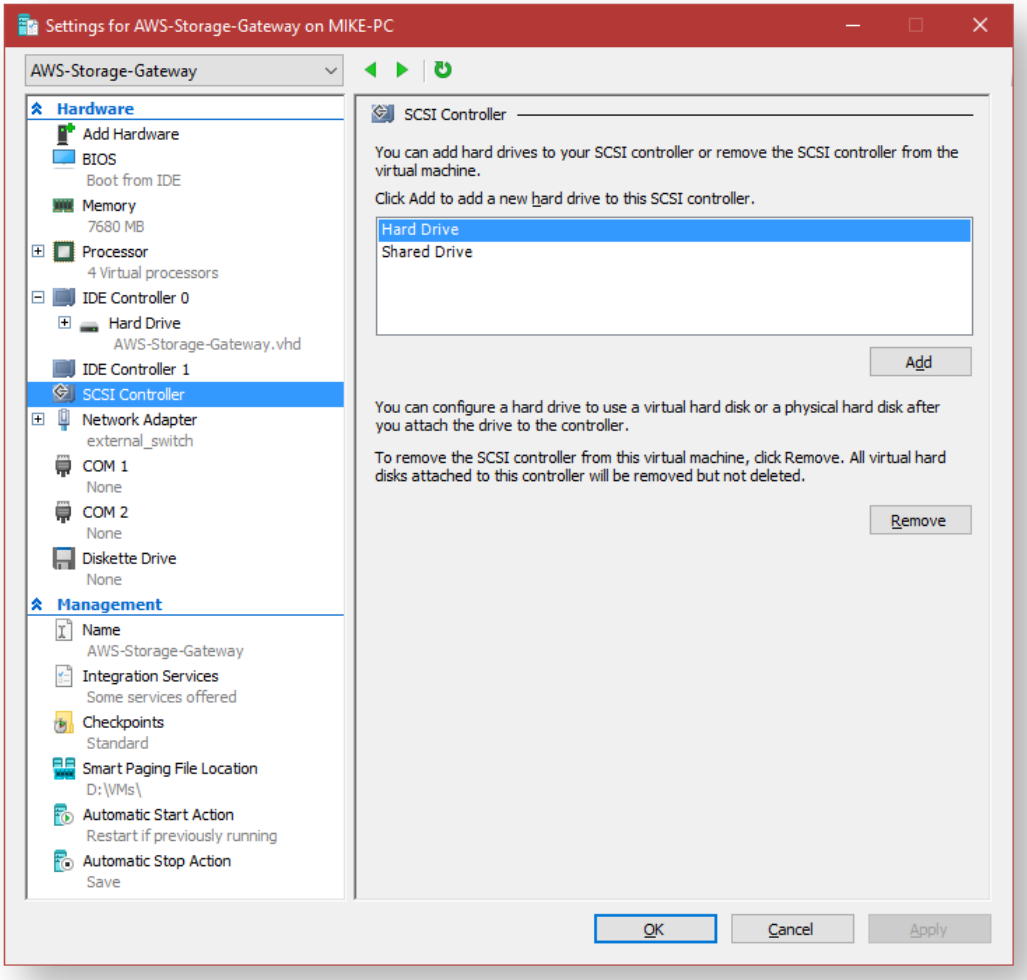
Click "Finish" to complete the VM creation process

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



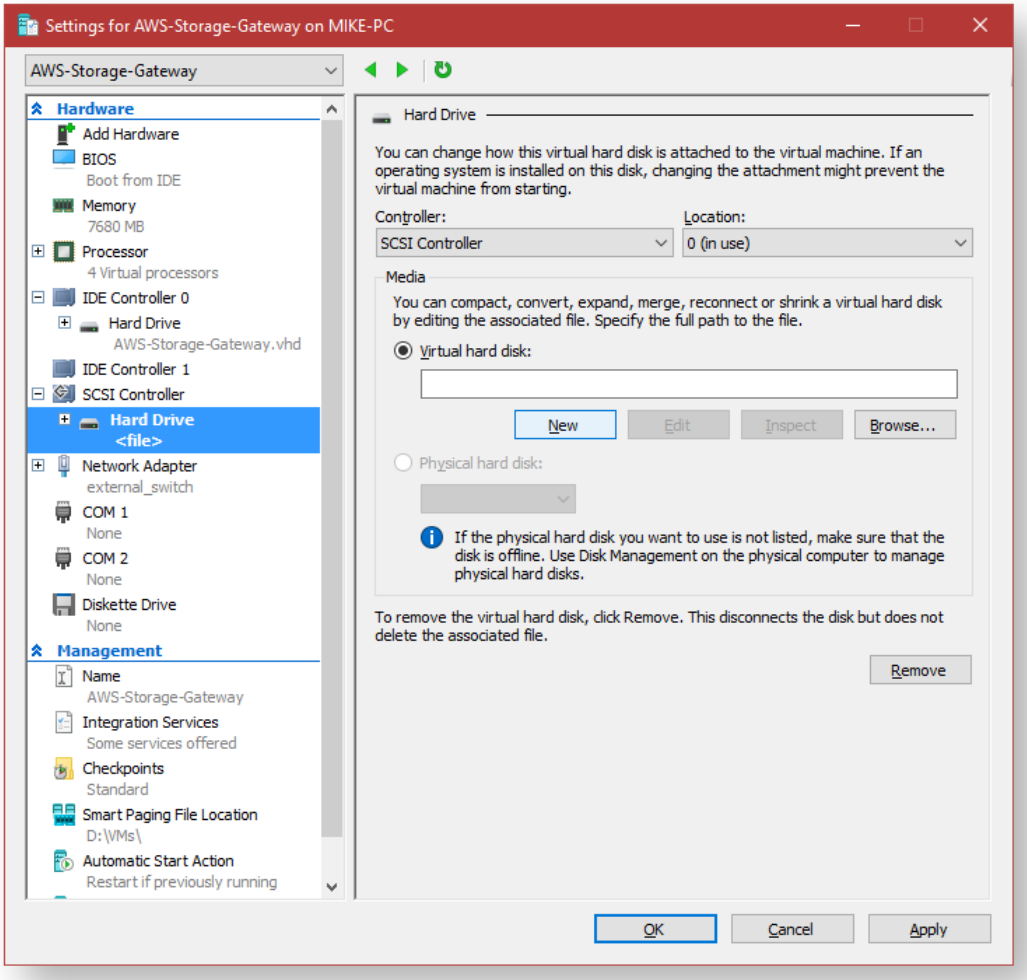
Once the VM is created two new virtual hard drives are required for the Volume Gateway. Edit the settings for the new VM and create two new hard drives.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



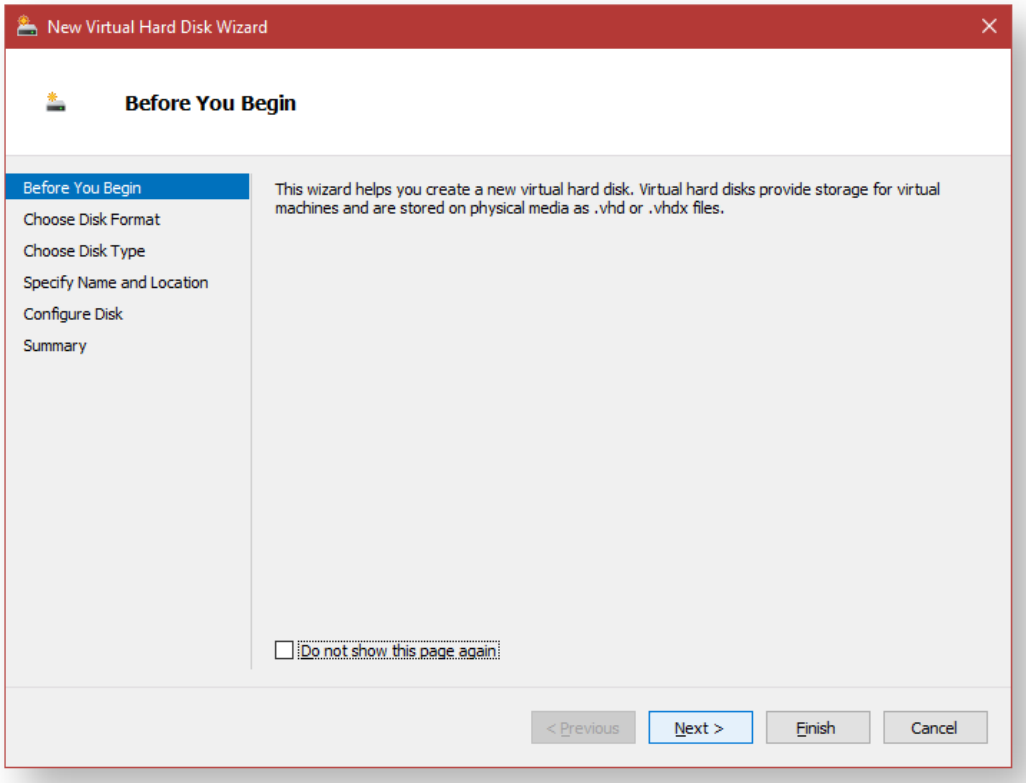
Create the hard drives on the SCSI Controller.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



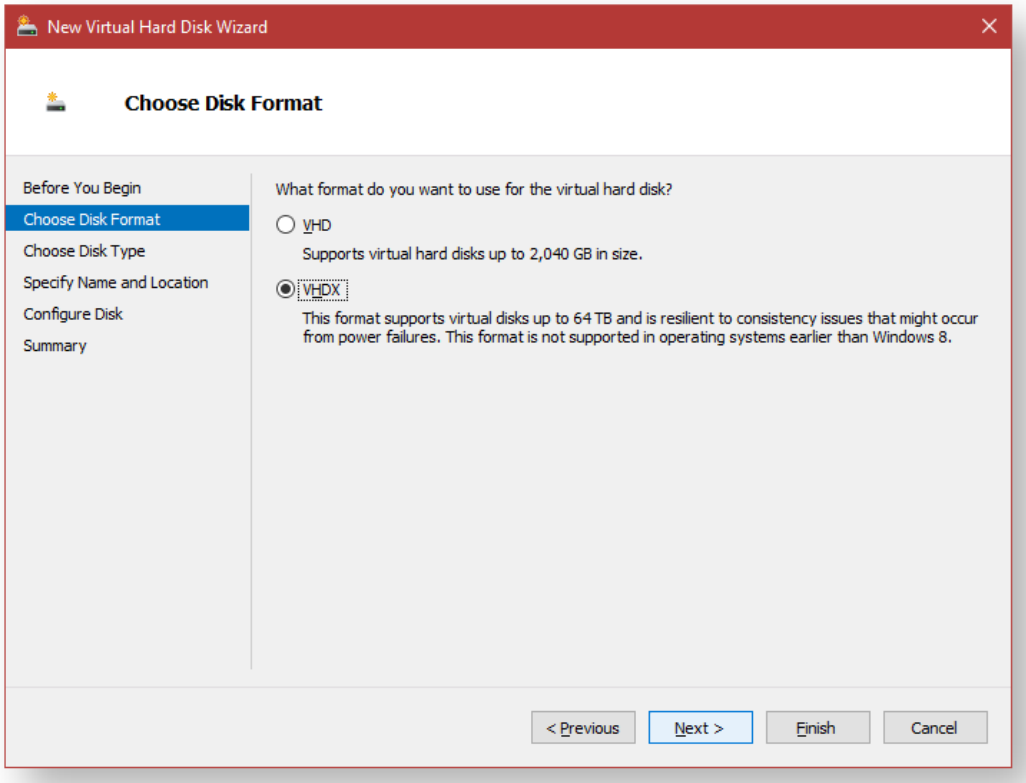
Click "Next" to continue.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



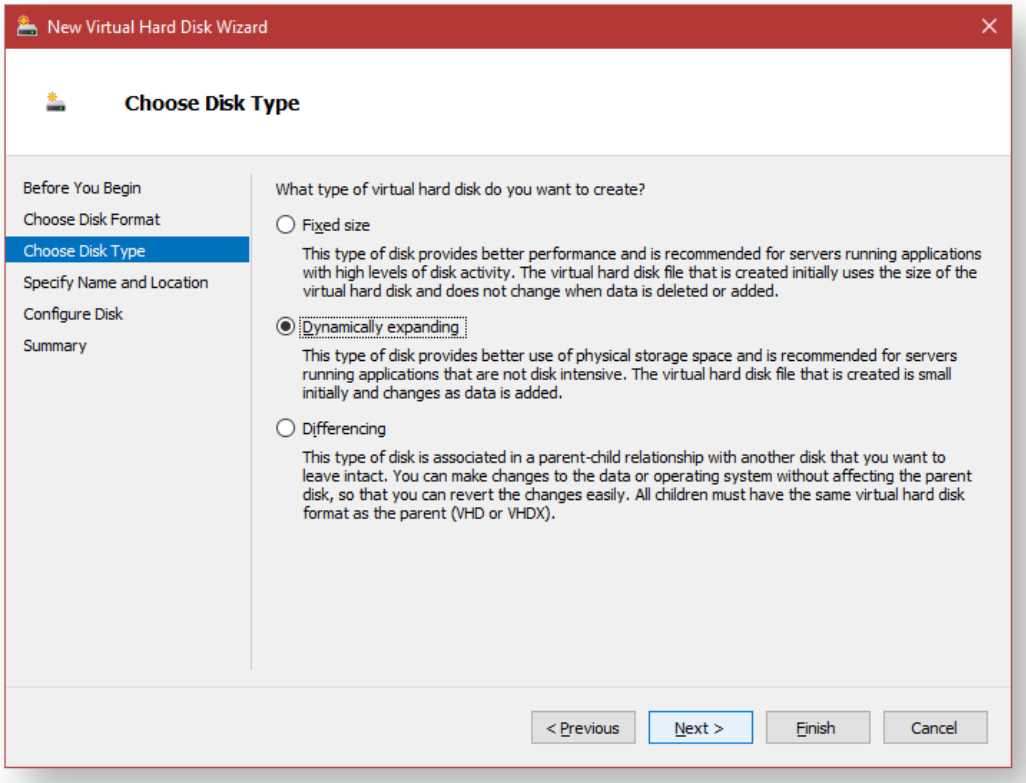
Specify the "VHDX" format for the disks.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



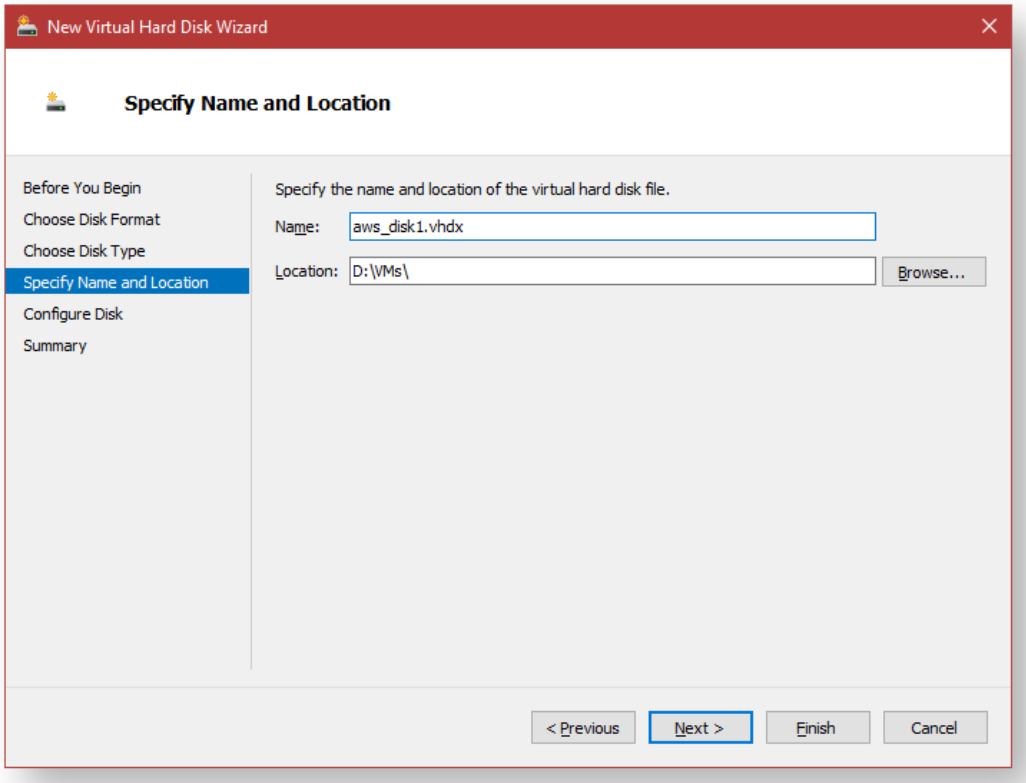
In this example the the disks will dynamically use physical disk space.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



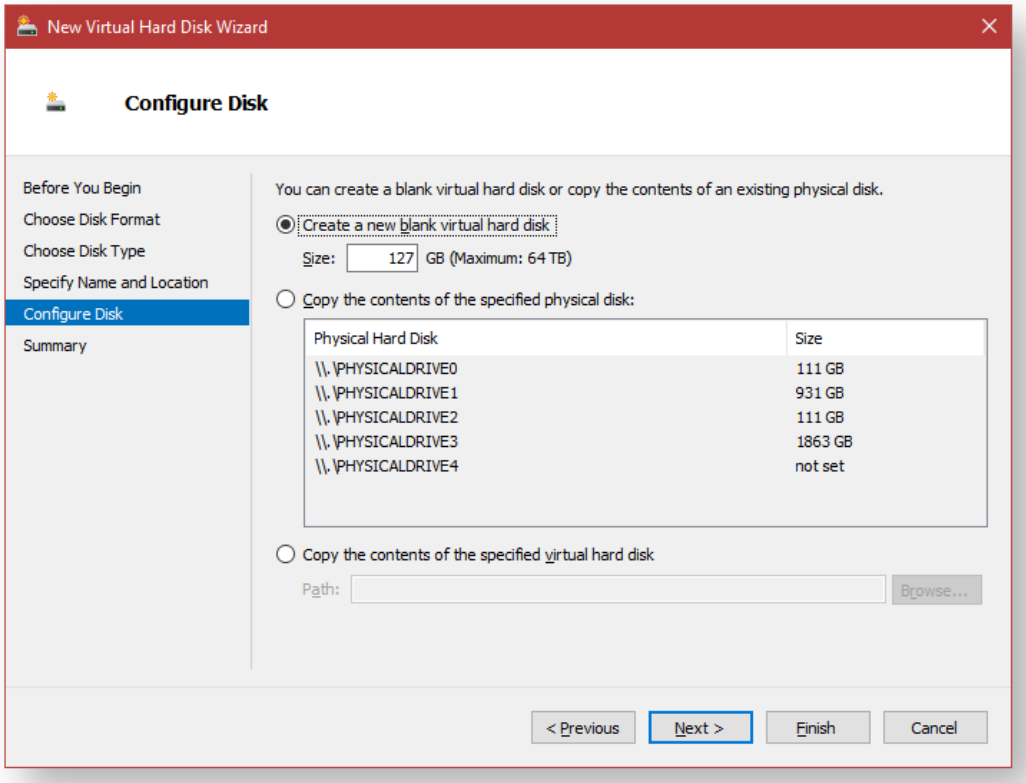
Specify location for the virtual disks.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



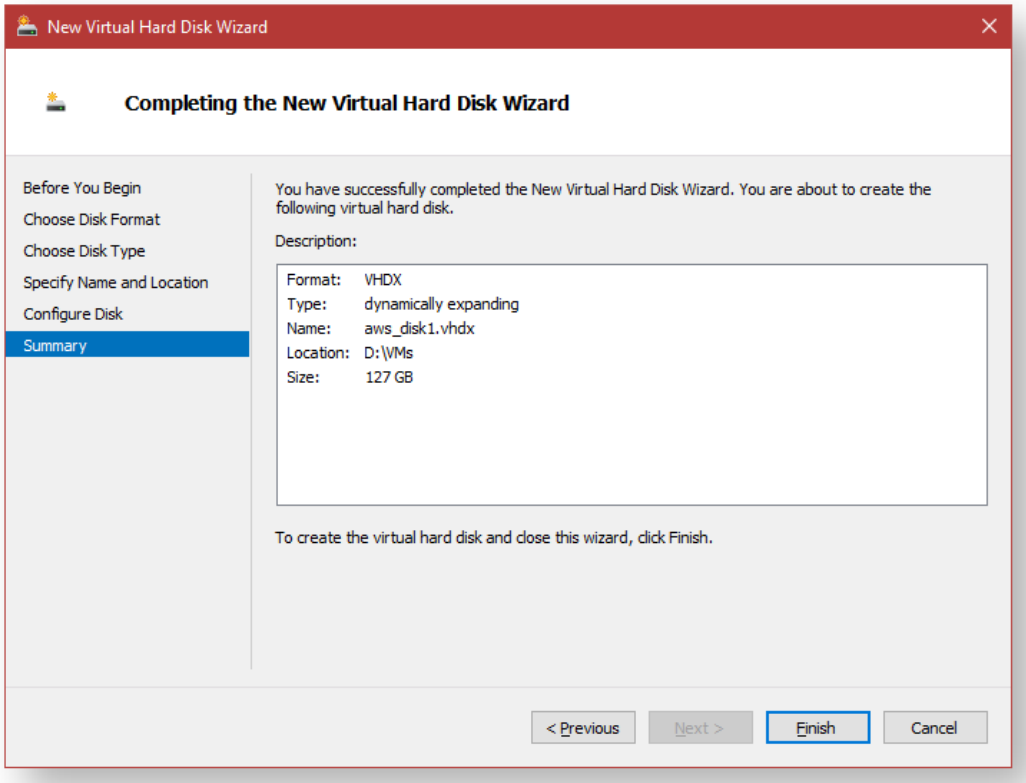
Specify the size of the virtual hard disk.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

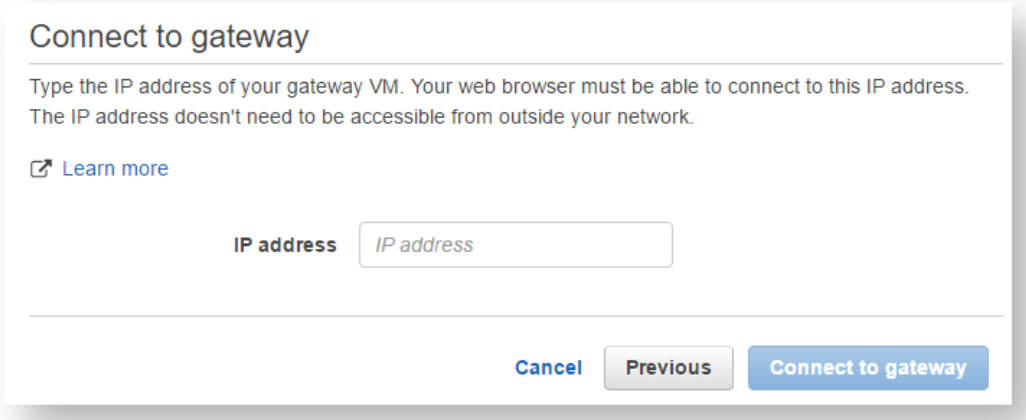


Click "Finish" to create the hard disk. *Repeat this process to create the second disk.*

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

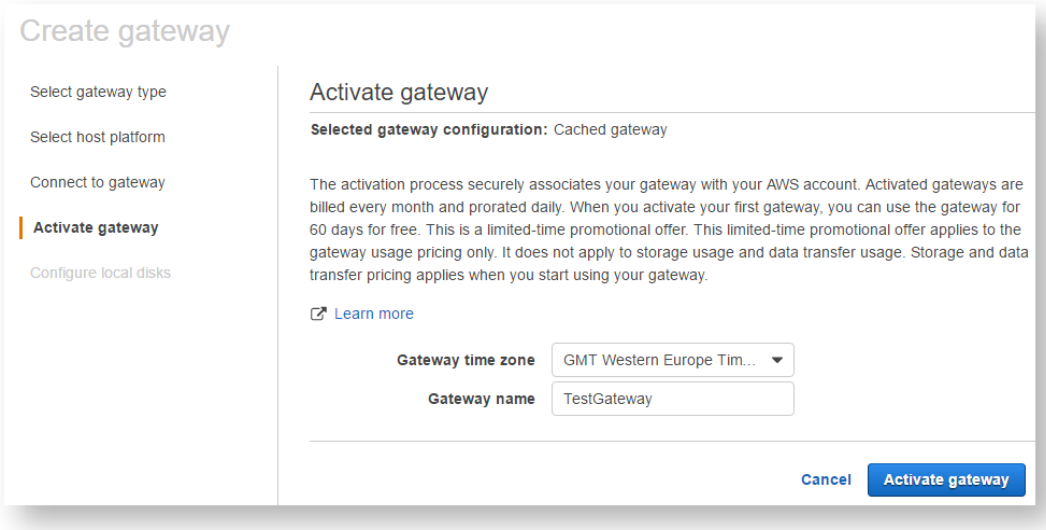


Once the VM is configured, creation of the gateway can continue by providing the IP address of the VM:

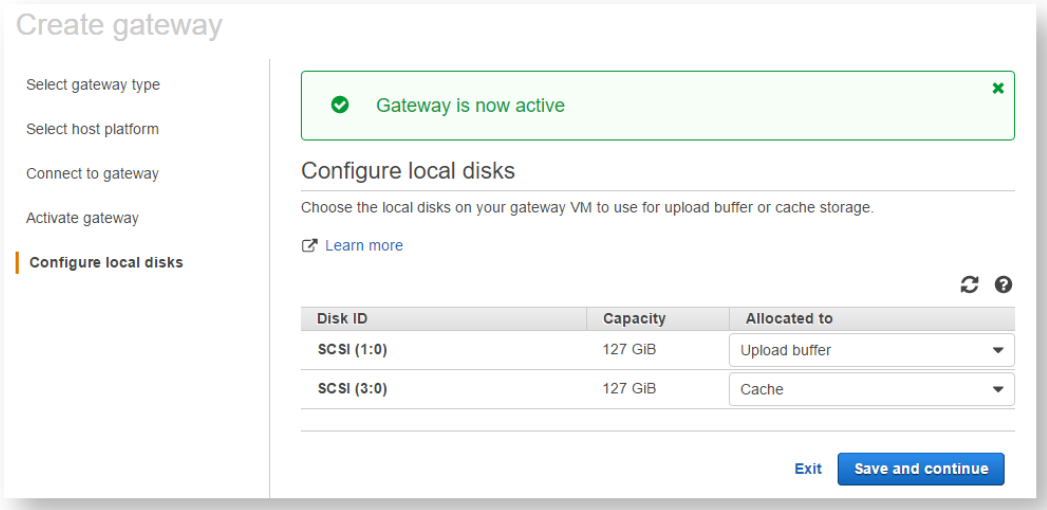


Specify the timezone for the gateway and provide a name:

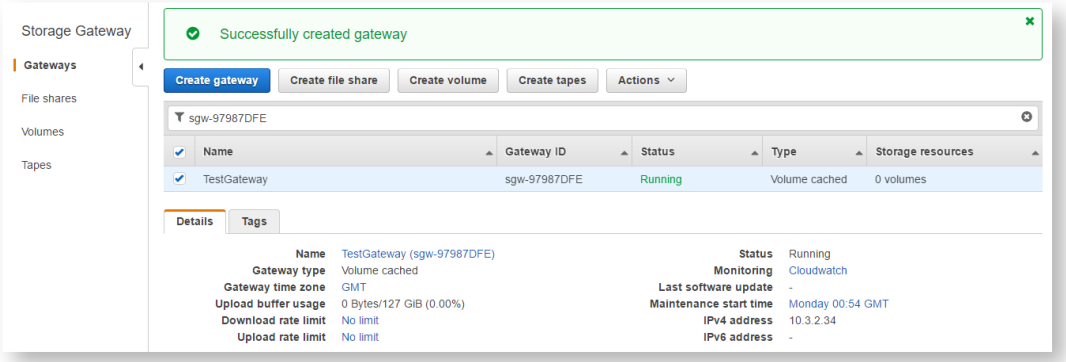
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



Once the gateway is activated, we need to specify which disk is the "Upload buffer", and which is the local "Cache":



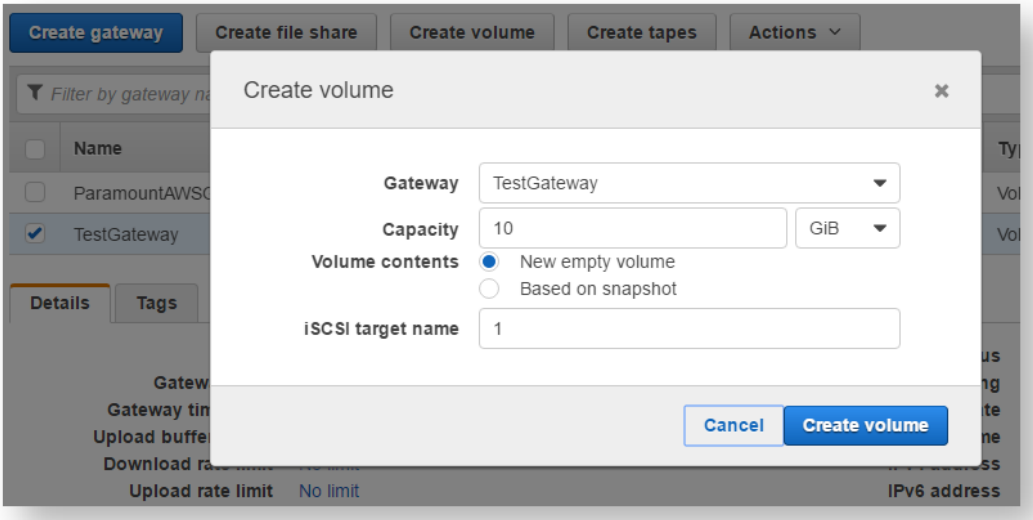
Once the settings are saved, the gateway will be fully created:



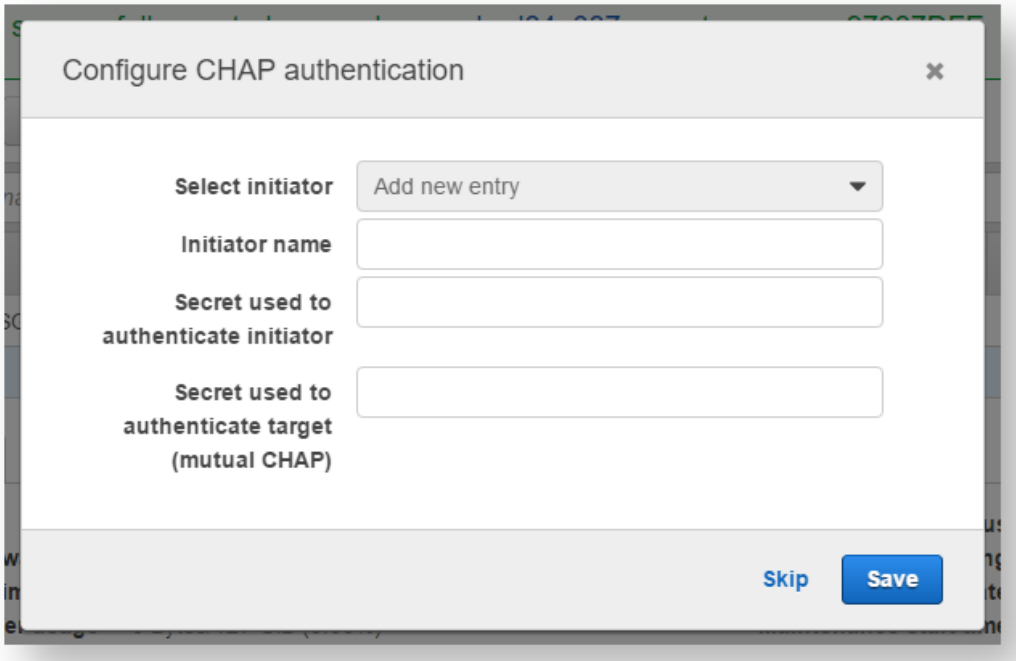
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Create a Volume

Once the gateway is created, we need to add a volume to the gateway by **clicking "Create volume" button**. After selecting the gateway, and specifying the capacity, **click the "Create volume" button**:

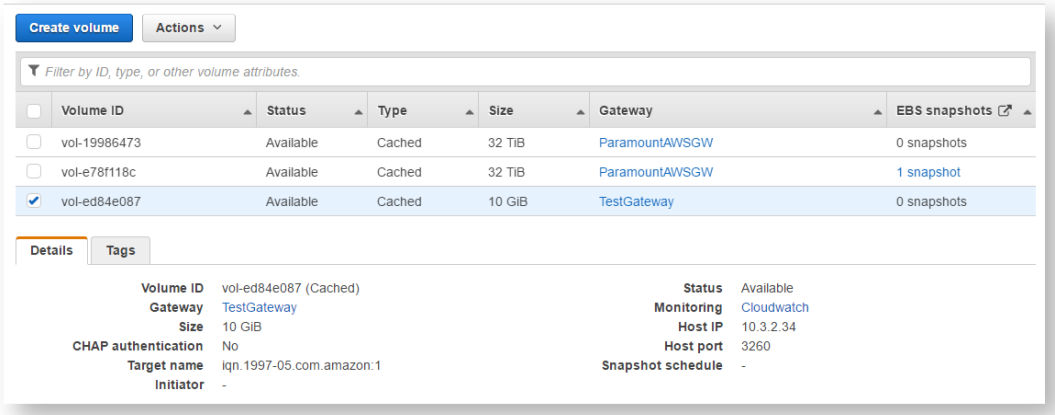


The volume can optionally be authenticated using CHAP, or saved for immediate use:



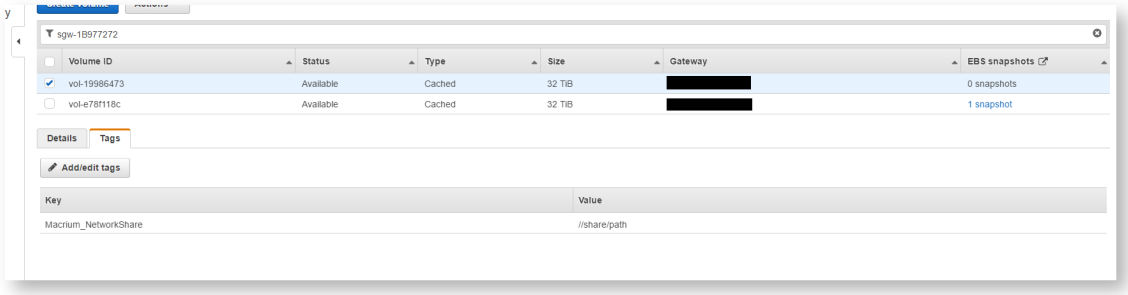
Once you have created a volume on the gateway, you can setup a network share for the volume on the VM and create a Amazon AWS Storage Gateway repository within Site Manager.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



To automatically connect an UNC share to an S3 volume, a Tag has to be created for the S3 volume.

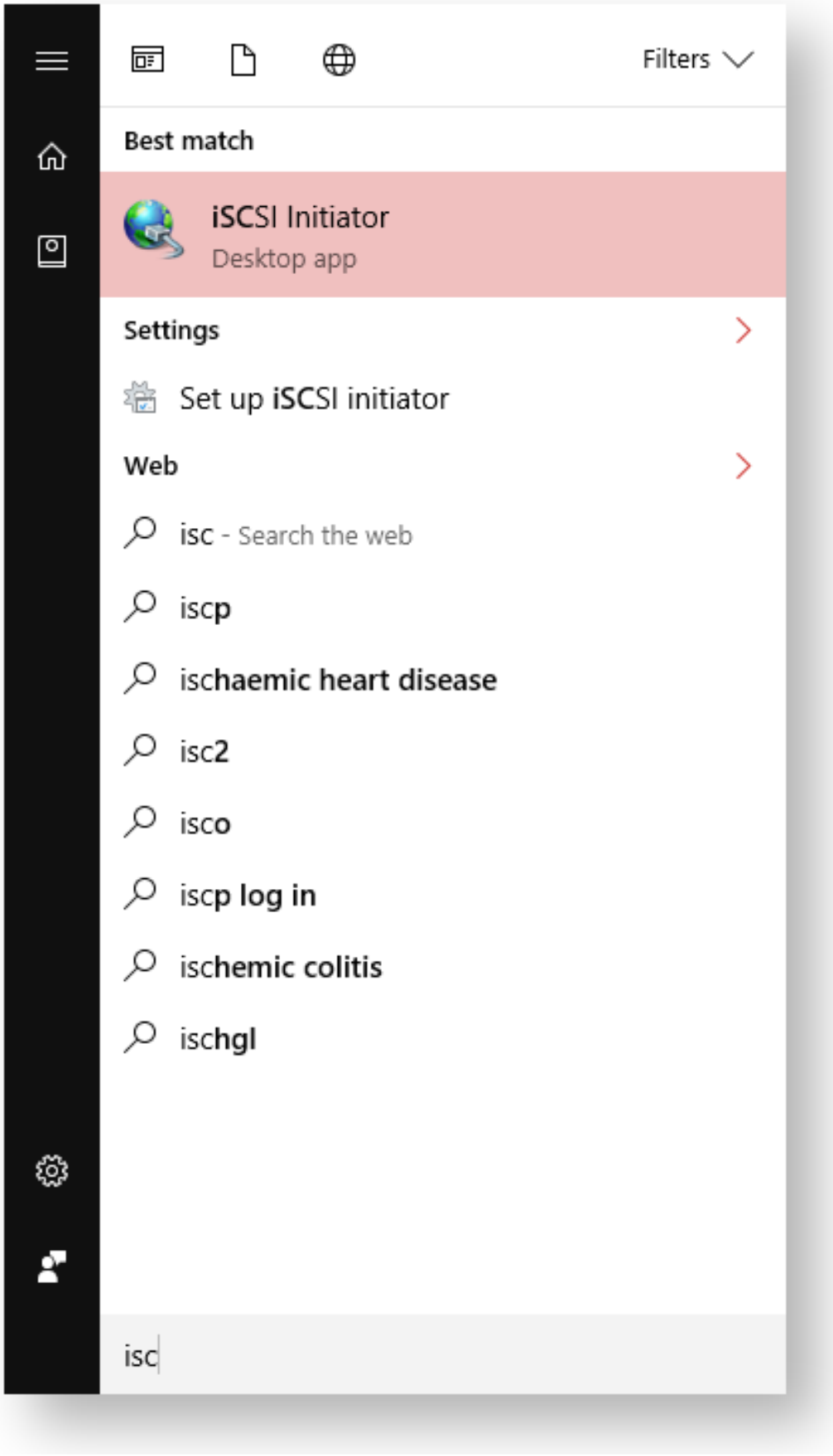
This tag must have key equal to "Macrium_NetworkShare" and back slashes must be replaced with forward slashes.



Creating an iSCSI Initialtor

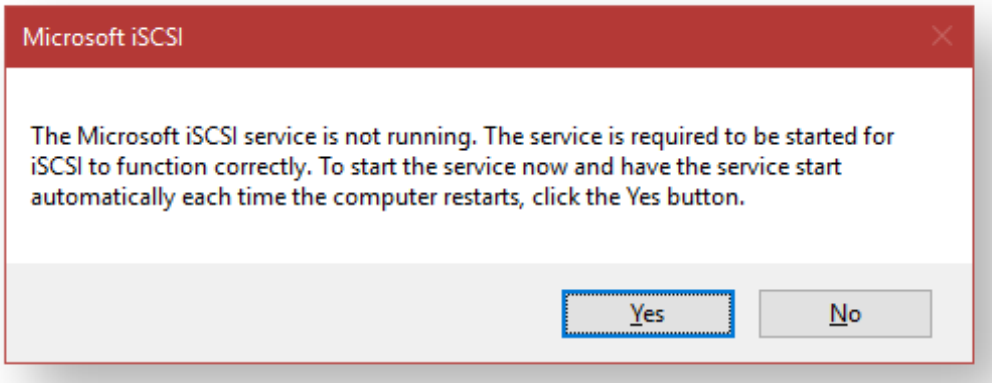
Launch the iSCSI control panel (iscsicpl.exe) from the Windows Start menu.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



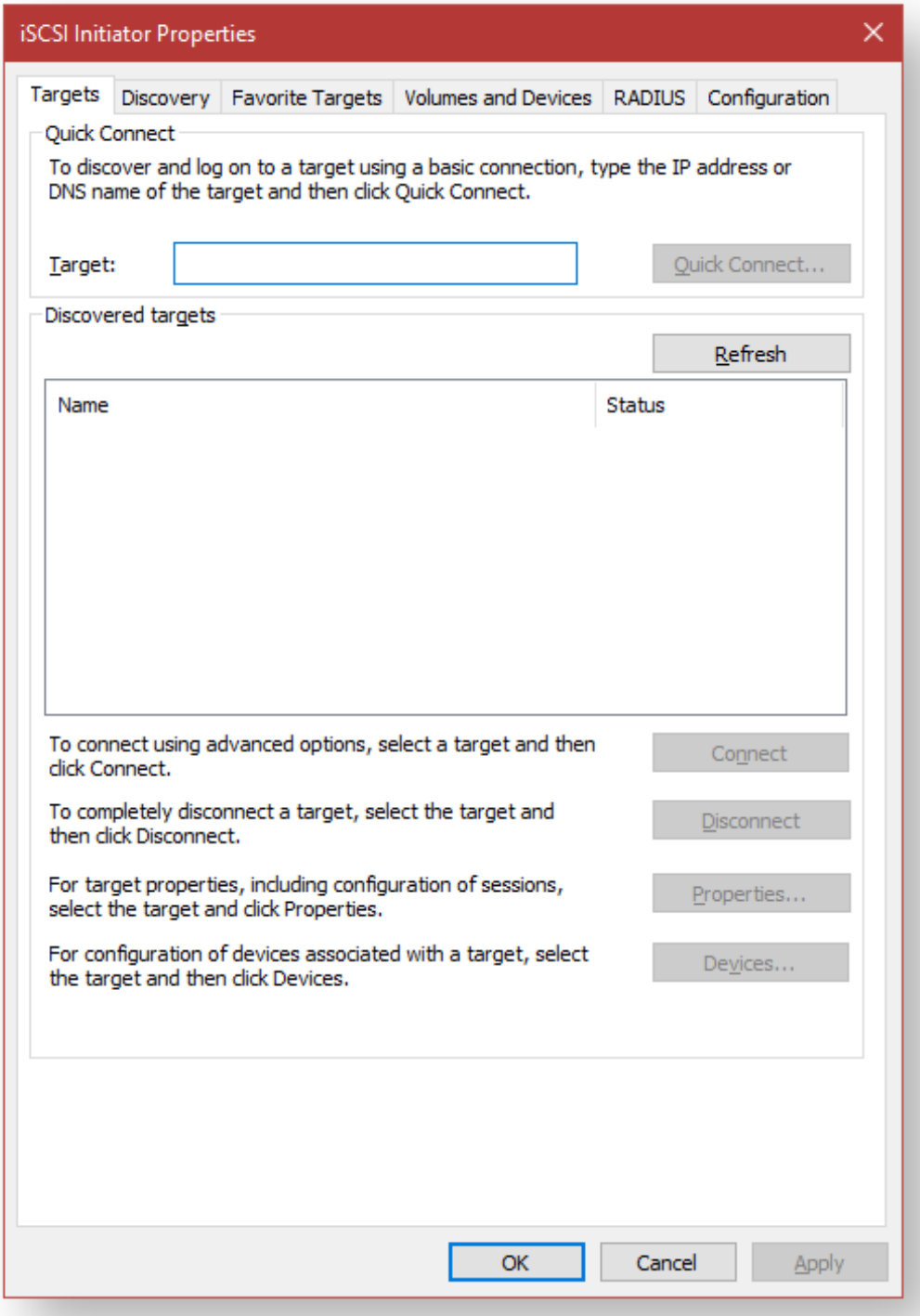
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

If the iSCSI service is not running you will be prompted to start the service.

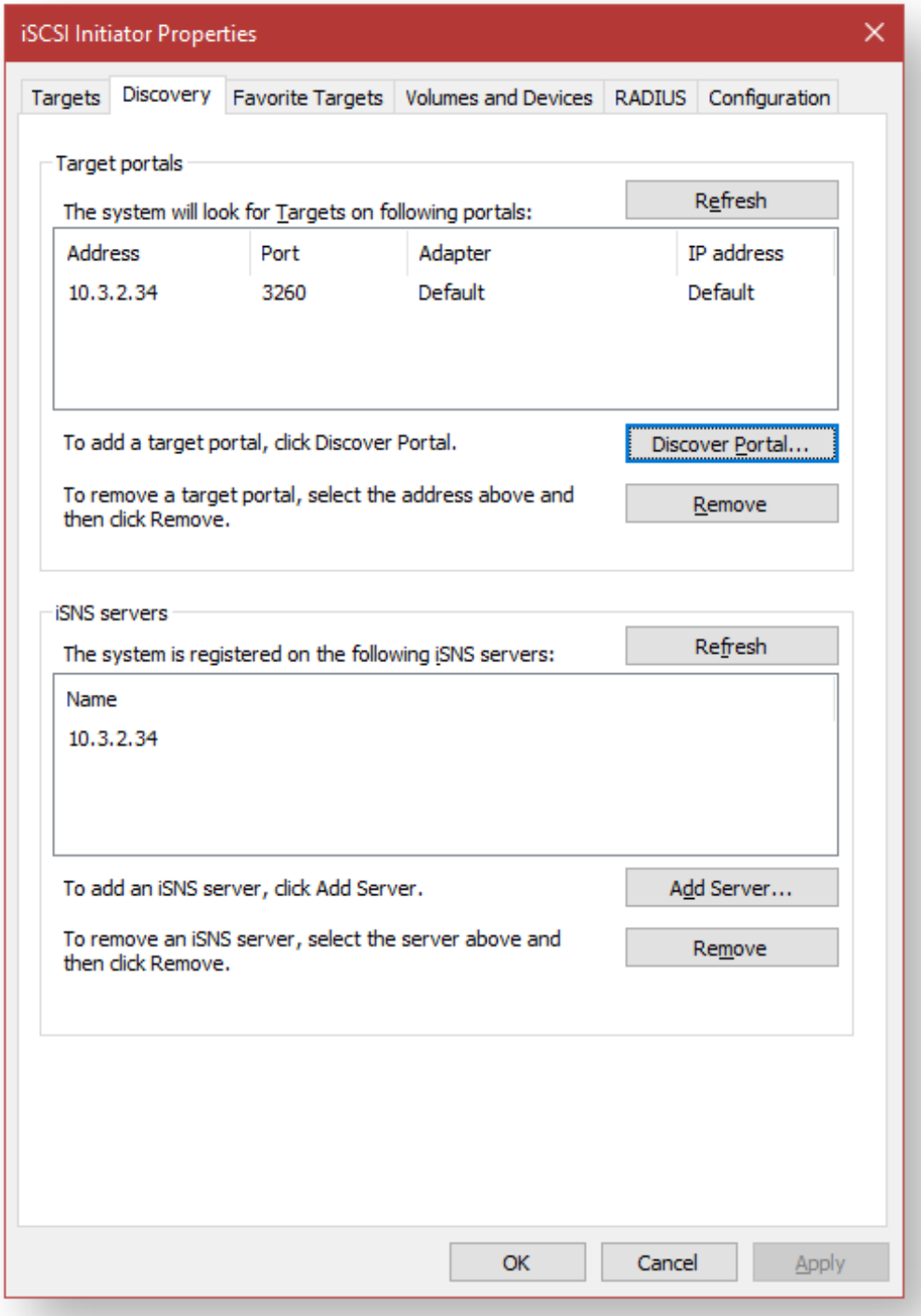


Click on the "Discovery" tab to locate the iSCSI targets.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

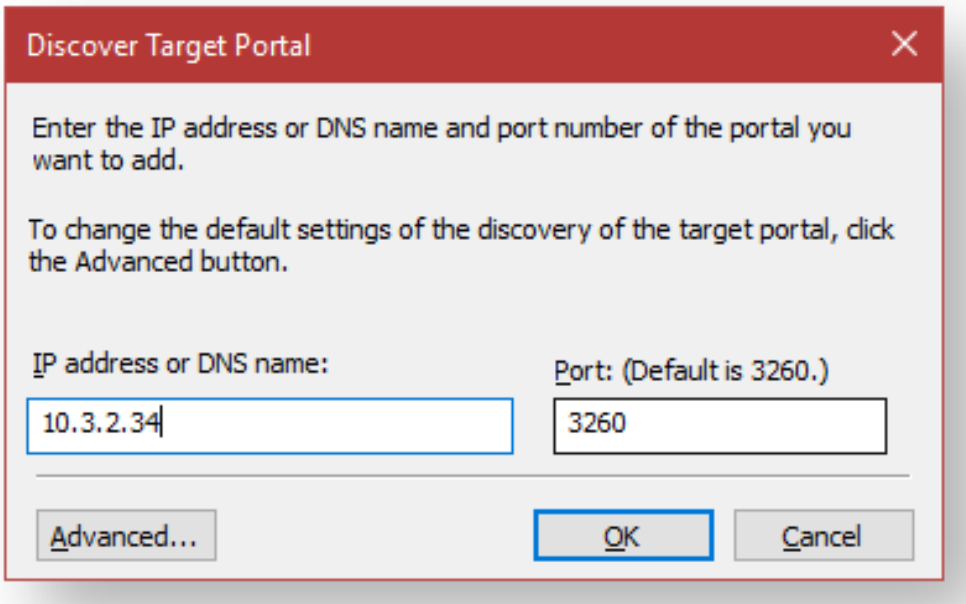


Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



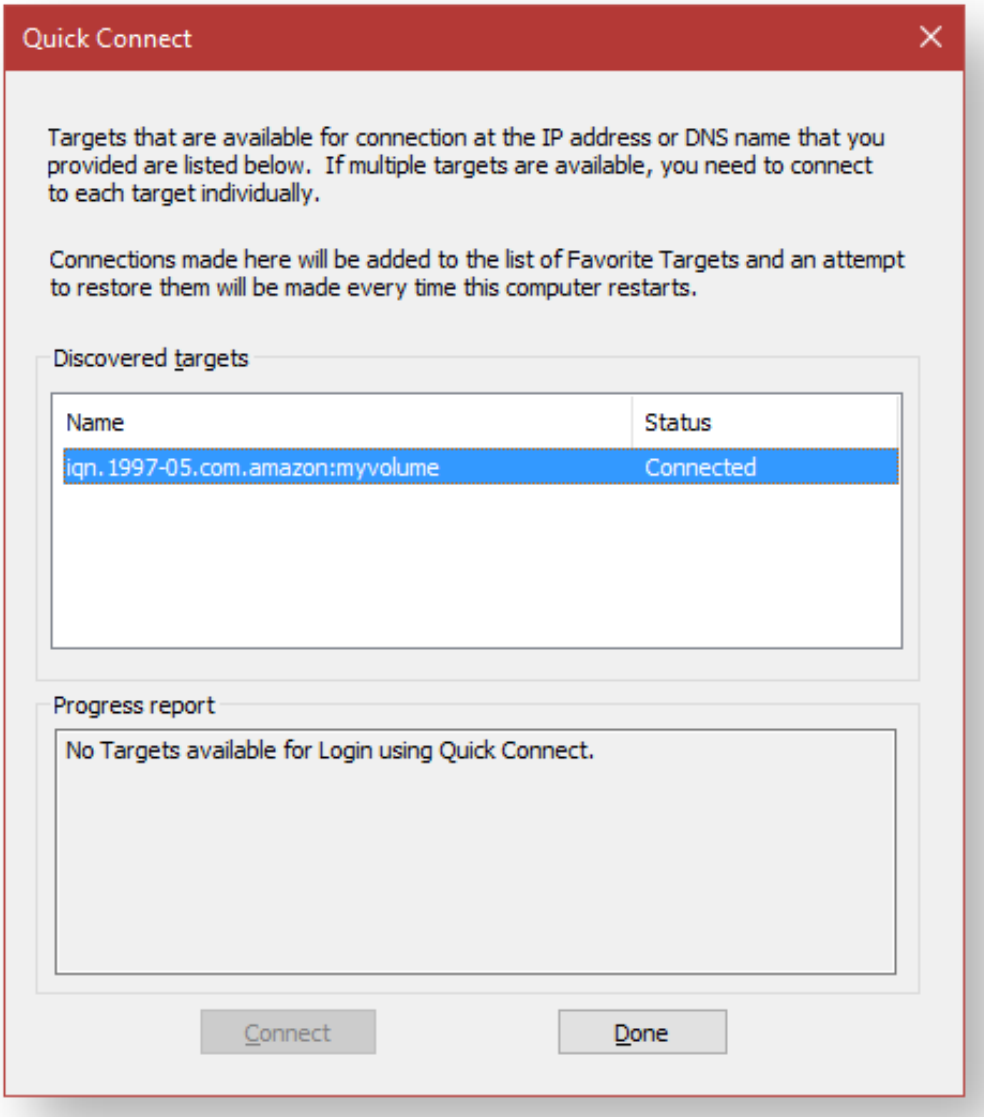
Specify the IP address of the VM.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



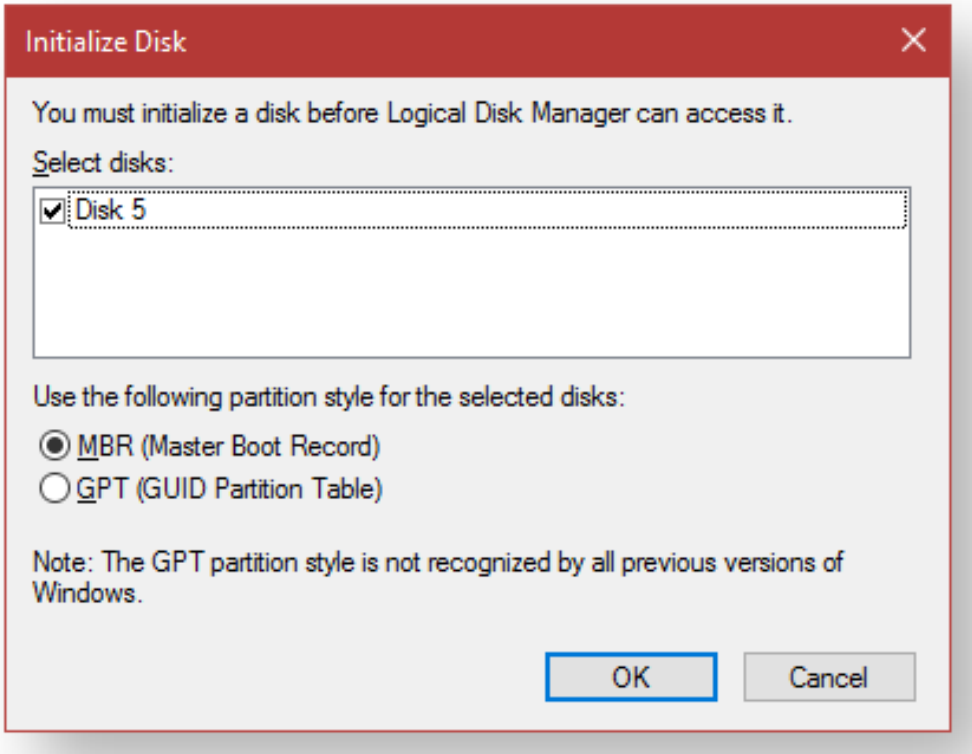
Switch back to the "Targets" tab, and click "Quick Connect". Connect to the iSCSI volume, then click "Done". the iSCSI will now create a iSCSI reference to the Volume gateway volumes and will be visible to the Windows client.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



After you have connected to the iSCSI volume, run "diskmgmt.msc". When Disk Management starts it detects the iSCSI Disk and prompts you to initialise it.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



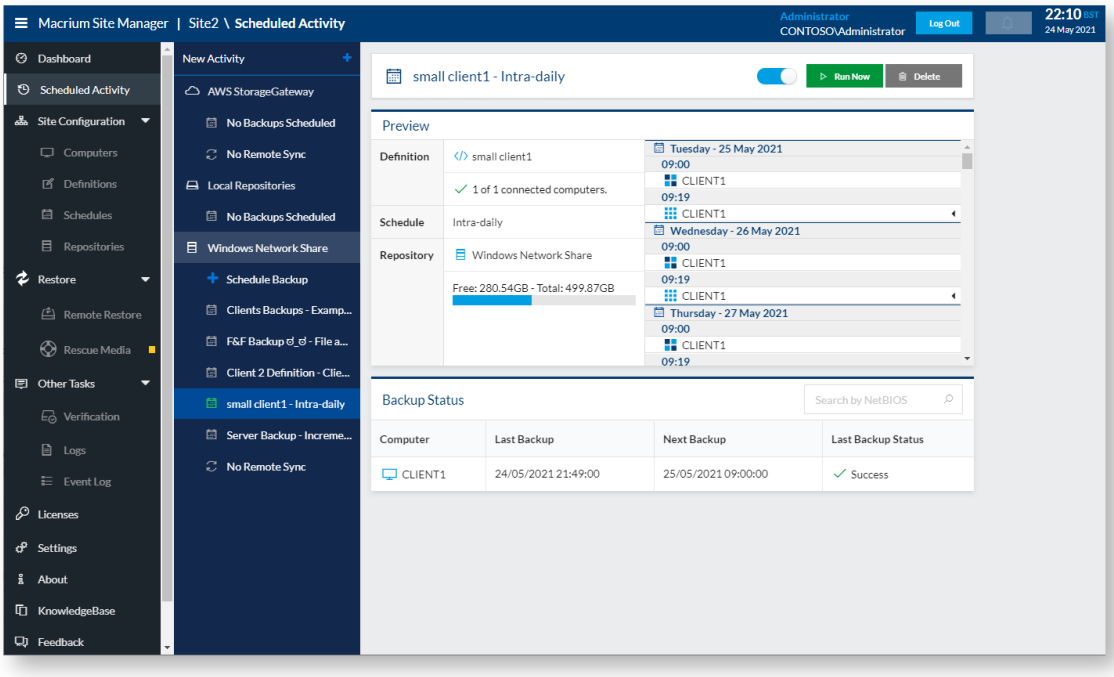
Once the disk is initialised, it can be formatted and assigned a driver letter and shared across the network as a UNC share.

Scheduled Activity

- Introduction
- Scheduling Backups
- Viewing Scheduled Backup Status
    - Enabling/Disabling the Scheduled Backup
    - Running the Scheduled Backup on Demand
    - Deleting the Scheduled Backup
    - Preview Section
    - Backup Status Section
    - Scheduling Remote Synchronization

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Introduction



The Scheduled Activity page is used to create, view and manage any regularly scheduled activity configured using the Backup Definitions, Schedules and Repositories configured in Site Manager.

The following activities can be scheduled:

Activity	Description
Backup	Backups are scheduled by selecting a Backup Definition to define what gets backed up and a Schedule to control when the backups happen.
Remote Synchronization	Remote Synchronization can be scheduled to synchronize the contents of a Repository to an external server or disk. ⚠ Only one Remote Synchronization can be scheduled for each Repository. Repositories of the **Local** type cannot have Remote Synchronization as the data in these Repositories is spread across multiple machines.

The left hand menu for this page shows a list of Repositories, with each scheduled item listed underneath. Each scheduled activity item is color coded to show status:

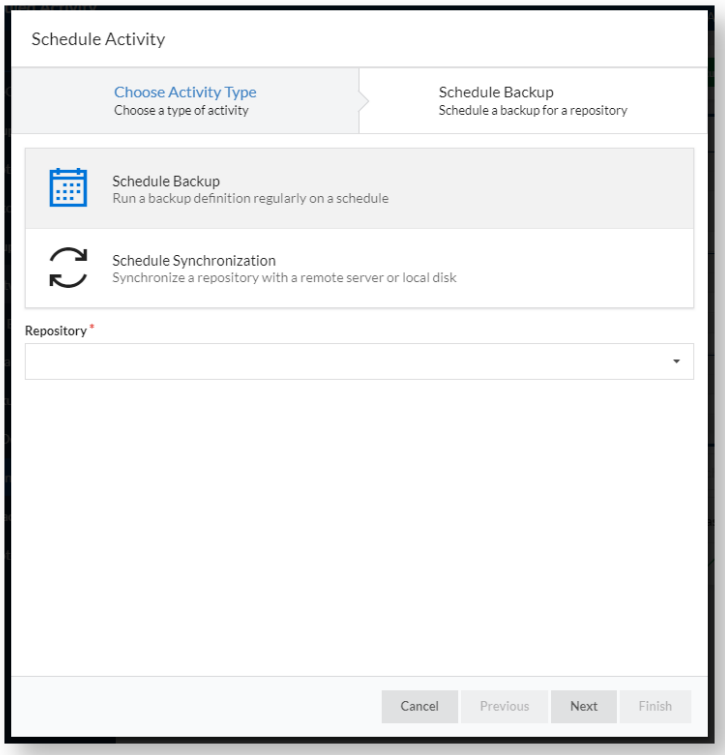
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

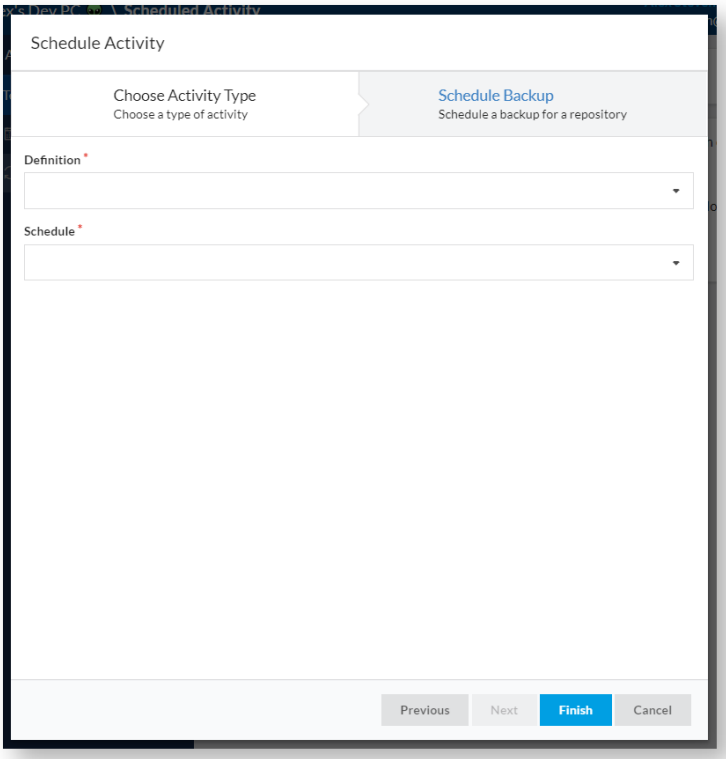
Colour	Meaning
Red	An error has occurred - for example, one computers in a the scheduled backup encountered an error during backup
Green	The scheduled activity is successful
Gray	The activity is disabled or has not yet run for the first time

Scheduling Backups

Backups can be scheduled by selecting the **New Activity** option at the top of the left-hand side panel, or selecting the **Schedule Backup** option under each Repository. If using the former method, the page below is shown. If **Schedule Backup** is used, this stage is skipped.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



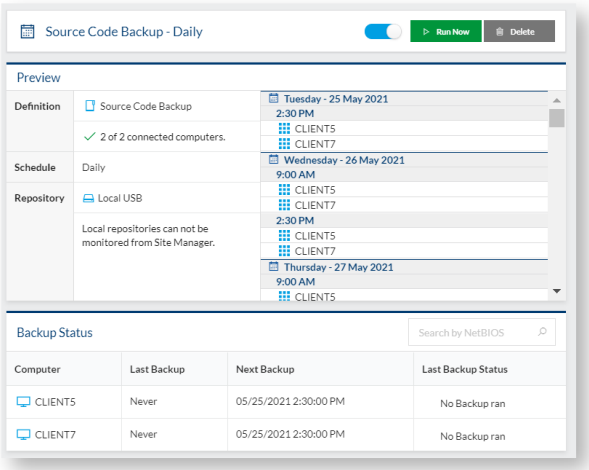


Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Once a Repository is selected and **Schedule Backup** is selected, the second wizard page is shown, where the Definition and Schedule can be selected. Once they are picked from the drop-down list, the wizard can be finished and the newly scheduled backup will appear in the list under the repository with the name of the Definition and Schedule.

Viewing Scheduled Backup Status

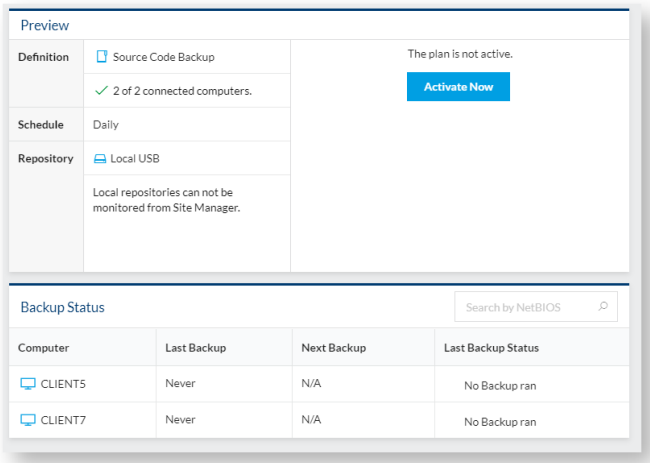
When a scheduled backup is selected, the view below is shown:



This contains a header, plus a **Preview** and a **Backup Status** section.

Enabling/Disabling the Scheduled Backup

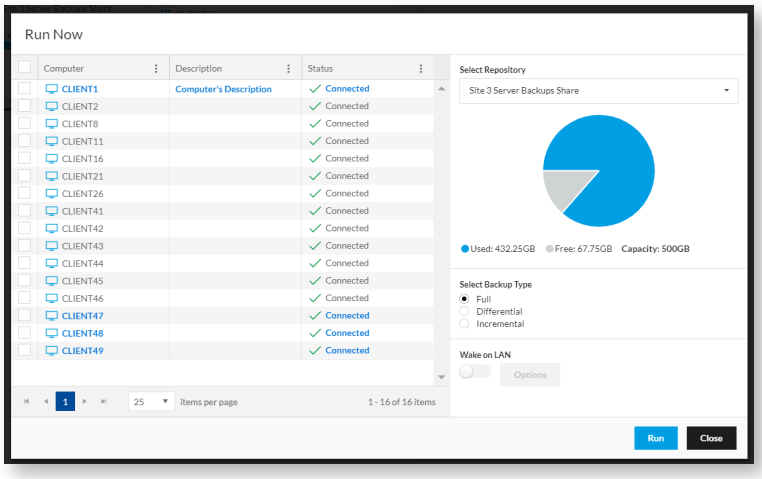
The backup may be disabled or enabled by clicking the toggle in the header bar. When the backup is disabled, the Preview pane will indicate this:



Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Running the Scheduled Backup on Demand

The **Run Now** option in the header allows one or more of the computers to start a backup now, rather than at the next scheduled time. This will bring up the **Run Now** dialog:



After selecting the computers and type of backup (Full, Differential or Incremental), pressing **Run** will start the backups.

> Note that backups may not run immediately based on simultaneous backup limits in Repository settings. Disconnected computers will wait until connection to run.
>
> Computers must be connected to perform a Run Now backup unless the Wake-on-LAN option is set. See Backup Definitions for more information on Run Now backups

Deleting the Scheduled Backup

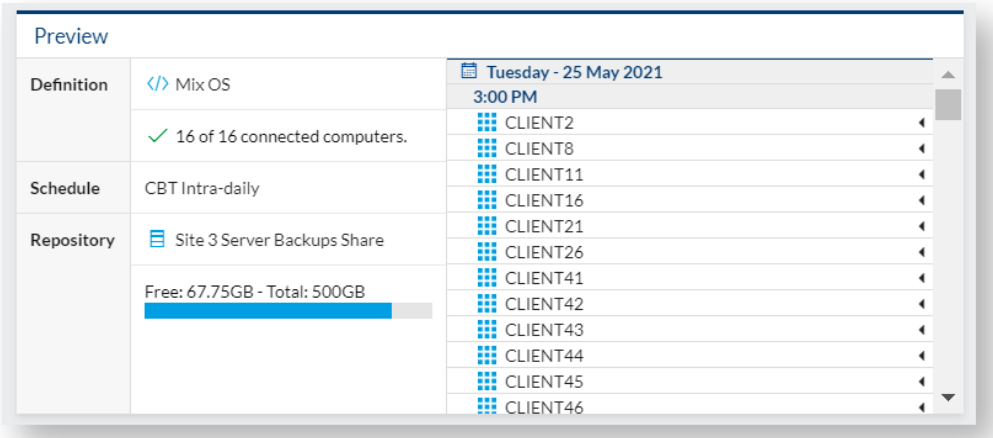
The Scheduled Backup can be deleted, preventing any further backups.

> Backup files created in the repository are not deleted by deleting the scheduled backup. They are only deleted through the browse feature of the repository or if manually deleted.

Preview Section

The preview contains a summary of information about the scheduled backup:

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



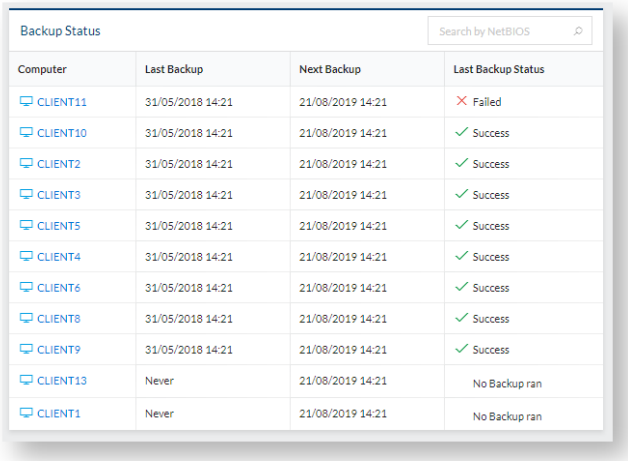
This contains the following information:

Heading	Description
Definition	The Backup Definition used by this scheduled backup, along with some information on the number of computers and their overall status
Schedule	The Schedule used by this scheduled backup
Repository	The Repository the backups will be stored in, along with free space information
Right Hand Panel	If the backup is active, it will show a forecast for this backup plan, if inactive it will indicate this. The forecast here shows only the backups for the selected backup schedule. To see a forecast of all activity to a repository, use the **Repository** or **Dashboard** pages.

Backup Status Section

This section contains the last backup information for each computer in the scheduled backup:

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



Each computer lists:

- Last backup time
- Last backup status - Success, Failure or Succeeded with warnings
- Next scheduled backup time

Scheduling Remote Synchronization

Remote Synchronization can be configured through the **New Activity** wizard, or through selecting the **No Remote Sync** entry under the appropriate repository and clicking **Configure Synchronization**. Remote Synchronization is covered in detail in this article.

Synchronizing a Repository with a Remote Server

- Overview
- Configuring Remote Synchronization
  - Stage 1 - Activity Type
  - Stage 2 - Synchronization Type
  - Stage 3 - Connection Details
  - Stage 4 - Configuration
  - Finishing the Wizard
- Viewing Remote Synchronization Status
  - Current Server Status
  - Last Synchronization Results
- Viewing a Synchronization in Progress
- Common Issues and Fixes
  - Synchronization Failures

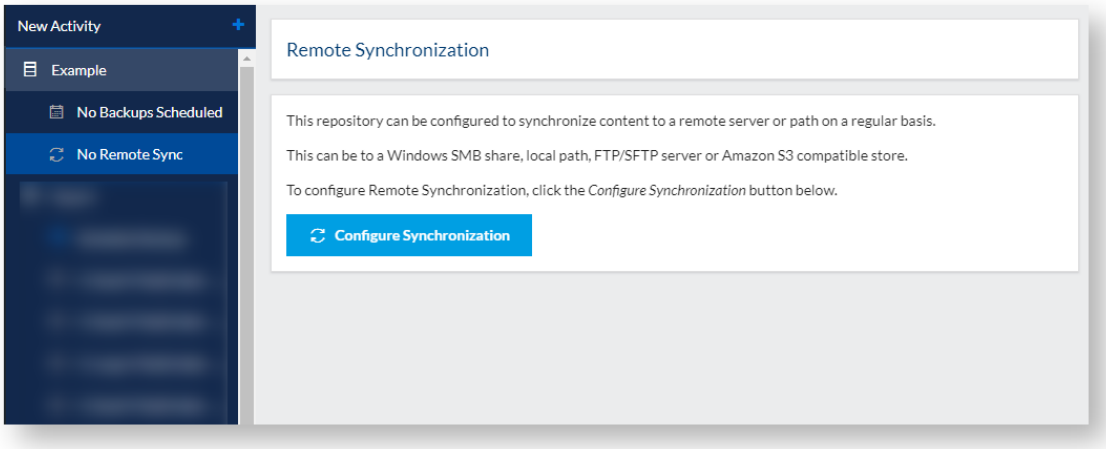
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

- Full Backup Files are Synchronized When Creating Incremental Backups
- Remote Server ID mismatch

Overview

Site Manager can automatically synchronize all backups stored in a Repository to a remote server or disk on a daily basis. This can be used to efficiently ensure that offsite replication of backup data is performed. The Site Manager server will manage stopping backups on the server and ensuring that the synchronization process has a consistent view of the Repository. The synchronization process will also manage failed and partially uploaded files and ensure the remote copy of the Repository is always in a consistent state.

This feature can be accessed through the Scheduled Activity page and is configured on a per-Repository basis:



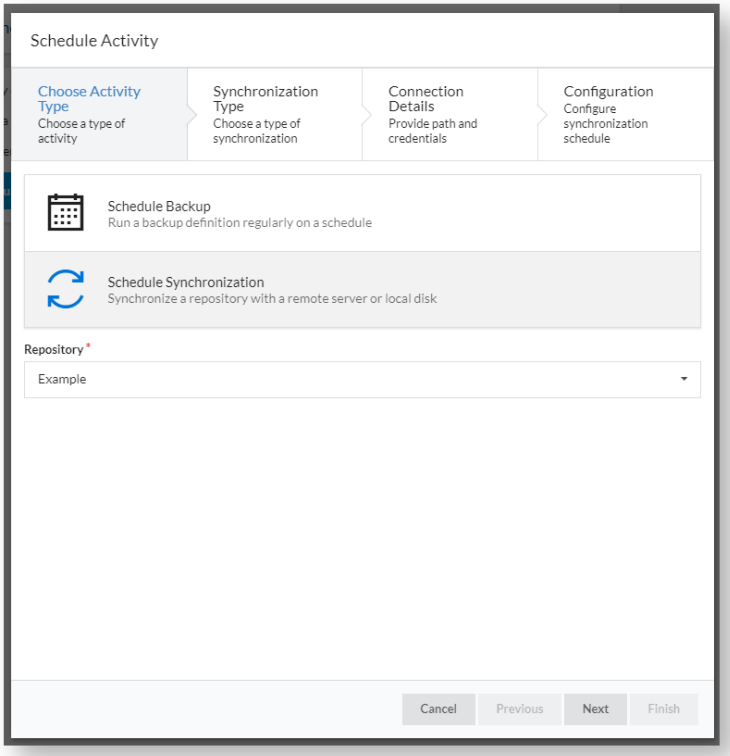
Configuring Remote Synchronization

The **Scheduled Activity** page has an entry for each Repository (except Local Repositories) which will either display information on the remote synchronization configuration or offer the option of creating a new remote synchronization. Clicking **New Activity** or **Configure Synchronization** will display the Synchronization Setup wizard. The steps of this wizard are described below:

Stage 1 - Activity Type

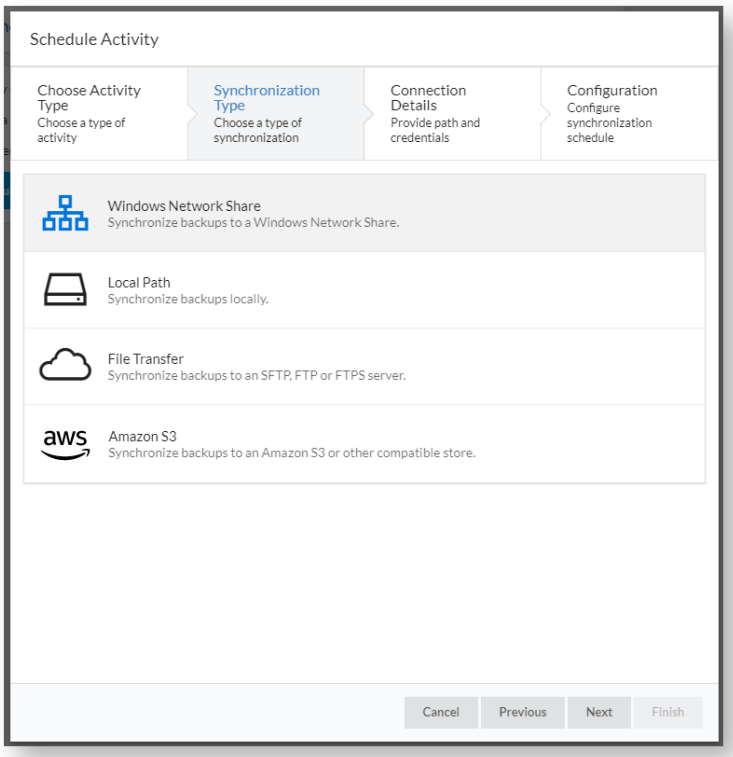
In the first stage, the type of activity and Repository are chosen. For Remote Synchronization, this should always be **Schedule Synchronization**. This stage may be skipped depending on how the wizard is launched.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



Stage 2 - Synchronization Type

In the second stage of configuration, the type of remote sync is chosen. The types available are:



Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

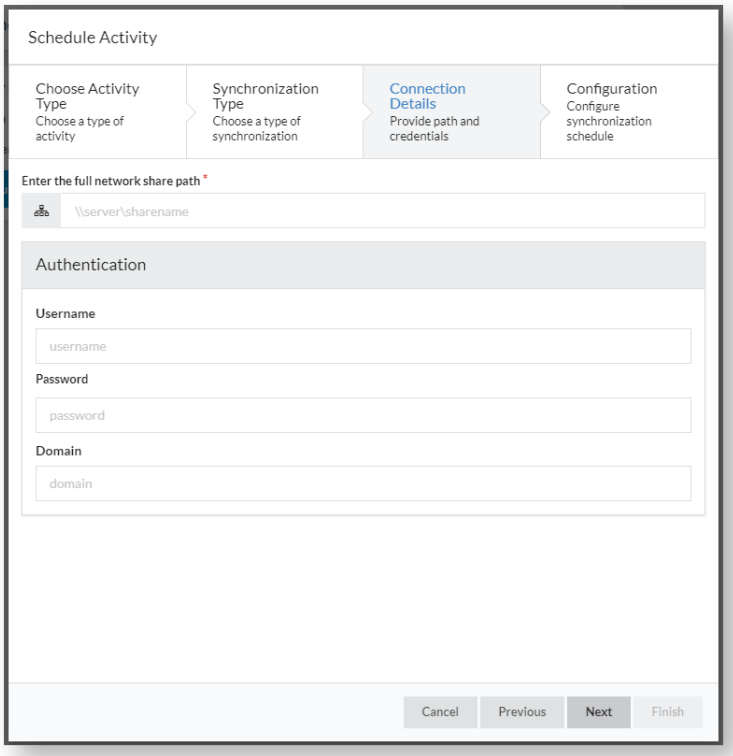
Synchronization Type	Description
Windows Network Share	Synchronization to any remote server which can communicate as a SMB/CIFS share of the form \\servername\share
Local Path	Synchronization with any file path local to the Site Manager server. This might be a folder, a local USB disk or any other path which can be read and written to as a folder
File Transfer	Synchronization to a server running SFTP, FTP or FTPS
Amazon S3	Synchronization to a Amazon S3 server or other compatible store

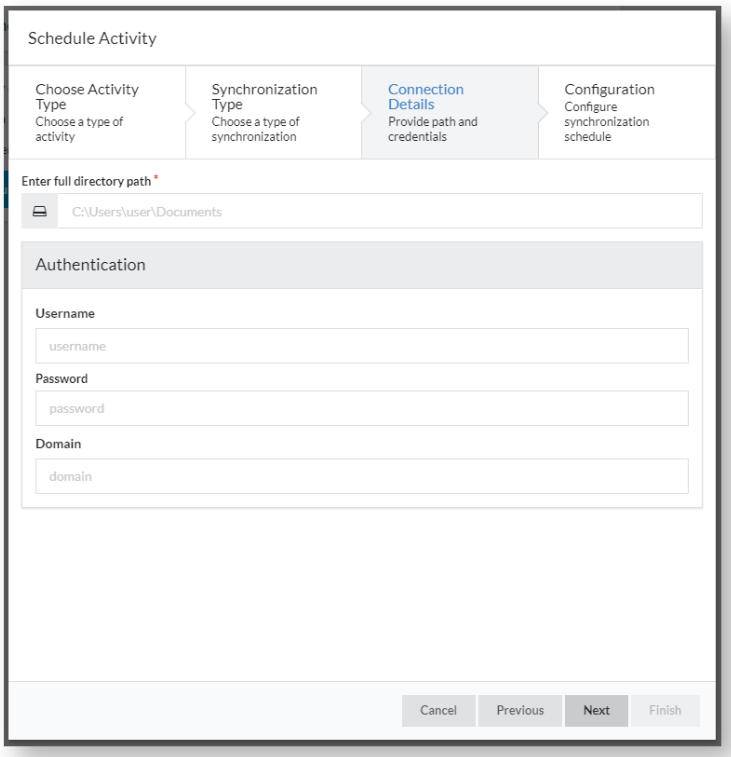
The next step will change depending on which synchronization type is chosen.

Stage 3 - Connection Details

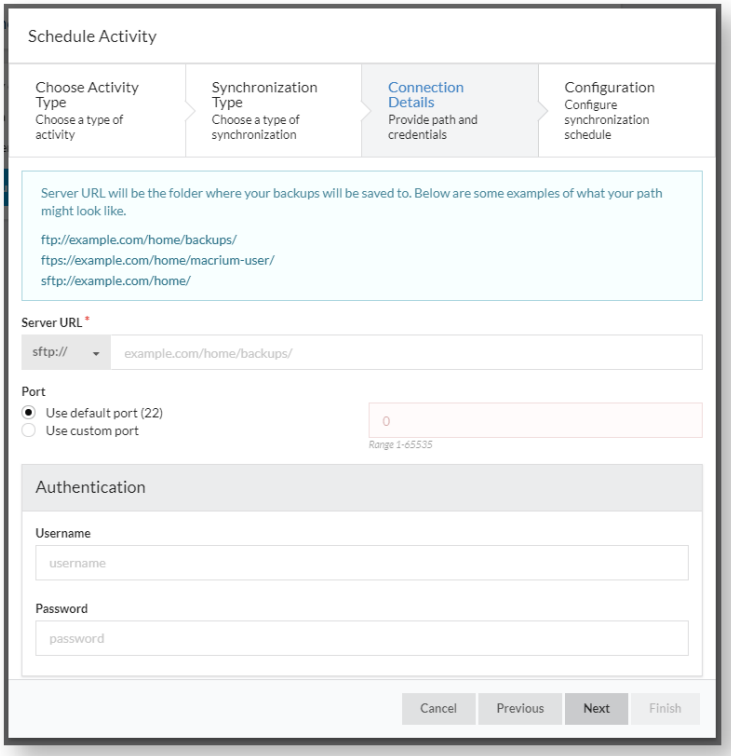
The third stage of configuration includes all the options specific to configuration type. This includes the path to the remote server or folder and any authentication details. The different remote synchronization types take the following details:

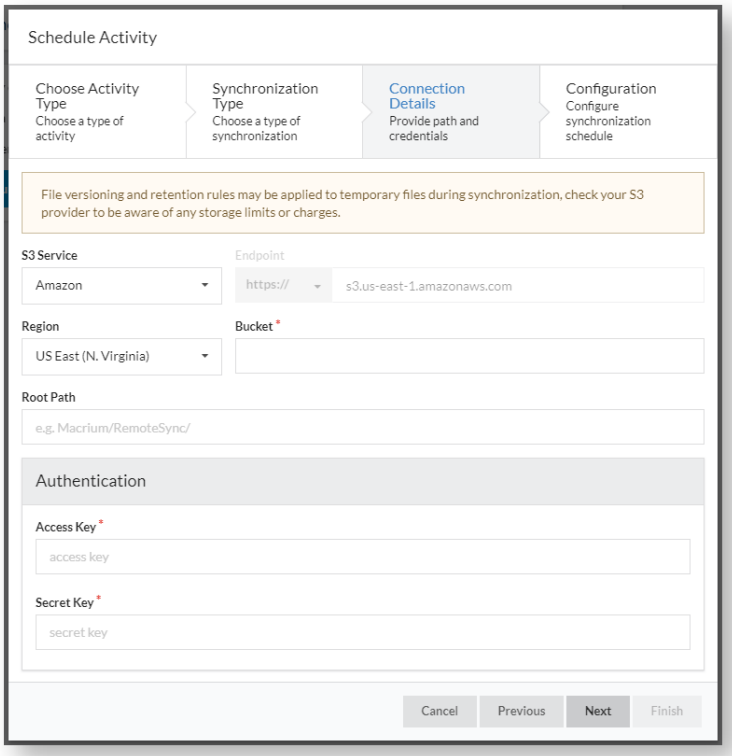
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.





Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.





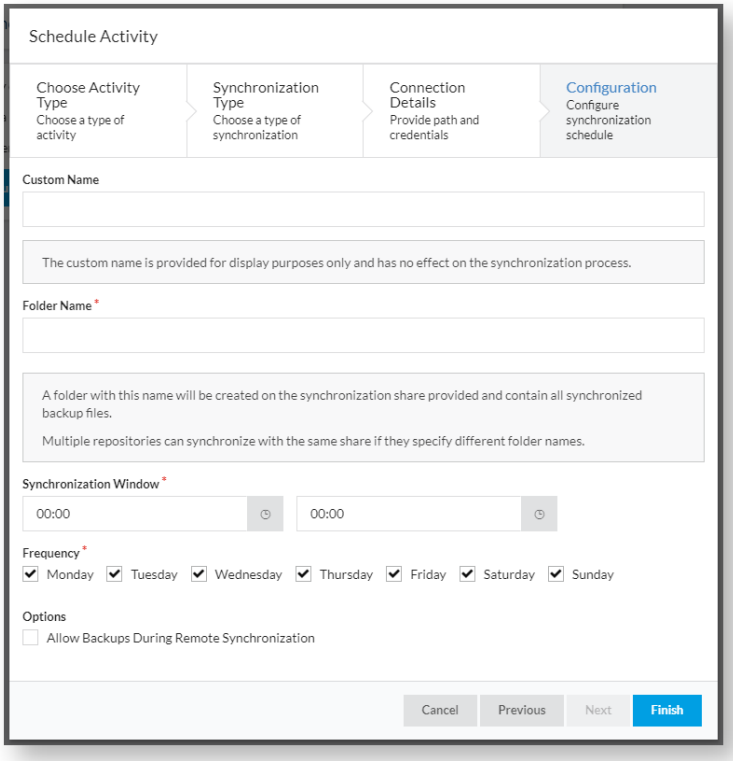
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Synchronization Type	Available Options
Windows Network Share	Network share path in UNC format (\\server\share\folder, backslash separated), username, password and domain. If a domain is entered as part of the username (in DOMAIN\User or user@domain.dns form), the domain field is disabled.
Local Path	Local path in Windows path format (Backslash separated) with optional username, password and domain. If these are omitted, the path is accessed using the SYSTEM account of the Site Manager server.
File Transfer	Type of protocol (FTP, FTPS or SFTP in the URI dropdown), Path to the server in URI format (sftp://example.com/home/backups/macrium, omitting the leading sftp:// and using forward slash separators), username and password for the remote server. A custom port may also be supplied. **SFTP Paths** When configuring an SFTP server, include the full path to the folder to sync to in the server path, NOT the path relative to the user's home folder. For example, when connecting to a server as **user**, to sync to the user's home folder the full path must be specified e.g. **example.com/home/user/macrium** not **example.com /macrium** **This may not apply to all SFTP servers or to FTP servers.**
Amazon S3	• S3 Service - Amazon, Wasabi, Backblaze or Custom for full configuration control. • Endpoint - URL per the service providers specification, required only for custom configurations, protocol type (Https or Http) with URL omitting the leading protocol type. • Bucket - Active bucket as configured within the service providers console. • Region - The selected buckets region identifier per service providers specification. • Root Path - Location within the bucket to upload remote sync files to, should be forward slash separated. • Authentication - Access key and secret key as configured within the service providers console. Further information can be found in this article.

Stage 4 - Configuration

The final stage configures options which apply to all synchronization types. The options are as follows:

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



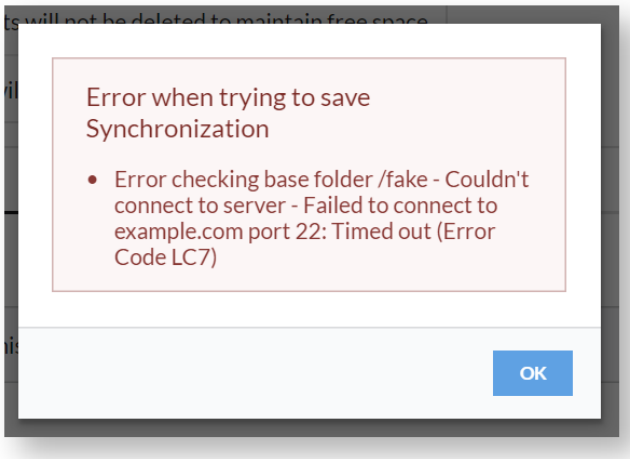
Option	Description
Custom Name	The custom name is shown in the UI to identify the sync. If left blank, the server/local path of the sync will be used instead
Folder Name	The folder name set here will be created on the server/remote path to store the synchronized backups The path configured as part of the network or server path must exist on the remote server or the sync process will generate an error, however Site Manager will create the folder set as the **Folder Name** if it does not already exist. For example, if remote sync is configured with a server of **sftp://192.168.0.1/home/backups** and a folder name of **SiteManager1**, the sync process will store image files in **/home/backups/SiteManager1**, creating the **SiteManager1** folder if necessary. Multiple repositories can sync to the same server/network path so long as the folder name is different for each one.
Synchronization Window - Times	The synchronization window controls what time of day the sync will run. When the start time is reached, Site Manager will stop scheduling backups on the repository, wait for any existing backups to finish then run the sync. After the sync has finished, backups resume. If the sync

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Option	Description
	can't be started before the sync end time is reached, the sync attempt is abandoned until the following day. This option allows some control over when high internet bandwidth options like sync get run.
Synchronization Window - Frequency	The sync process can be limited to only happening on some days of the week by selecting the desired days here.
Options - Allow Backups During Remote Sync	If this option is selected, backups to the repository will be allowed to continue during the synchronization process, with some limitations. 1. The remote sync can only start when no backups are running - this is so that there is a consistent, point in time view of which backups exist 2. The sync process will find changes and data to upload and sort them by computer 3. Changes are uploaded for the computer with the smallest amount of data to upload 4. The computer from step 3 is 'unlocked' and backups for this computer may now start 5. Steps 3 and 4 are repeated until all data is uploaded 6. The change is committed in the remote location. Before this step, if the sync fails, the changes can be rolled back to the previous repository state

Finishing the Wizard

When finishing the wizard, a connection test is performed by the server and any errors are highlighted to be fixed:

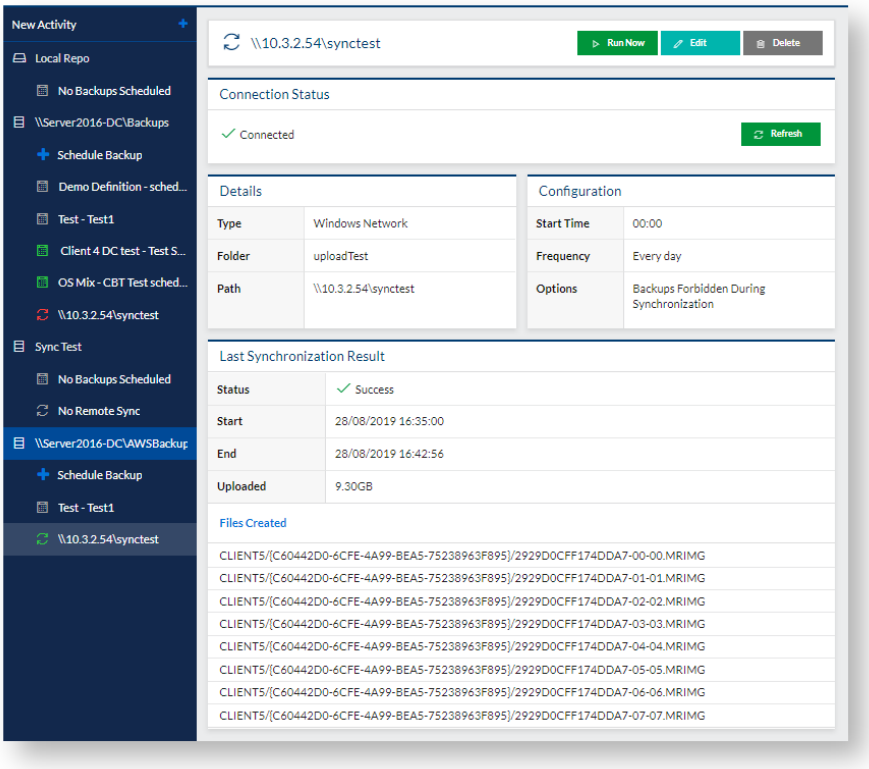


Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Viewing Remote Synchronization Status

Current Server Status

Once Remote Synchronization has been configured, the Remote Synchronization activity in the **Scheduled Activity** page will display the following status:



The **Run Now** option allows a sync to be started manually. This manually started sync will wait for any active backups in the Repository to finish before starting and will prevent any backups from starting until the sync is completed.

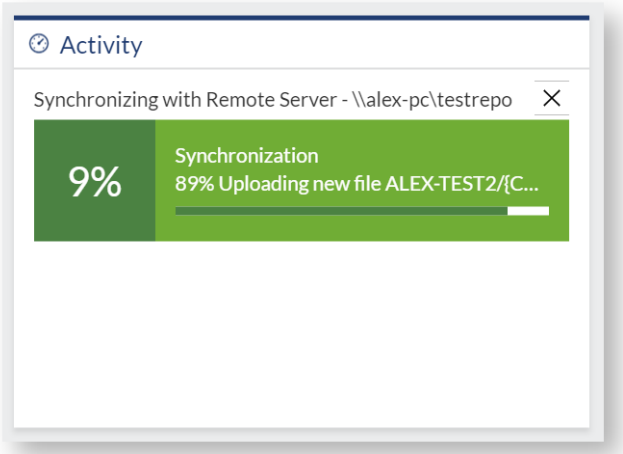
Last Synchronization Results

This section shows the results of the last sync which ran, including whether it succeeded, any error messages, the amount of data uploaded and which files were affected.

Viewing a Synchronization in Progress

Upcoming syncs are shown in the forecast of the Repository and active syncs are shown in the Activity widget on the Dashboard page just as for backups

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



Common Issues and Fixes

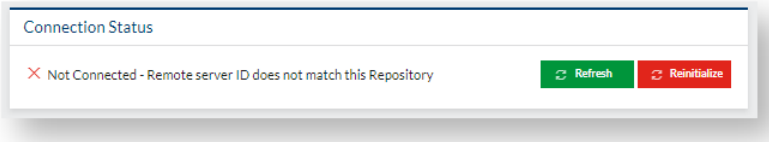
Synchronization Failures

If a sync fails part way through the upload process, the next sync will roll the remote server back to it's previous state before starting - there is no need to do anything to repair the remote sync repository state, this will happen automatically on the next sync. Communications issues are handled by internally retrying the upload for up to 10 minutes if a disconnection from the server happens.

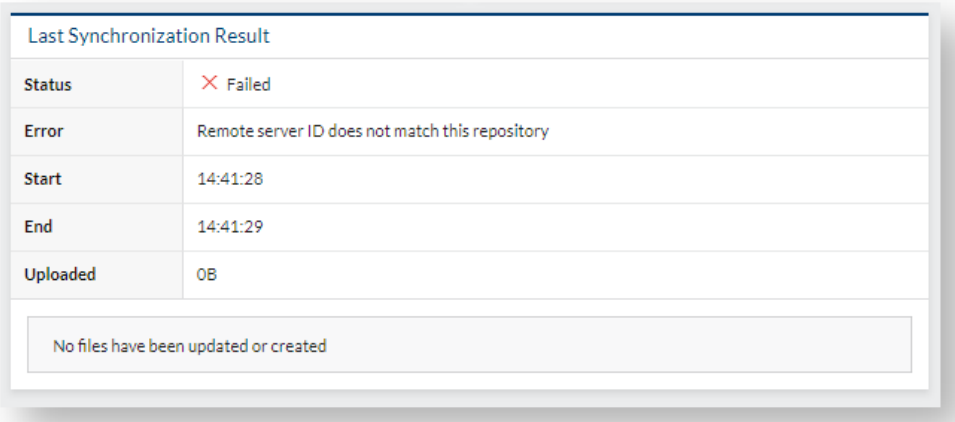
Full Backup Files are Synchronized When Creating Incremental Backups

The remote synchronization process uploads any new or changed backups. As this works at a file level, a change to a full backup caused by the ***Create Synthetic Fulls*** option in the a backup schedule will cause the full image file to be re-uploaded. It is recommended to avoid this option if the amount of data uploaded is a problem.

Remote Server ID mismatch



Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



Sometimes a remote sync connection or sync attempt will fail the error **Remote server ID does not match this repository**. This error means that the local repository's unique ID does not match the one recorded on the server for this sync. This can have many causes:

- **An error on the Repository** - If the ID file is deleted from the repository, a new ID will be generated. If this happens the remote sync is stopped to prevent local repository data with errors from overwriting the remote copy
- **Multiple Repositories syncing to the same server** - if multiple repositories sync to the same server and path, the one which connects first and writes their unique ID file to the server will own it and sync to it. The other repository will generate an error instead. This prevents multiple repositories from overwriting each others data.
- **Server space is being reused for a different Repository** - If a Site Manager server is moved or the remote sync destination has old Site Manager sync data, there may be an ID error generated because the remote sync server still has the ID from the old Repository.

If the ID mismatch has been caused by old data or is otherwise not relevant, the Repository can write a new ID file to the remote server and take it over by using the **Reinitialize** option. This will update the ID file and allow the remote sync to proceed.

Remote Synchronization with Amazon S3 or Other Compatible Stores

- Overview
- S3 Store Configuration
  - Buckets
  - Regions
- Authorisation
  - IAM
  - Policies
- Service Billing

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Overview

Site Manager can automatically synchronize all backups stored in a Repository to Amazon S3 or other compatible stores like Wasabi or Backblaze. This article covers key aspects specific to S3 that should be understood and managed before remote synchronization with S3 can operate. For an overview of remote synchronization and how to configure it (including S3 configuration) see this article.

S3 Store Configuration

Buckets

A bucket is the first layer of storing file objects within an S3 store, it must be created and configured before attempting to connect Site Manager to S3. This can generally be done in the S3 service providers user console. Some of the possible options include region selection, object versioning/retention policies and storage encryption.

Regions

Regions select the specific servers that will be used to store the file objects and are entirely subjective to the user.

Authorisation

IAM

IAM users and groups are a fundamental part of Amazon S3 that can be used to produce managed access to an S3 bucket, the IAM user assigned to remote synchronization must have a valid access key and secret key to establish a connection with Site Manager. Other compatible stores may not use the same exact key terms, but should provide a similar interface to acquire the access key and secret key to the user account.

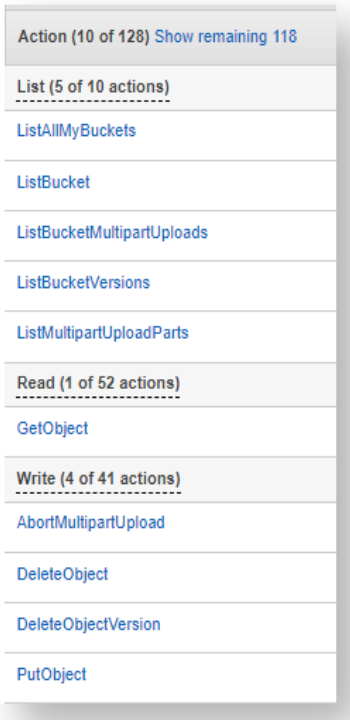
Policies

Policies are another fundamental part of Amazon S3 that allow specific S3 actions to be bundled together and applied to an IAM user/group account. Other compatible stores may not use the same exact key terms and in most cases the service provider will have similar policy options, but some may be limited with this level of policy selection. The minimum required policy actions for remote synchronization to operate with S3 are included below:

Category	Permission
List	ListAllMyBuckets, ListBucket, ListBucketMultipartUploads, ListBucketVersions and ListMultipartUploadParts
Read	GetObject
Write	AbortMultipartUpload, DeleteObject, DeleteObjectVersion and PutObject ⓘ DeleteObjectVersion is optional if bucket versioning is **not** used

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Amazon S3 Example:



Service Billing

S3 object storage services generally incorporate a billing policy based on various forms of usage like disk space, transfers, server-side operations and deletion to name but a few. Billing policies vary greatly between different service providers and should be closely reviewed to avoid unexpected costs from your selected provider.

Where possible, remote synchronisation to an S3 store will be performed in an as efficient manner as possible, but due to some necessary remote synchronization procedures, temporary objects and temporary server-side object duplication is often required and may result in additional charges depending on the service providers billing policies.

Monitoring and Management Tools

Macrium Site Manager contains a number of tools for monitoring and managing a backup deployment on an ongoing basis. These tools, with notes on how to use and interpret the data provided are documented here. Available tools are:

- Backup Logs - Detailed logs from all backups of Site Manager are collated in Site Manager so any backups can be examined in detail and any failures diagnosed.
- Event Logs - Actions in Site Manager are logged in an event log so that they can be audited and reviewed.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

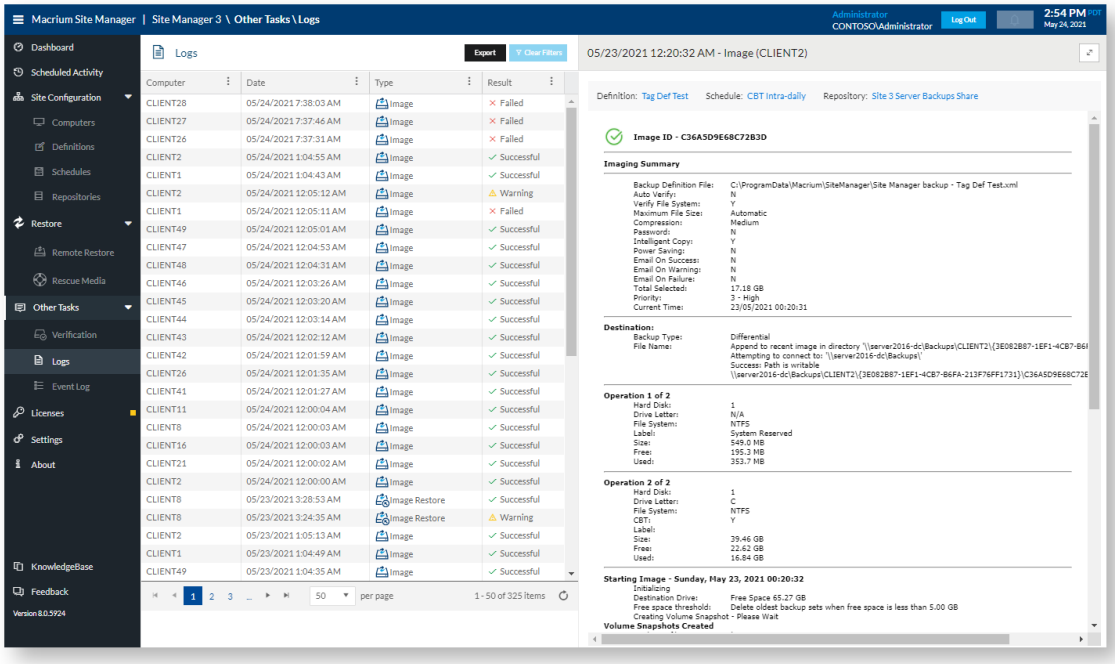
Reviewing Backup Logs

All remote backup logs are stored centrally for review. To access the logs, follow these steps:

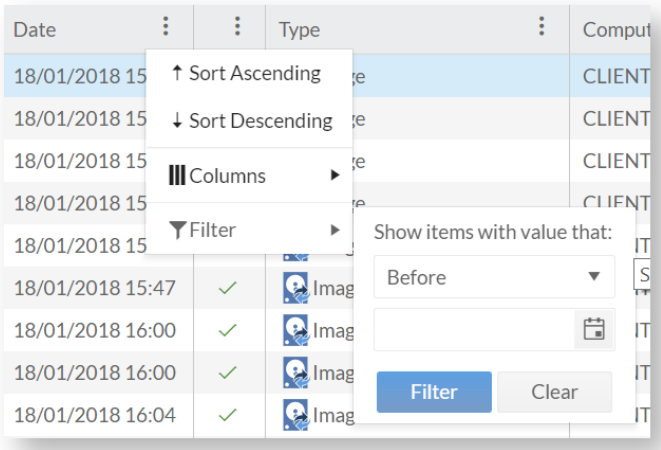
Viewing Backup Logs

Click '**View Logs**' under '**Other Tasks**' on the main console view.

The log view can be sorted by clicking the column headings in the log list.



The columns can also be filtered by selecting the dropdown menu on the column selecting the appropriate filter option.

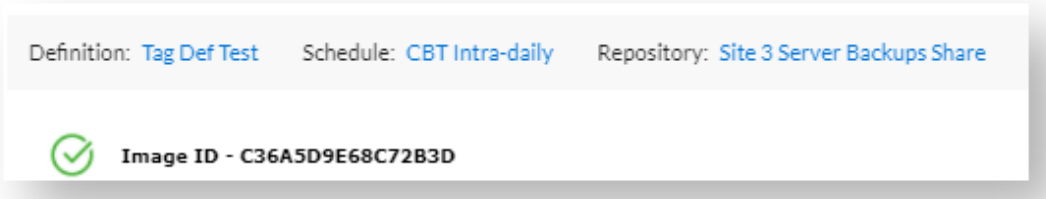


Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

The 'Date' column can be filtered by logs either before, on or after a given date. Other columns can be filtered by matching computer names or have a selection of types to include in the list.

Filters can be reset using the **Clear Filters** button at the top of the page.

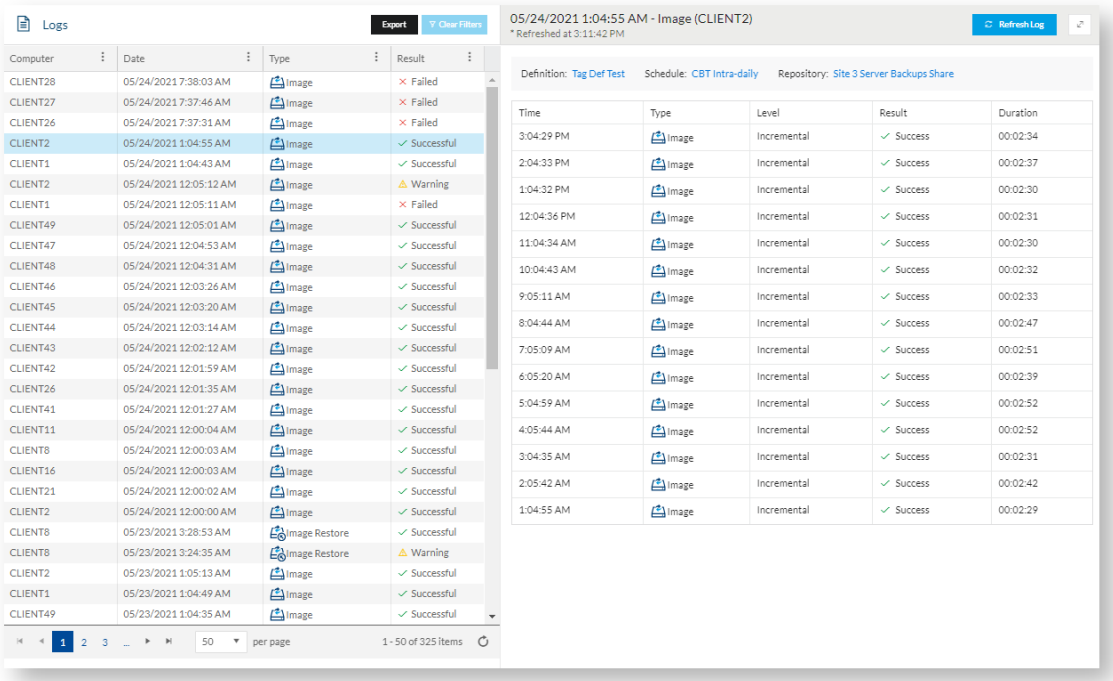
To view a log, click on the row in the table and the log will be loaded into the right hand side of the screen. There is also an expansion button in the top right of the log view for maximizing the log. If the log is from a Site Manager scheduled backup, there will be links to the appropriate definition, schedule and repository at the top of the log:



Note that these links may not be present if the Definition, Schedule or Repository has been deleted from Site Manager since the backup occurred.

Intra-Daily Backups

When scheduled backups are taken with an Intra-daily schedule which has the **Intra-daily Stealth** option set, normal logs are not created except in cases of backup error or warning. Instead, each computer has an intra-daily log for the day, with the backup times and results for that day. Each Computer and Backup Definition pair will be in a separate daily log.



Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Exporting Backup Logs

Backup log information may be exported in CSV format in order to help analysis and auditing tools. Clicking the **Export** button will download a CSV file in the browser containing the information from the log list. This data can be imported into any tool which can work with CSV data, such as Excel.

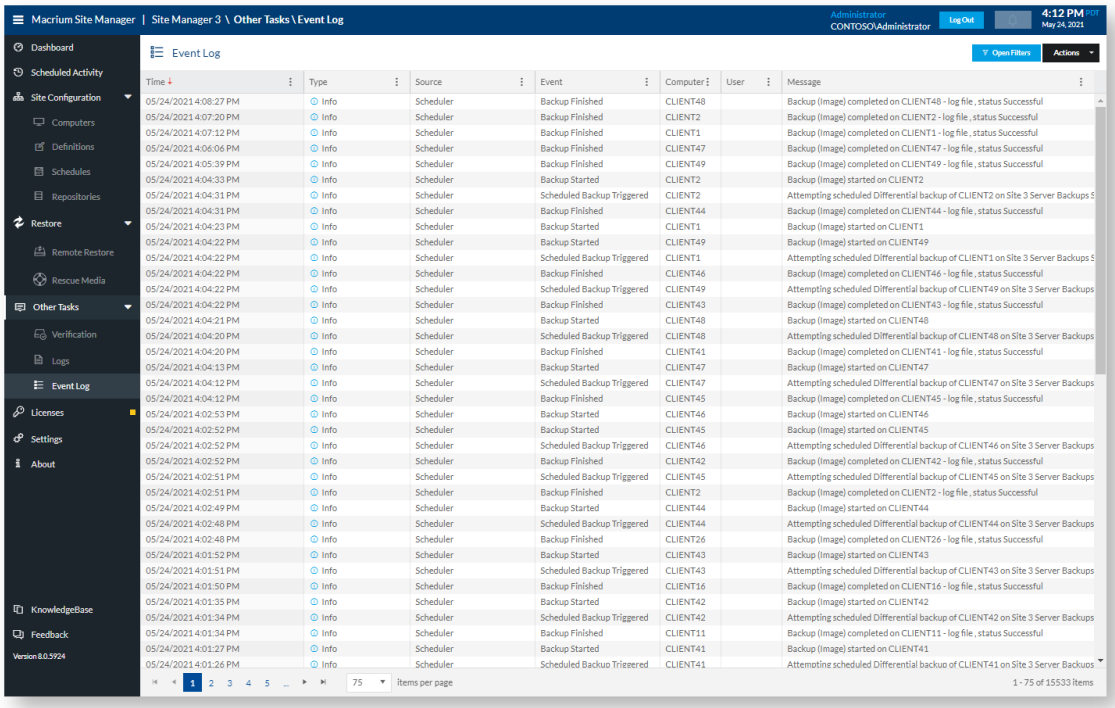
Reviewing Event Logs

All actions which have been taken by Site Manager or by users in the console are logged in the Event Log, This allows administrators to review activity for auditing, security or reporting purposes.

Viewing Event Logs

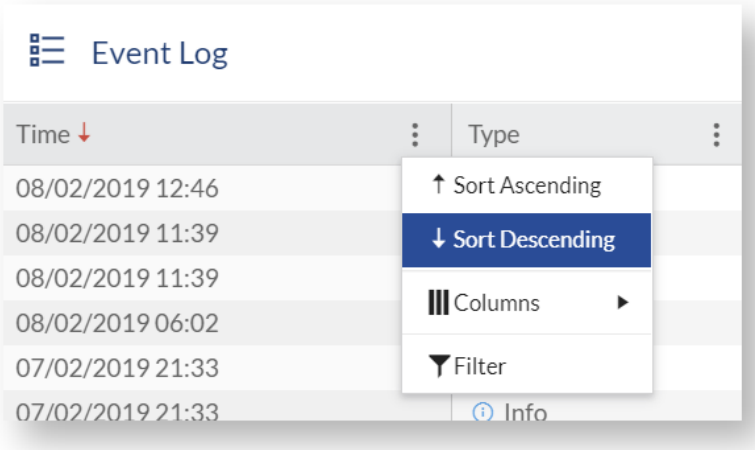
To view the event logs, follow the steps below:

Click '**View Event Logs**' under '**Other Tasks**' on the main Site Manager interface. The Event Log page will be shown as below:

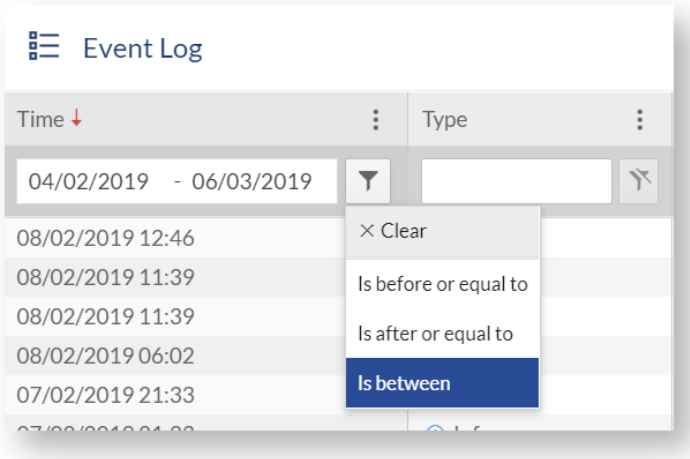


To sort the event log, click on column heading you want to sort by (multiple clicks will cycle through ascending, descending and unsorted) or click the dropdown menu on the right hand side of a column heading and select the appropriate sort option.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



To filter, select any column heading and click **Filter**. This will display the filter bar below the headings:



To apply a filter, click the edit box under the column to be filtered and select the appropriate option. The filter button to the right of the edit box allows clearing the filter or selecting between different filter types where available.

Event Log Columns

The Event Log table has columns as follows:

Column Name	Description
Time	The date and time when the event was logged.
Type	The 'Type' column indicates the severity of the event. The types are: • Info - A normal event in the operation of the Management Console • Warning - Something unusual which may indicate a problem or unusual operation

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Column Name	Description
	• Error - A failure of some sort which may require investigation
Source	There are a number of different sources for each event. These sources show which part of the system the event originated from and filtering on source may be useful to show related events from the same area
Event	The event which has occurred. A full list is available below
Computer	If the event is associated with a computer, the NetBIOS name of the computer will be shown here.
User	If the event was initiated by a user, the user's login name will be shown here.
Message	This contains the message detail for the event. The message can vary depending on whether the event is a success or failure event. For example, a 'Backup End' event may show additional error information for a failed backup over a successful one.

Event Log Sources

The available Event Log sources are listed below:

Event Log Source Name	Description
System	Events from the server which is running Site Manager such as startup and shutdown events from the Windows service running Site Manager.
Logon	Events relating to user login/logout of sessions
Settings	Changes to any of the items in Site Manager settings
Update	Notifications of new Site Manager software versions
Licenses	Upgrade, Addition and removal of Macrium Agent License keys, warnings for problems with client licensing
Computers	Additional and removal of managed computers, online/offline status notifications
Backup Definitions	Changes to Backup Definitions

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Event Log Source Name	Description
Schedules	Changes to Schedules
Repository	Changes to Repositories
Scheduler	Events from the internal scheduling of backups by repositories including backup scheduling, start and end.
Reflect	Backup and restore events initiated from an individual computer's installation of Macrium Reflect rather than centrally
Dashboard	Events triggered from user interaction with the Dashboard page
Restore	Events from Site Manager triggered restore operations
Agent	Errors and notifications from Agents running on managed computers
Backup	Events from Site Manager triggered backup operations
Verification	Events from Site Manager triggered verification operations
Image File Browser	Events triggered by browsing image files in the repository page
Rescue	Events relating to Rescue Media generation

Event Log Events

The list of possible events and useful information that may be logged us shown below. Note that if relevant, all events will contain a username and/or computer NetBIOS:

Event Log Event	Description	Data available
Startup	The Site Manager service has started up	Site Manager version
Shutdown	The Site Manager service has been requested to stop	
User Login	A user has logged in.	

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Event Log Event	Description	Data available
		Username, IP address
User Logout	A user has logged out	Username
Security Settings Changed	The security settings were changed by a user	
Slack Settings Changed	The Slack settings were changed by a user	
Notification Settings Changed	The Notification settings were changed by a user	
Update Available	An update to the Management console is available	New Software Version
Update Installed	The Site Manager has started with a new version	Old and new software version numbers
License Key Added	A License Key has been added as a Client Access License	License key and number of seats
License Key Removed	A License Key has been removed	License key
Unlicensed Computers	One or more computers cannot be accessed by Site Manager due to licensing issues	Number of affected computers
Computer Added	A computer has been added to Site Manager	Computer NetBIOS
Computer Removed	A computer has been removed from Site Manager	Computer NetBIOS
Agent Remotely Installed	Site Manager has attempted remote installation of an Agent	

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Event Log Event	Description	Data available
		Computer NetBIOS affected, install success, error messages
Agent Patched	The automatic Agent patching has pushed a patch to a remote Agent	Computer NetBIOS, patch name
Repeat Last Backup	The Repeat Last Backup function has been used to trigger a backup	Computer NetBIOS
Set Passphrase	The Passphrase for a computer has been changed on the server	Computer NetBIOS, passphrase
Agent Updated	A remote Agent is now running a new version of the Agent software	Old and new versions
Backup Definition Created	A new Backup Definition was created	Backup Definition name
Backup Definition Removed	A Backup Definition was removed	Backup Definition name
Backup Definition Updated	A Backup Definition was edited and updated	Backup Definition name
Schedule Created	A new Schedule was created	Schedule name
Schedule Removed	A Schedule was removed	Schedule name
Schedule Updated	A Schedule was edited and updated	Schedule name
Repository Created	A new Repository was created	Repository path

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Event Log Event	Description	Data available
Repository Removed	A Repository was removed	Repository path
Repository Updated	A Repository was edited and updated	Repository path
Repository Offline	The server lost contact with a Repository	Repository path
Scheduled Backup Added	Backups have been scheduled in a Repository	Repository path, Backup Definition name, Schedule name
Scheduled Backup Removed	Scheduled backups have been removed from a Repository	Repository path, Backup Definition name, Schedule name
Scheduled Backup Active	A scheduled backup has been set as active on a Repository	Repository path, Backup Definition name, Schedule name
Scheduled Backup Stopped	A scheduled backup has been stopped on a Repository	Repository path, Backup Definition name, Schedule name
Scheduled Backup Triggered	Scheduled backups have triggered a backup to start on a managed computer	Computer NetBIOS, Repository path, Backup Definition name, Schedule name
Backup Started	A backup has started or failed to start on a managed computer	Computer NetBIOS, error information
Backup Finished	A backup has finished or failed on a managed computer	Computer NetBIOS, error information, log file name

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Event Log Event	Description	Data available
Restore Started	A restore has started or failed to start on a managed computer	Computer NetBIOS, error information
Restore Finished	A restore has finished or failed on a managed computer	Computer NetBIOS, error information, log file name
Clone Started	A clone operation has started or failed to start on a managed computer	Computer NetBIOS, error information
Clone Finished	A clone operation has finished or failed on a managed computer	Computer NetBIOS, error information, log file name
Backup Paused	A backup has been paused from the Site Manager interface	Computer NetBIOS
Backup Cancelled	A backup has been cancelled from the Site Manager interface	Computer NetBIOS
Session Start	A web session to Site Manager has been started	IP Address
Session End	A web session to Site Manager has closed. ⓘ The session will be closed by the server some time after the user has closed their web browser. This can be up to 10 minutes	
Restore Requested	A restore operation has been requested through Site Manager	Computer NetBIOS, image file name
Message Response	A request to an Agent has failed.	Computer NetBIOS, message type, error
Agent Status Changed	A managed computer has changed online status	Computer NetBIOS, Online or offline
Backup Requested	A backup operation has been requested through Site Manager	Computer NetBIOS

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Event Log Event	Description	Data available
Verification Started	A backup file verification operation has started	Backup file name and path
Verification Finished	A backup filed verification operation has finished	Backup file name and path, success, error
Home Edition Agent Limit Reached	The number of Home Edition standalone licensed clients has exceeded the limit (4).	Number of Home Edition clients, whether excess clients are using MALs
Email Settings Changed	The Email settings were changed by a user	
System Settings Changed	The System settings were changed by a user	
Agent Settings Changed	Agent section of the settings page has been changed	
Rescue Media Settings Changed	The Rescue Media section of settings was changed by a user	
Network Settings Changed	The Network section of settings was changed by a user	
Daily Export Settings Changed	The Daily Data Export section of settings was changed by a user	
Email Notification	An email notification has been sent or failed to send	Email recipient, authentication type, error
		Computer NetBIOS

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Event Log Event	Description	Data available
Agent Passphrase Remote Update	The secure passphrase on a remote agent has been updated. This occurs when advanced agent security is set in settings and an agent has been connected for the first time or the global passphrase has been set on the Site Manager server	
Remote Management Settings Changed	The Remote Management settings were changed by a user	
Macrium Agent License Key Upgraded	A MAL has been upgraded. This may occur when a version 6 key is upgraded to version 7 when added to Site Manager.	Old and new keys
Standalone Reflect License Key Upgraded	A client computer with a standalone Macrium Reflect install has had the Reflect license key upgraded by the Site Manager. This occurs when the user requests an upgrade from a Reflect version 6 to a Reflect version 7 key.	Computer NetBIOS, old and new license keys
File Downloaded	A file has been downloaded by opening an image file in the Repository browser and downloaded	Image file, Downloaded file
Remote Synchronization Started	A Repository has started to sync to a remote server	Repository, remote server
Remote Synchronization Completed	A Repository has completed a sync to a remote server	Repository, remote server, error if appropriate
Run Now Remote Synchronization Triggered	A user has requested that a manual remote synchronization should be started	Repository, remote server
Remote Synchronization Reinitialized	A user has reinitialized a remote server so that it can be used as a target for remote synchronization	Repository, remote server
	User has cancelled a running remote synchronization through the Site Manager user interface	Repository, remote server

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Event Log Event	Description	Data available
Remote Synchronization Cancelled		
Configuration Import	A configuration backup has been imported into Site Manager through the settings page **Load Configuration** option	
Event Log Cleared	The Event Log was cleared by a user	
Provider Deleted	A Login Provider has been deleted by a user	Provider name
Provider Created	A Login Provider has been created by a user	Provider name
Provider Configured	A Login Provider has been edited by a user	Provider name, success or failure
Permissions Modified	Login Provider permissions have been changed by a user	Provider name, success or failure
Agent Migration Start	A migration of an Agent from this Site Manager to another has started	Agent name, destination Site Manager details
Agent Migration End	A migration of an Agent from this Site Manager to another has completed	Agent name, success or failure
Server Connection Settings Changed	The network configuration of the Site Manager server connection has been changed	New configuration details
Agent Manual Upgrade	An Agent has been queued for upgrade by a user	Agent name
Backup Warning	A non-fatal warning about a backup has been generated	

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

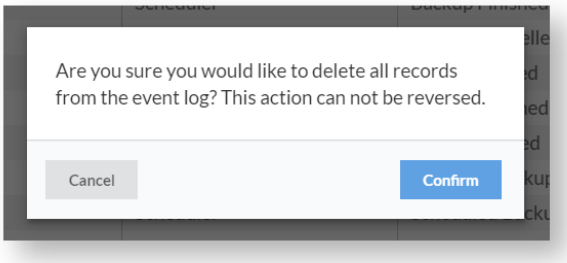
Event Log Event	Description	Data available
Rescue Media Build Started	A Rescue Media build has been started	Rescue Media type
Rescue Media Build Succeeded	A Rescue Media build has succeeded	Rescue Media type
Rescue Media Deleted	A Rescue Media image file was deleted	Rescue Media type
Rescue Media Build Cancelled	A Rescue Media build was cancelled	Rescue Media type
Purged Logs	Event Logs or Backup Logs have been purged due to age	Number of log entries purged
Restore Preparation Failed	An error happened while preparing for a remote restore - this can be related to the backup itself or the PE rescue environment	Error
Cancel Backup Request	A **Run Now** backup was cancelled from the forecast.	Computer, Definition and backup type
Permissions Granted	A user or group has been granted access to Site Manager	User or group name
Permissions Revoked	A user or group has had access revoked from Site Manager	User or group name
Configuration File Load Error	A Site Manager configuration file has failed to load. A copy has been made of the failed file for backup and support purposes	The file that failed to load

Clearing the Event Log

To remove any unwanted log entries such as from early testing of a deployment before going live, the Event Log can be cleared. This will remove all entries. Once the Event Log has been cleared, a single **Event Log Cleared** event is logged.

To clear the Event Log, press the **Clear** button above the top right of the Event Log table:

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



Exporting the Event Log

The Event Log can be exported as a CSV file to allow analysis or archiving off the Site Manager Server. To export the Event Log, press the **Export** button above the top right of the Event Log table. A CSV will be downloaded which can be imported into other systems:

	A	B	C	D	E	
1	Event Time	Event Source	Event Type	Event	User	Comput
2	08/02/2019 12:46	Logon	Info	User Login	Administrator	
3	08/02/2019 11:39	System	Info	Session End	Administrator	
4	08/02/2019 11:39	Logon	Info	User Logout	Administrator	
5	08/02/2019 06:02	System	Info	Session Start		
6	07/02/2019 21:33	System	Info	Session End	Administrator	
7	07/02/2019 21:33	Logon	Info	User Logout	Administrator	
8	07/02/2019 17:21	Scheduler	Info	Backup Finished		CLIENT1
9	07/02/2019 16:59	Scheduler	Info	Backup Started		CLIENT1
10	07/02/2019 16:59	Scheduler	Info	Run Now Backup Triggered		CLIENT1
11	07/02/2019 16:41	Computers	Info	Agent Status Changed		CLIENT1
12	07/02/2019 16:39	Computers	Info	Agent Status Changed		CLIENT1
13	07/02/2019 16:38	Scheduler	Warning	Backup Finished		CLIENT4
14	07/02/2019 16:38	Dashboard	Info	Backup Cancelled	Administrator	CLIENT4
15	07/02/2019 16:38	Dashboard	Info	Backup Paused	Administrator	CLIENT4
16	07/02/2019 16:22	Scheduler	Error	Backup Finished		CLIENT1

Automatically Purging the Event Log

The Event Log can be configured to automatically purge any entries older than a specified number of days. This can be configured in the **System** section of **Settings** - see Configuration and Security for details.

Events will be deleted at midnight, with **Purged Logs** events being created when Event Logs or Backup Logs are purged.

Managing and Restoring Backups

Once backups have been created and stored in a repository, Site Manager provides tools to manipulate these backups and restore them. The options available are:

- Restoring an Image through Site Manager - How to use the restore functionality of Site Manager to remotely restore an image
- Restoring an Image Through Macrium Reflect - How to open images in standalone Macrium Reflect or the Site Manager Agent and how to decode the repository file structure
- Verifying Images - How to verify the integrity of image files in a repository

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

- Synchronizing a Repository with a Remote Server - How to set up automatic remote synchronization between a Site Manager Repository and a remote server
- Creating Rescue Media - How to create rescue media to be used in bare metal restore scenarios.

Restoring an Image through Site Manager

- Introduction
- Advanced Restores
- Restoring an Image using Site Manager
  - Selecting a Computer
  - Selecting an Image File to Restore
  - Selecting Restore Options
  - Reviewing the Restore and Finishing
  - Viewing a Restore Progress

Introduction

Site Manager allows image backups to be restored to the managed computer they were taken from without leaving the Site Manager interface. This process is designed for simple restore activity with the following features:

- Non system partitions will be restored without restarting the client computer.
- System partitions will be restored by restarting the client computer in Windows RE (if available) or Windows PE.
  Note: If required, the Windows PE Component files will first be automatically copied to the client PC and the recovery boot menu added. The restore will then automatically be continued in the PE rescue environment.
- Full progress of the restore is shown in the dashboard 'Activity' widget. This includes restorations running in Windows PE.
- A configurable restoration alert message dialog can optionally be shown on the client computer.
- Users logged on to the client computer can optionally cancel the restore operation.

Advanced Restores

To restore a computer which is not online in Site Manager or requires options not available in the Site Manager restore, see the Restoring an Image Through Macrium Reflect.

Site Manager will copy user-supplied drivers from the server to the target agent immediately before the restore so that the recovery environment supports agent hardware. Drivers to be copied should be placed in the Rescue Media Working Directory generic drivers folder appropriate for the operating system of the target agent. Use the table below to determine the right path:

Operating System of Target Agent	CPU Size	Subfolder Name
Windows Vista or later	64-bit	**PE10x64**

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

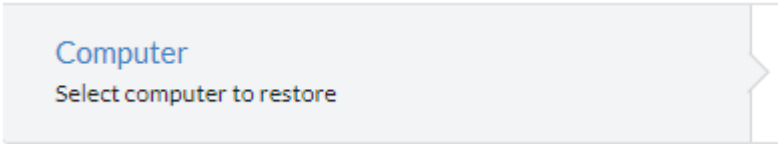
Operating System of Target Agent	CPU Size	Subfolder Name
Windows Vista or later	32-bit	**PE10x86**
Windows XP or Windows 7	64-bit	**PE3x64**
Windows XP or Windows 7	32-bit	**PE3x86**

For example, drivers to be used during restores of 64-bit Windows 10 machines should be placed in **workingDirectory\drivers\PE10x64** where **workingDirectory** is the Rescue Media Working Directory as specified in the Rescue Media settings. These folders will need to be created manually.

Restoring an Image using Site Manager

The Site Manager restore process is a wizard driven process with a number of stages. These are:

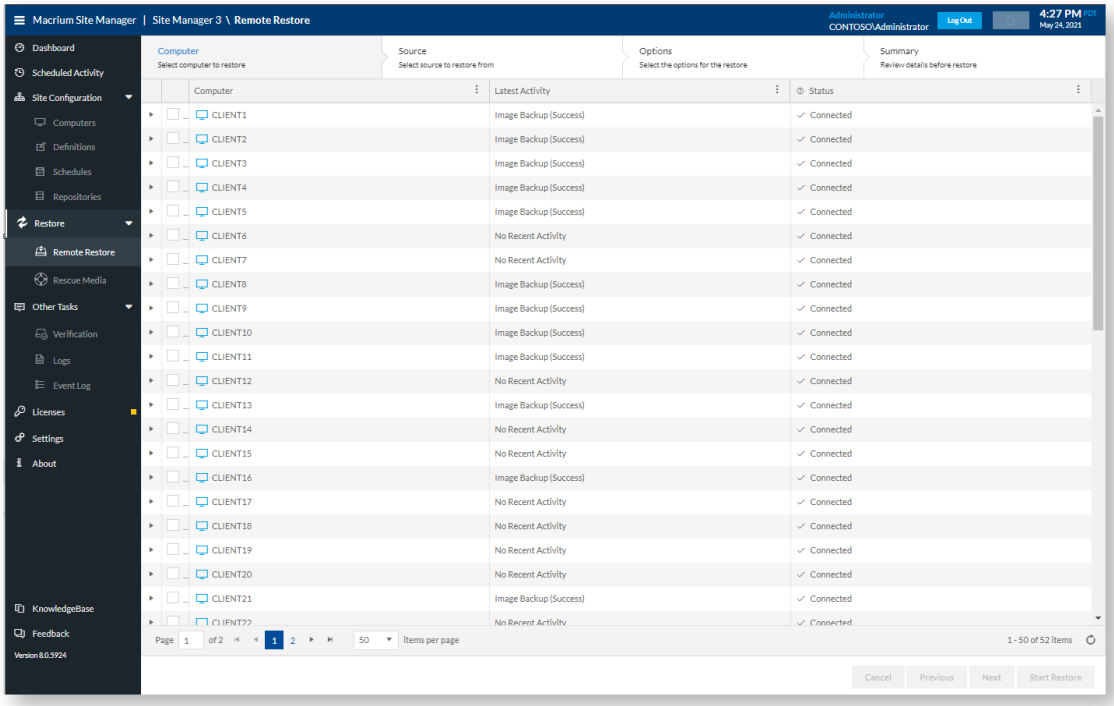
Selecting a Computer



Select the 'Restore' side menu and select a computer to restore.

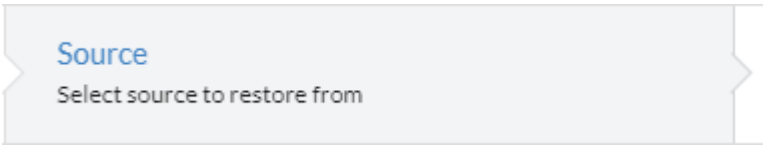
Note: Only one PC can be restored at a time

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



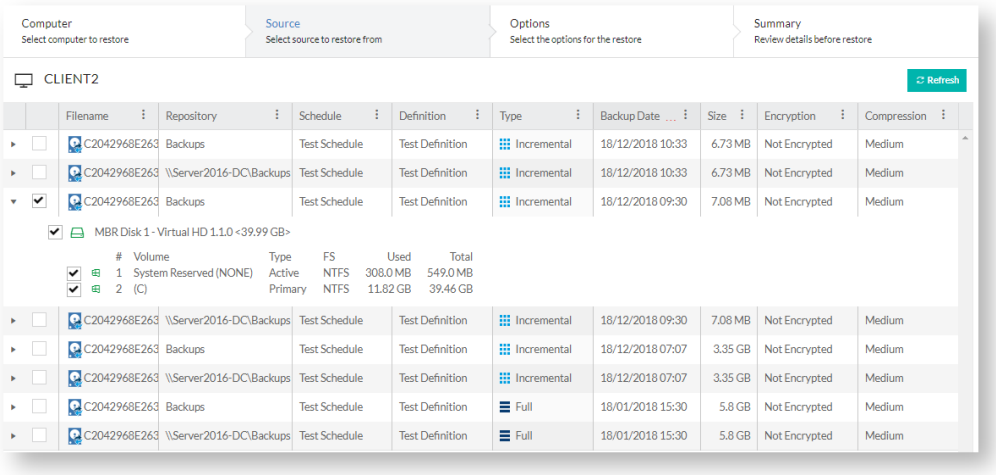
Click 'Next' to display a list of images found in repositories for the selected computer. Selecting an image file will display the Disk(s) and Partition(s) in the image file.

Selecting an Image File to Restore



Note: You can only restore one disk at a time, but you can select one or many partitions on each disk.

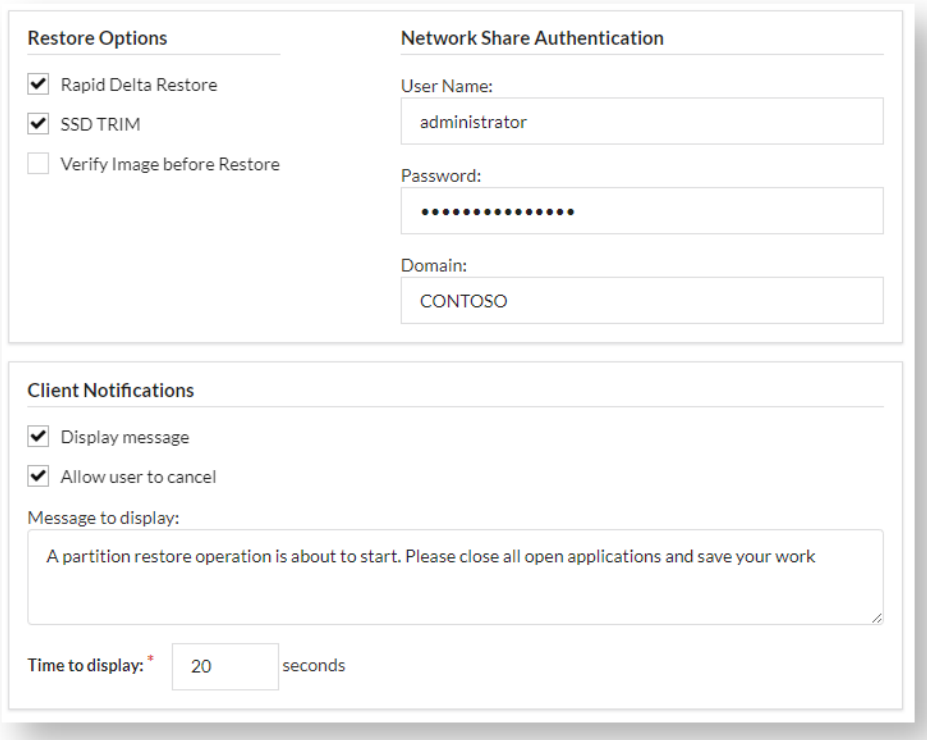
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



Select the partition(s) to restore and **click Next.**

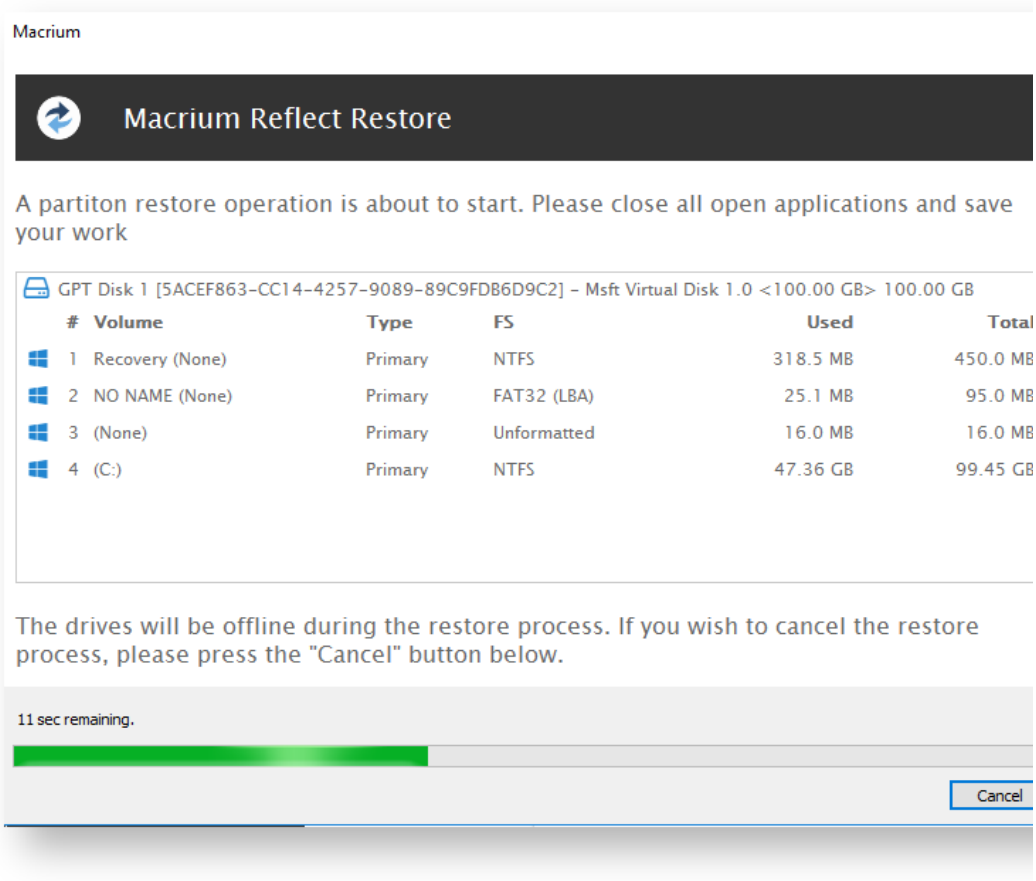
Selecting Restore Options

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



Option	Description
Rapid Delta restore	Only changed blocks are restored and the restore completes much faster with this option selected.
SSD TRIM	Affects restore operations to SSD only. Reflect can flag all unused blocks using the TRIM operation. Writing to an unused block is much qu block as it avoids both the slow erase operation and the read-modify-write cycle. This results an inc lifetime and the performance of the device. It is effective for all Windows operating systems, even those that support SSD trim as the file syster blocks on de-allocation; it cannot TRIM blocks written by another process. It is also effective for USI
Verify image before restore	Perform a full image verification prior to starting the restore process. If any corruption is found in the then the restore will be aborted. **Note:** Selecting this option with increase the restore time considerably.
	Enter any authentication details to enable the computer being restored to access the image file netv be pre-populated with the authentication information saved in the repository configuration.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

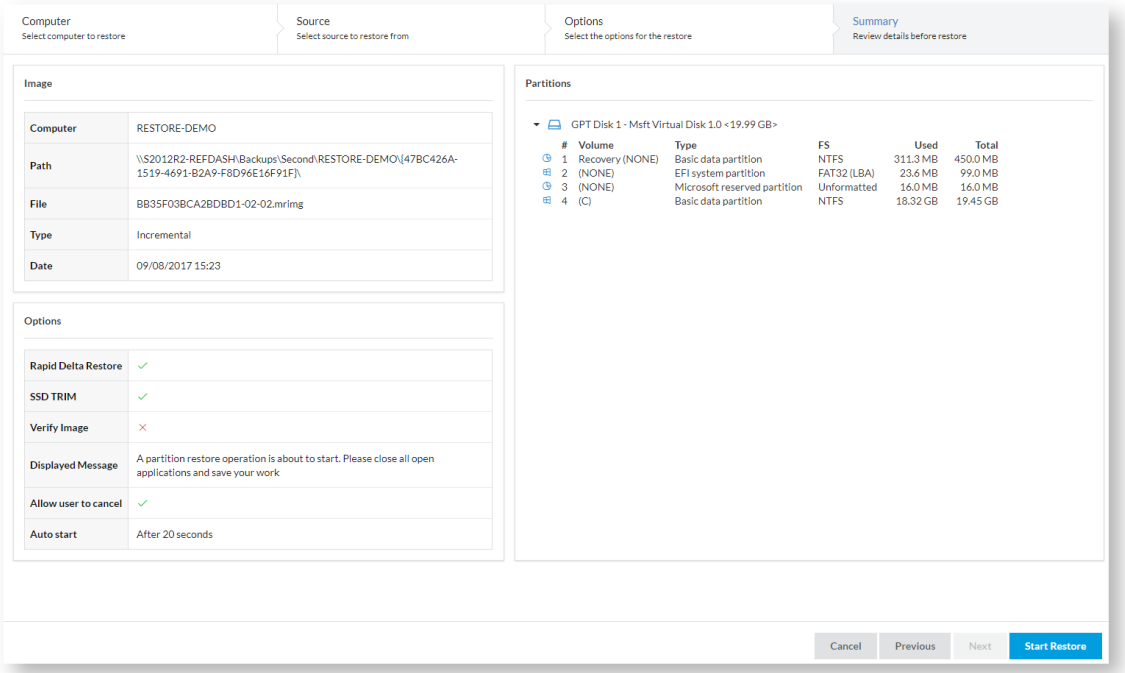
Option	Description
Network Share Authentication	
Display Message	When enabled, a message dialog is displayed to inform the client user(s) that a restore operation is dialog includes a list of the partitions being restored together with custom message text. Example restore message dialog... 
Allow user to cancel	When enabled, the restore can be cancelled by the client logged in user.
Message to display	The text to be display in the message dialog.
Seconds to display	The number of seconds to display the client message dialog.

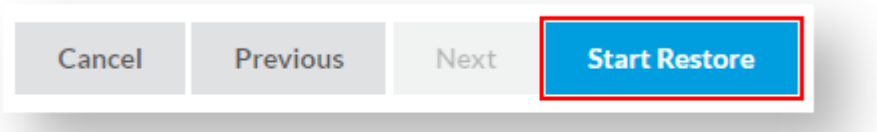
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Enter/Select the restore options and **click Next**

Reviewing the Restore and Finishing

A summary of the restore selections and options is displayed. Confirm everything is OK and **click 'Start Restore'**

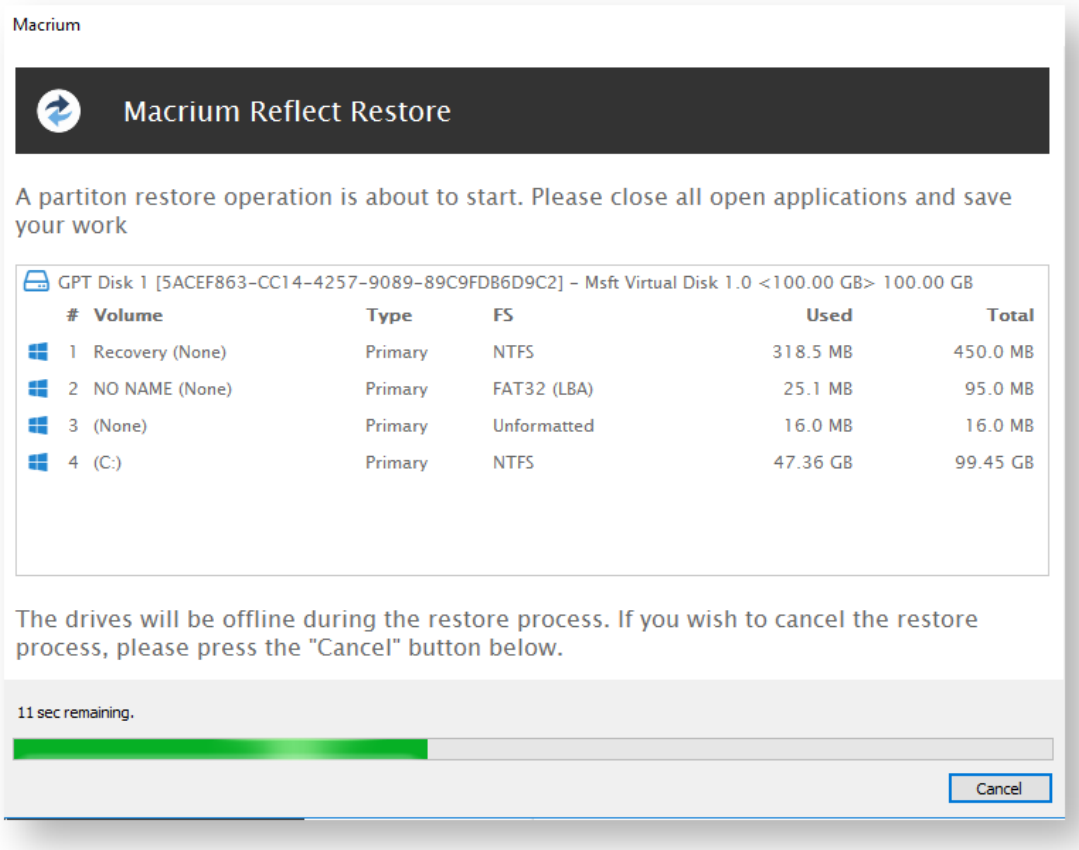




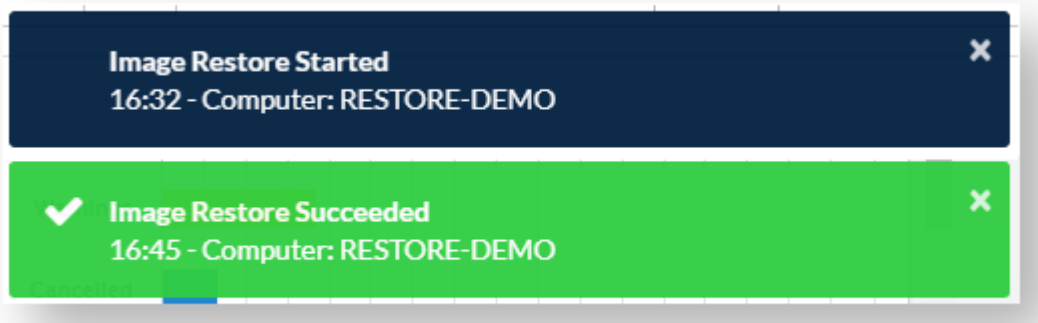
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Viewing a Restore Progress

The Restore starts and a message dialog is displayed on the client computer (if the **Allow user to cancel** option has been selected)



In Site Manager, notifications indicate the success of the restore request and initialization.



The message countdown and restore can be monitored in the dashboard **Activity** widget.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Manual Restore Options

A restore within Macrium Site Manager performs a simple restore of data in the image file with few advanced options. This is good for performing a quick restore, but if more complex restore operations are required, the image files created by Macrium Site Manager can be viewed and restored by either a standalone installation of Macrium Reflect or by the Macrium Agent itself.

Opening images in this way allows the following:

- Restore to dissimilar hardware
- Restore by rescue media
- Browsing image files for file-level access
- Creating VHD files or VMs

See Macrium Reflect - Restoring and Browsing Images for more details.

Finding Images in a Repository

The repository folder structure is automatically created as needed. It follows this pattern:

```
<Repository root path>\<Computer name>\<Definition ID>\ImageFile.mrimg
```

Where **Computer Name** is the NetBIOS name of a computer in Site Manager and **Definition ID** is an ID number corresponding to a Backup Definition. Inside that folder are image files. All image files created for a computer using a backup definition go in the same folder, even if they were performed with a different schedule or using a **Run Now** backup.

To translate the backup definition ID into a backup definition name, the Site Manager creates an information file in the top level of the repository. This file is called **Macrium Repository Information.txt**

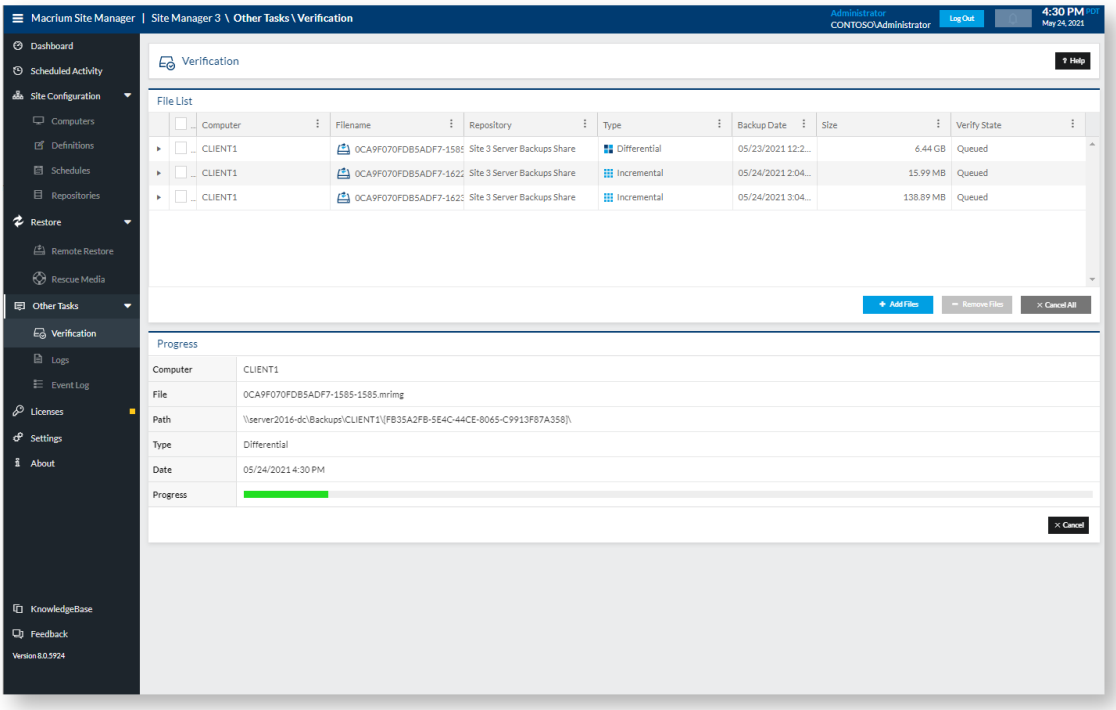
```
Macrium Repository - v1
This file lists folder names associated with Backup Definitions - Centrally
scheduled backups are stored in <NETBIOS>\<BACKUP DEFINITION ID> folders.
{A7D12C32-10DD-48D1-BE06-EF0E9412480A} - Sales Team
{96D60D41-B0D9-4FF4-B562-BBF11F4290F8} - Support Team
{8A25D491-5DE7-41AE-9E91-AEDD51304A42} - Server Backups
{8CABEE54-267F-481D-BD18-55ECA7E1E80F} - this office
{8E6FB6D3-F8B7-432E-BBBC-1D188702D23A} - Servers
```

This lists all backup definition IDs and links them to the name of backup definitions. The reason this is done is so that changing a backup definition name doesn't cause the repository layout to change or a backup set to break because it's stored in a different folder

If a backup definition has been deleted, it will be removed from the information file but the folders and image files will remain in the repository. If you find a backup definition ID without a name in the information file, this is most likely a deleted definition

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Verifying Images



The Verification page allows image files which have been backed up to any of the repositories to be checked to ensure file integrity and detect any data errors which may have occurred in storage.

Rescue Media

- Introduction
- Rescue Media Types
    - Agent Rescue Media
    - Generic Rescue Media
    - Universal Rescue Media
- Windows PE
    - Creating Rescue Media Offline
- Managing Rescue Media
    - Rescue Media Working Directory
    - Drivers
    - Creating Rescue Media
    - Using Rescue Media
- Rescue USB Tool

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Introduction

Rescue Media are live discs or USB sticks from which computers can boot directly into the Macrium Rescue Environment. This is a lightweight version of Windows (the Windows Preinstallation Environment or Windows PE) customised to include Reflect so users can manually recover computers which cannot boot Windows normally. Such computers are unable to run the Site Manager Agent; consequently, they can not be restored remotely.

Site Manager can create Rescue Media which can be downloaded through the Site Manager interface; giving users easy access to a centralized source of Rescue Media to recover failed agents.

Site Manager can create generic Rescue Media or Rescue Media which is targeted for a managed computer. Generic Rescue Media only contain the Macrium Rescue Environment and will be compatible with most machines with dynamic network settings. Agent Rescue Media includes driver and network information from the agent; it should be used for computers with static network settings or hardware not supported by Windows PE.

For advanced needs, use a copy of Reflect on a managed computer or the Site Manager server to create Rescue Media manually. See Restoring an Image Through Macrium Reflect for further information.

Rescue Media Types

Agent Rescue Media

Site Manager can create Rescue Media which is custom built for a particular agent to minimise the manual configuration required to restore it. Agent Rescue Media will be based off the right version of Windows PE for the target agent and contain copies of hardware drivers for devices which the agent detects as being unsupported by Windows PE. These devices can then be used in the Rescue Environment even if they are not supported in Windows PE by default. An up-to-date set of agent drivers are stored on a database on the Site Manager so that Agent Rescue Media can be created for failed agents at the time of need.

Agent network configurations are also stored in the Rescue Media so that the backup repository can be easily accessed through the Rescue Environment. Note that network settings must be configured manually within the Rescue Environment if the agent is restored to different hardware as network configurations are associated with a MAC address.

Generic Rescue Media

Site Manager can also create Generic Rescue Media which does not target any single agent. These media will not include any extra drivers but users can manually specify drivers to be included in Rescue Media for a given Windows PE configuration (see below). Such rescue media will be appropriate for use on agents with common hardware configuration.

Network settings for all agents are stored in Generic Rescue Media. Appropriate network settings are selected when an agent boot the Rescue Environment from the Rescue Media. Note that network configuration selection is determined by MAC address so network settings may not be configured automatically if agent hardware has changed.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Universal Rescue Media

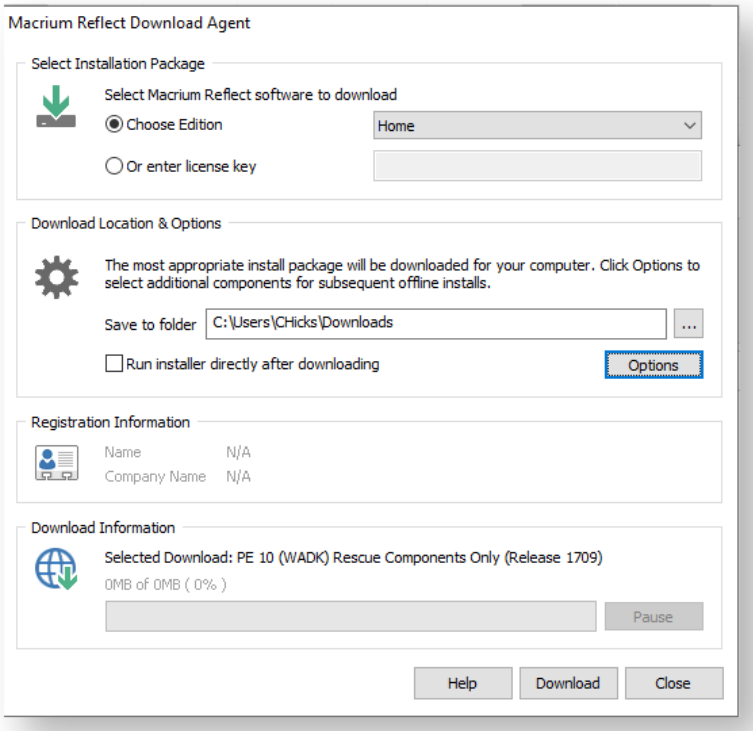
Universal rescue media contain all versions of Generic Rescue Media on a single bootable disk. This can be used to restore groups of computers which run different versions of Windows without creating the necessary Generic Rescue Media individually. Drivers for generic rescue media will also be included in Universal Rescue Media and will be loaded with the corresponding version of Windows PE.

Windows PE

Site Manager Rescue Media are based off one of four Windows PE configurations. Windows PE for Windows 10 is suitable for use on computers running Windows 8 and later and Windows PE 3.1 should be used for Windows 7, Vista and XP. There is also support for 32-bit and 64-bit processors for each Windows PE version.

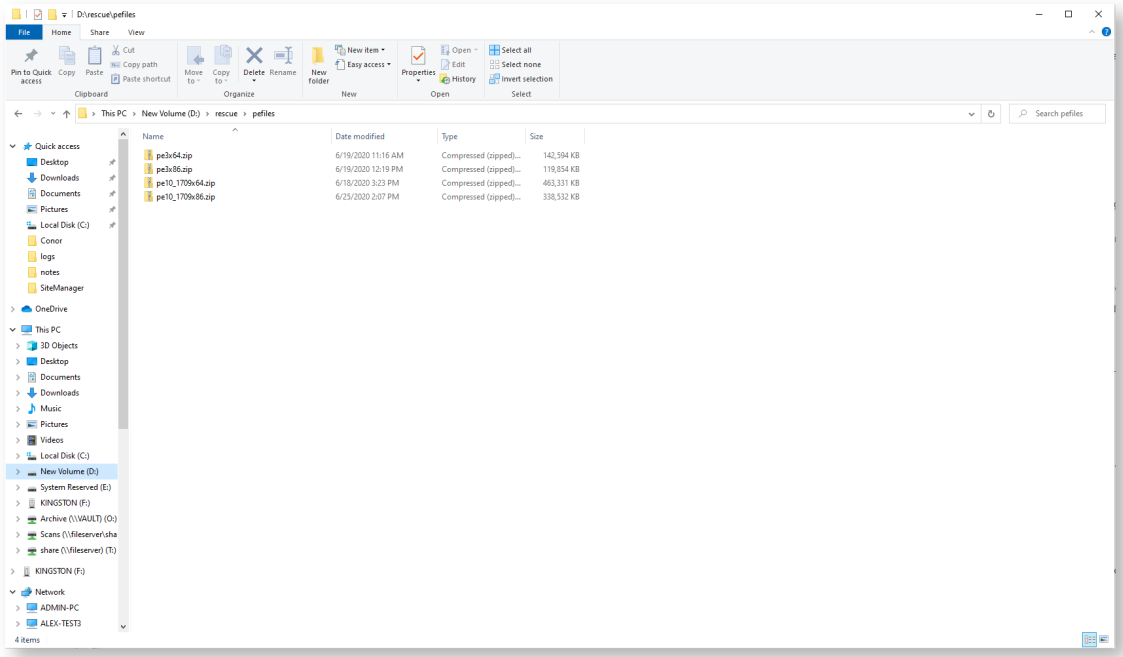
Windows PE files are downloaded when creating Rescue Media or performing agent restores and are stored for future use in the Rescue Media Working Directory (see below). This requires an active internet connection to download Windows PE from Microsoft.

Creating Rescue Media Offline



Rescue Media and restore operations can continue in networks without internet access if the Windows PE files were previously downloaded using the Reflect Download Tool as seen above. Click **options** to select the version of Windows PE to download (Site Manager only supports Windows PE 10 and Windows PE 3).

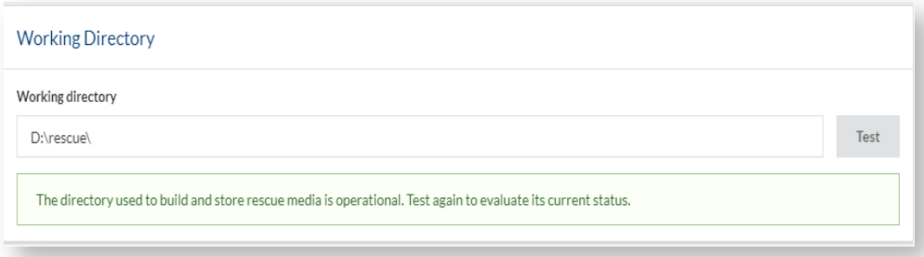
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



These files should then be placed into **\pefiles** subfolder within the Rescue Media Working Directory without changing the name of the zip; it may be necessary to create the pefiles folder manually.

Managing Rescue Media

Rescue Media Working Directory



The Rescue Media Working Directory will contain the Rescue Media images, Windows PE files downloaded from Microsoft and device drivers extracted from the driver database. Rescue Media are a few hundred MB so this folder can grow large if several media are created (this is one reason why it is advised to create Rescue Media only at the time of need).

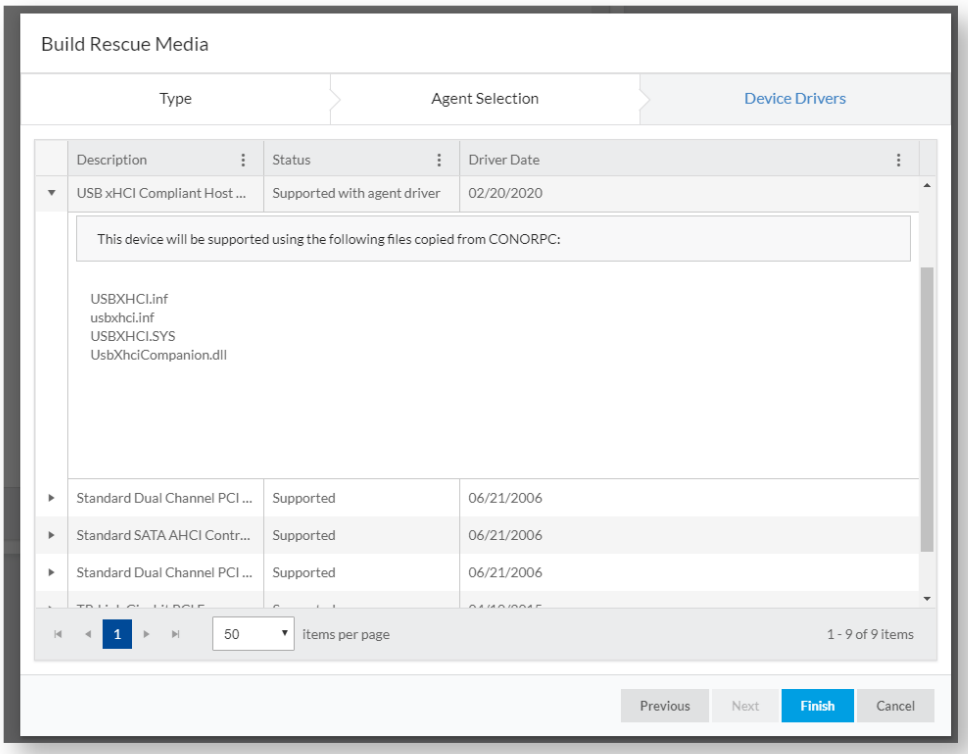
Consequently, users may want this directory to be on a drive with spare space and this can be set in the Rescue Media Settings. Before saving the setting, Site Manager will test the suitability of the folder by creating a small file which is deleted immediately; the save will fail if an error occurs during this process. There is no automatic cleanup of the previous working directory to avoid erasing custom driver files.

Note that the tools used to build Rescue Media require the working directory to be on an NTFS formatted drive, local to the Site Manager server.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

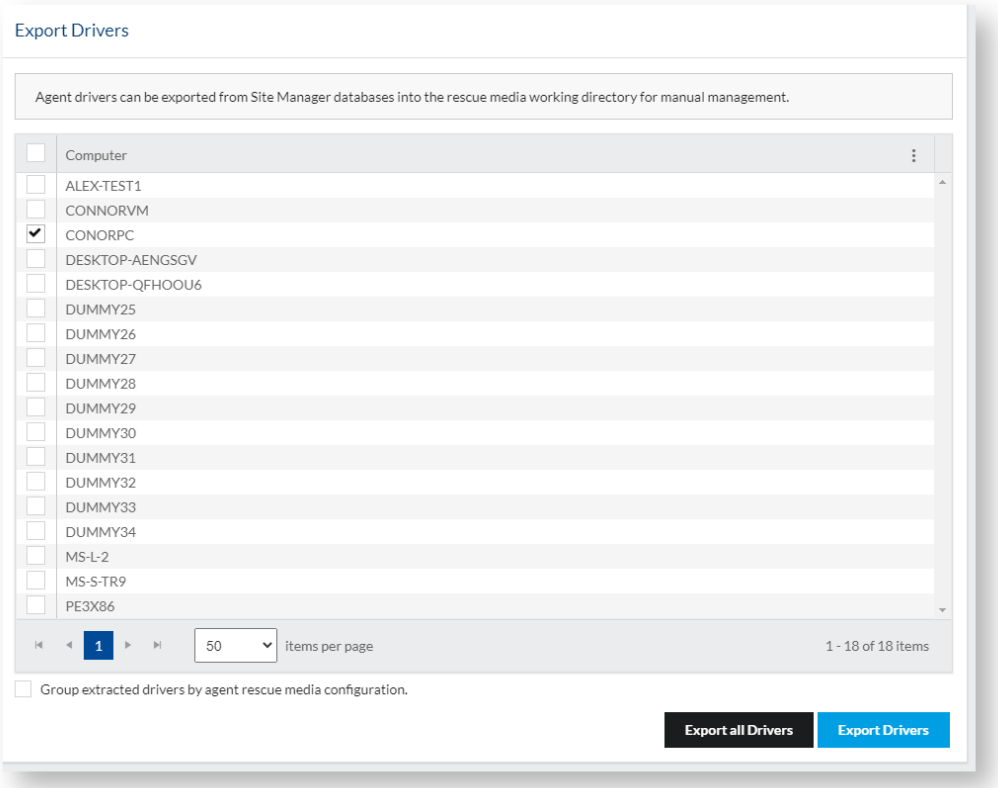
Drivers

Drivers for agent hardware which is not already compatible with Windows PE will be copied to the Site Manager server and stored in a database (“drivers.db” in the Site Manager data directory). Site Manager automatically requests new drivers from agents if a hardware change is detected and drivers of removed computers will be deleted from the database.



Agent Rescue Media copy drivers required by the target agent. These drivers are displayed in the Rescue Media Build Wizard (above).

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



Users can choose to extract the drivers from the database using the table on the Rescue Media settings page or extract drivers from all agents at once. Driver export destinations depend on the name of the agent; drivers from, say, AGENT will be copied into the **drivers\exports\AGENT** subfolder in the Rescue Media working directory (this folder will be created automatically). Alternatively, the exported drivers can be grouped by the Windows PE configuration suitable for the respective agent, this is controlled by the checkbox. For example, if AGENT was a Windows 10 machine then drivers would be exported to **drivers\exports\PE10x64\AGENT**. This may help users prepare Generic Rescue Media for use on groups of similar agents.

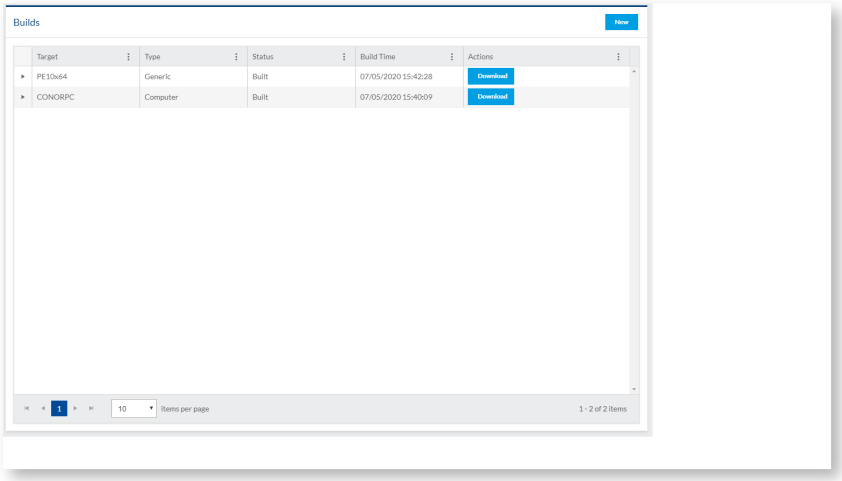
Management of Exported Drivers

Site Manager does not clear the contents of the export folder between exports - this may lead to old and new drivers existing in the same folder. We recommend users move drivers out of the export folder after export and clear the folder between exports.

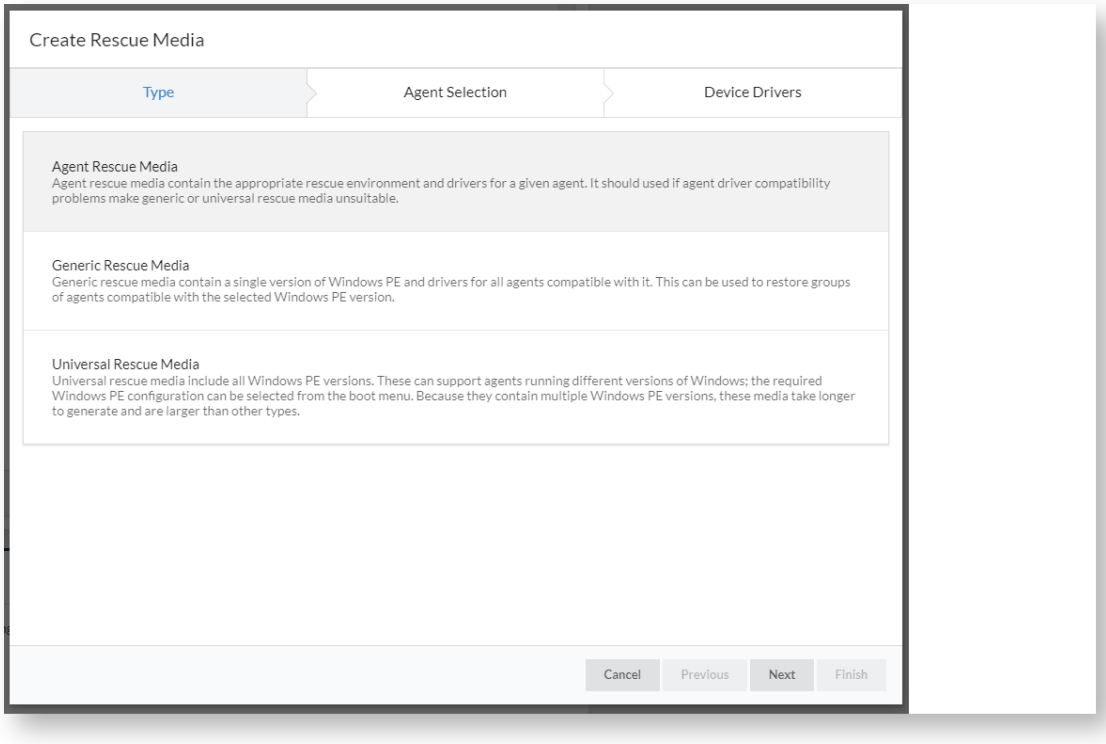
Drivers which should be included in all Rescue Media for a given Windows PE configuration should be placed in a subfolder named after the configuration (e.g. **drivers\PE10x64**). These drivers will be included in both generic and agent Rescue Media which are based on the corresponding Windows PE configuration.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Creating Rescue Media

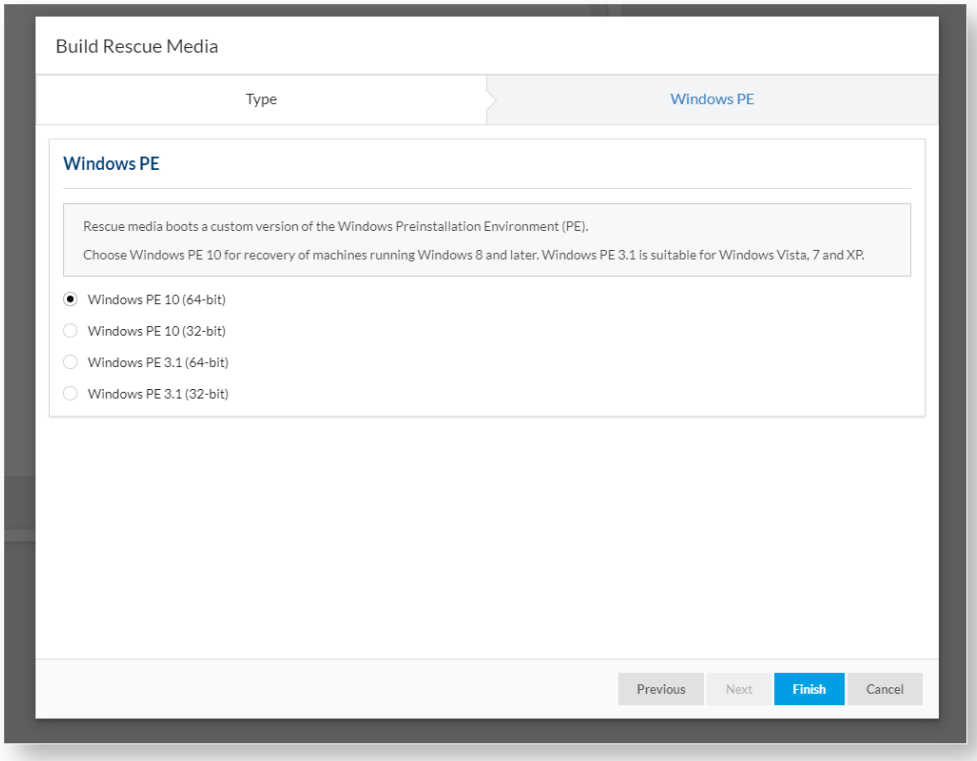


Rescue Media are created through a wizard on the Rescue Media page, accessed by clicking on the “New” button above the table.



A choice between building generic and agent Rescue Media is immediately presented. Generic Rescue Media should be created for restoring non-agent computers or computers without specialized hardware or network needs. Agent Rescue Media will be configured for the target computer.

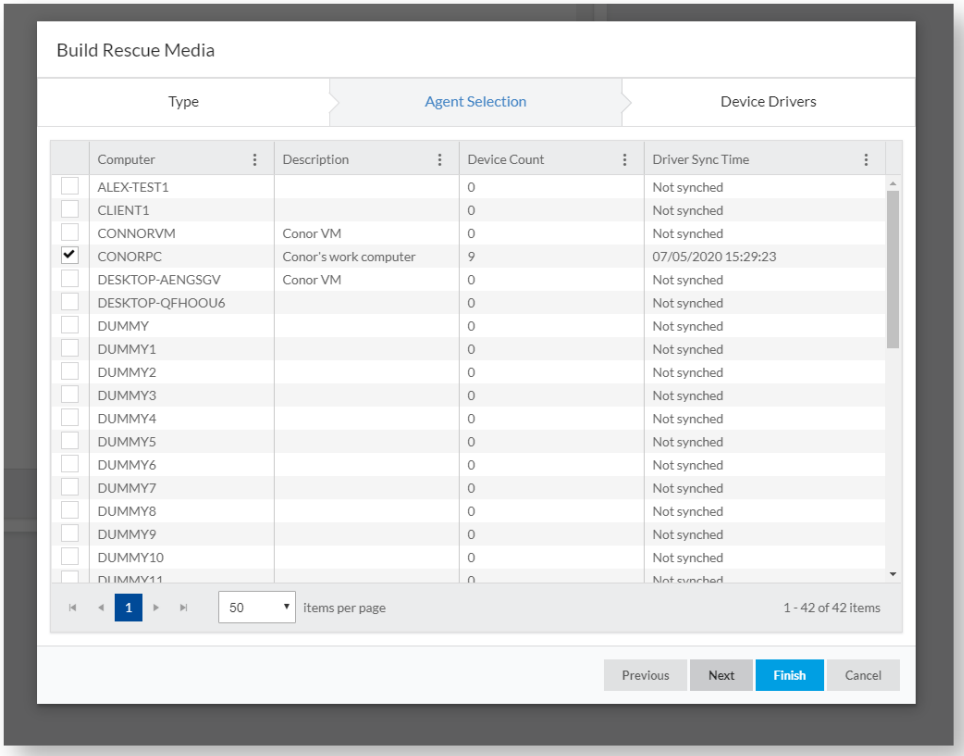
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



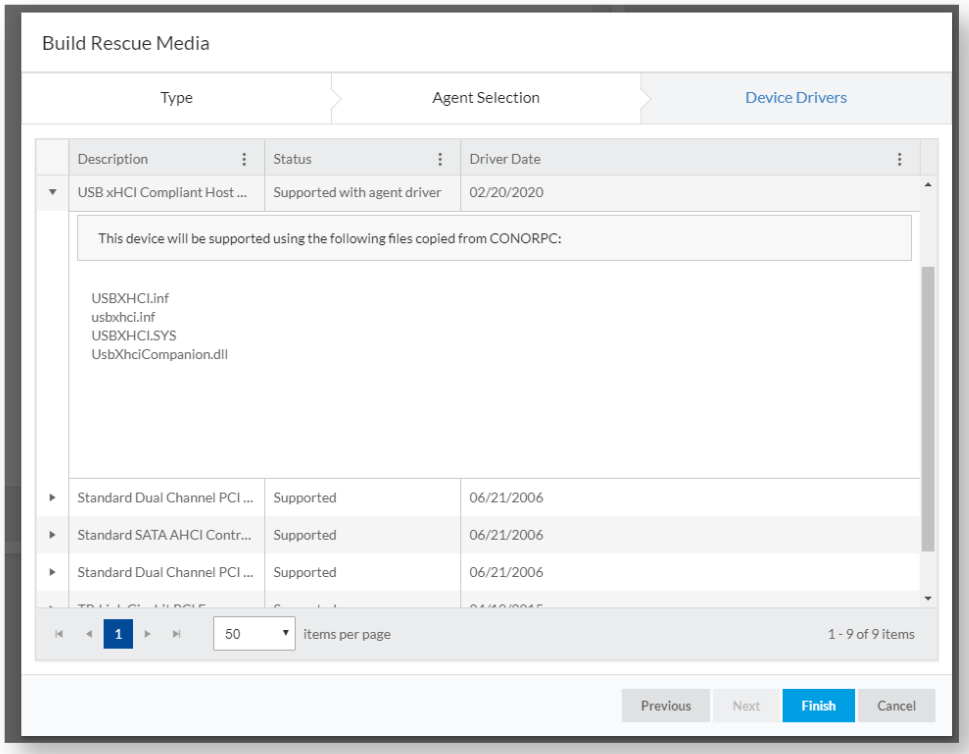
The generic Rescue Media build pathway continues with a selection of Windows PE versions which the medium will be based upon. The tools which Reflect relies upon varies between Windows PE versions so it is important to choose the right version for the operating systems the media may target. Use the following table as a reference:

Windows version of the target computer	**Architecture of the target computer**	**Rescue Media configuration**
Windows 10, Windows 8.1, Windows 8	x64	PE10x64
	x86	PE10x86
Windows XP, Windows Vista, Windows 7	x64	PE3x64
	x86	PE3x86

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



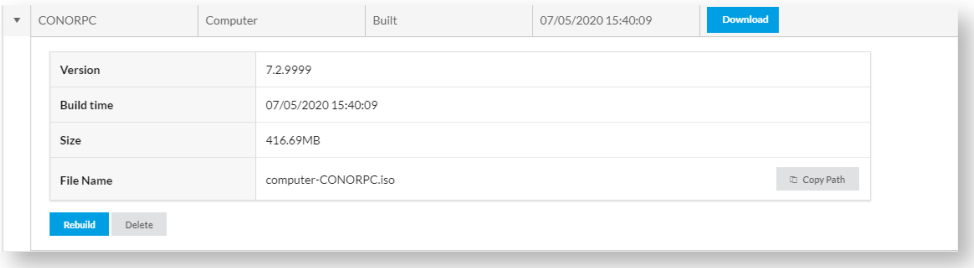
Agent Rescue Media creation begins by selecting the target computer from the computer table shown above.



Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Device and driver information for the selected computer is displayed in the final page of the sequence. The hardware is categorized as either supported in Windows PE by default, supported by drivers from the agent or not supported at all (in this uncommon case a driver will need to be supplied manually). Expanding a device will list the driver files (if any) to be included in the rescue medium.

Builds in progress will be listed in the Rescue Media table with a status of “Building”. Details on the progress of the build and any errors can be displayed by expanding the row. The build can be cancelled but this may not have immediate effect as some stages of the build process can not be interrupted or there may be terminal steps to stop the build cleanly.



Built Rescue Media can be rebuilt by clicking on the “Rebuild” button which appears when the row is expanded. This is useful for updating Rescue Media when there has been changes in agent hardware. Further details of the build and a deletion option are also shown in the expanded view.

Using Rescue Media

Rescue Media are stored as ISO image files in the Rescue Media working directory on the Site Manager server and can be downloaded by users logged into Site Manager. The image can be burned onto a disc or used to create a bootable USB stick which can be inserted into the target computer to load the rescue environment.

It is not necessary to create agent Rescue Media before it is needed. Agent drivers and network configurations are transferred to the Site Manager server during normal Agent communications so the server can generate Rescue Media for an agent even if that computer is offline. Storing Rescue Media for all agents ahead of time may be a significant storage burden.

> Rescue Media for the Site Manager server should be created ahead of time and stored on another system so that Rescue Media capabilities can be retained in disaster scenarios.

Rescue USB Tool

Rescue media can be loaded onto USB flash drives to create rescue USB sticks. Drivers can be copied onto rescue USB media after it has been created as the root of the USB is included in the driver load process. USB rescue media may then be the best choice when recovering from hardware failure or restoring older operating systems where the drivers may not have been added automatically, because drivers on these media can be continually updated to support recovery needs.

This flexibility means that rescue USB sticks are particularly suited for loading universal rescue media; drivers can be added as needed to support the set of computers the medium is intended for.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

However, some third party flashing tools are incompatible with Macrium rescue images. Therefore, Macrium has developed a tool to create rescue USB sticks from rescue media images created by Site Manager 8.

This tool has a command line interface and supports the following commands:

Command	Shortcut	Description
--help	-h	Prints help and copyright information
--list-devices	-l	Lists USB devices suitable for use as rescue sticks
--create	-c	Creates the rescue USB stick. Takes the path to the iso file (-i) and a device number (-d) as mandatory arguments. -f and -q are optional arguments to supress confirmation prompt and progress output respectively.

USB rescue stick creation begins by listing compatible USB devices with the --list-devices command. The tool will search for suitable devices and print their details in the console. This will display device numbers which are used to specify which device this tool should target.

The rescue USB stick will be created with the --create command. The path to the iso file containing the rescue media image and the target device number can respectively be used as the --iso and --device arguments to --create. A confirmation prompt may appear to confirm the selection because this process overwrites data already on the USB stick.

The optional parameters --force and --quiet are intended for use in non-interactive environments and are implied if the tool output is redirected into a file.

Troubleshooting and Advanced Guides

This section contains a number of guides for advanced topics including troubleshooting and integration with other areas of technology.

- Troubleshooting Agent Communications
- Deploying Site Manager Agents Using SCCM
- Migrating Site Manager to a new Computer
- MultiSite Integration
- Agent User Scripting
- Site Manager Advanced Communications Logging
- Site Manager Registry Keys

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Troubleshooting Agent Communications

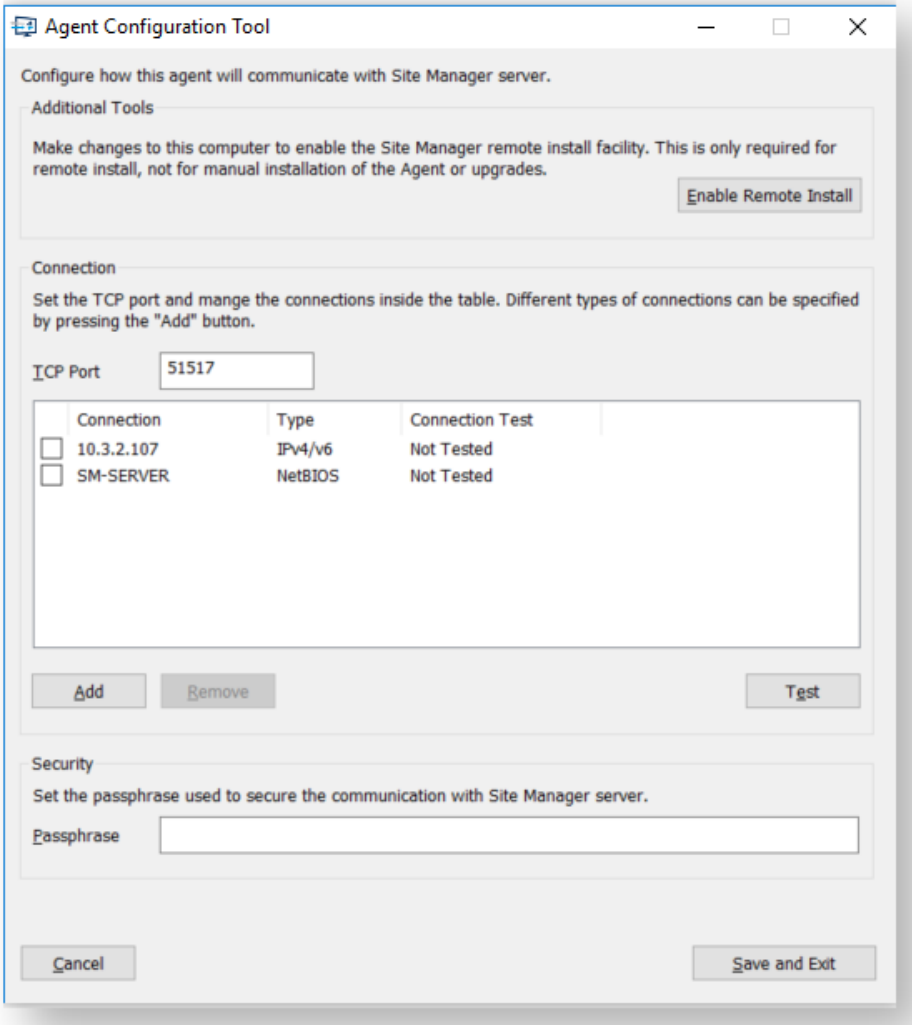
This section contains technical details of what technologies, firewall rules or other prerequisites are required to enable a Macrium Agent to communicate with the Site Manager server. This includes both normal communication and requirements for remote installation of the Agent.

- Agent Configuration Tool
  - Enable Remote Install
  - Connections
    - TCP Port
    - Connection Methods
    - Test the Connection
- Agent Configuration Tool is not able to Connect
  - Incorrect Port
  - Failed Lookups
  - The firewall is blocking the connection
    - Site Manager
    - Site Manager Agent
- Enabling Remote Installation of the Agent on client computers
  - Computers connected to a domain
  - Computers not connected to a domain
    - Enable File Sharing
    - Enabling Remote Management Users

Agent Configuration Tool

The Agent Configuration Tool is installed with the Macrium Site Manager server and remote agent.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



Enable Remote Install

If *Enable Remote Install* is clicked, the tool will open firewall settings for File & Printer Sharing as well as enable local account token filter policy, which are described in the section below: Enabling Remote Installation.

It is possible to enable the remote install via command line:

```
"C:\Program Files\Macrium\Agent\AgentConfigTool.exe" -SILENT_SETTING=YES -
ENABLE_REMOTE_INSTALL=YES
```

Connections

Site Manager and the agent use a TCP/IP connection in order to communicate.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

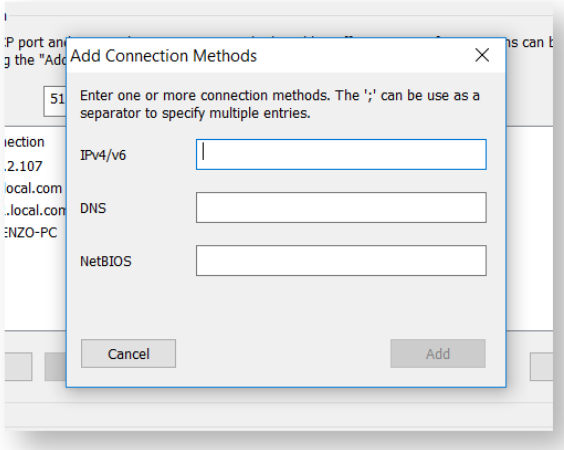
TCP Port

This is the port used by Site Manager in order to accept an incoming TCP connection. This can be check in the Site Manager settings page under Agent/Server Connection Details. Site Manager uses 51515 as default port.

Connection Methods

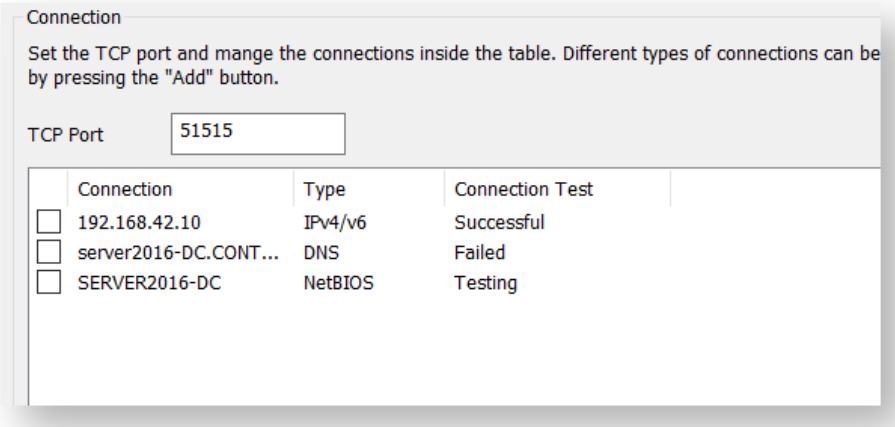
The agent needs the IP (v4 or v6) of the machine that is running Site Manager. Alternatively, the agent will try to resolve to IP DNS names or the NetBIOS of the machine.

Click the *Add* button in order to add entries in the table.



Test the Connection

By clicking the *Test* button the tool will attempt to connect to Site Manager with all the specified connection methods. The results of the test will be reported in the table.



If at least one test in the table is reported as *Successful* the agent will be able to connect to Site Manager.

If all the tests in the table are reported as *Failed* check the section below.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Agent Configuration Tool is not able to Connect

If the connection tests in the table are reported as **Failed**, this may be due to a number of reasons:

Incorrect Port

By default, Site Manager uses TCP port **51515** for communications. This can be changed in the Settings of Site Manager. Confirm that the TCP Port in both the test tool and the Site Manager server match.

Failed Lookups

To connect DNS or NetBIOS names, the Configuration Tool/Agent performs name lookups to resolve the name to an IP address. This uses both DNS and Broadcast (LLMNR) lookups. To confirm that the lookups are working correctly, check the logs in **C:\ProgramData\Macrium\SiteManager\AgentConfigTool.log** or attempt to ping the names directly on a Windows command line.

The firewall is blocking the connection

Site Manager

The firewall of the machine hosting Site Manager must allow incoming TCP connections on the port specified in Site Manager setting under Agent/Server Connection Details. Site Manager uses 51515 as default port.

Site Manager Agent

The firewall must allow outbound TCP traffic.

Enabling Remote Installation of the Agent on client computers

Computers connected to a domain

Site Manager's remote install mechanism uses 'File and Print Sharing' to perform remote installation. On most domains, this is enabled by default on all domain joined computers. If there are additional restrictions on the network, remote installation will not work.

Computers not connected to a domain

Non-domain networks require additional steps to enable the appropriate services and functions required to remote install the Macrium Agent. Each client computer must be configured with the steps below to allow remote installation.

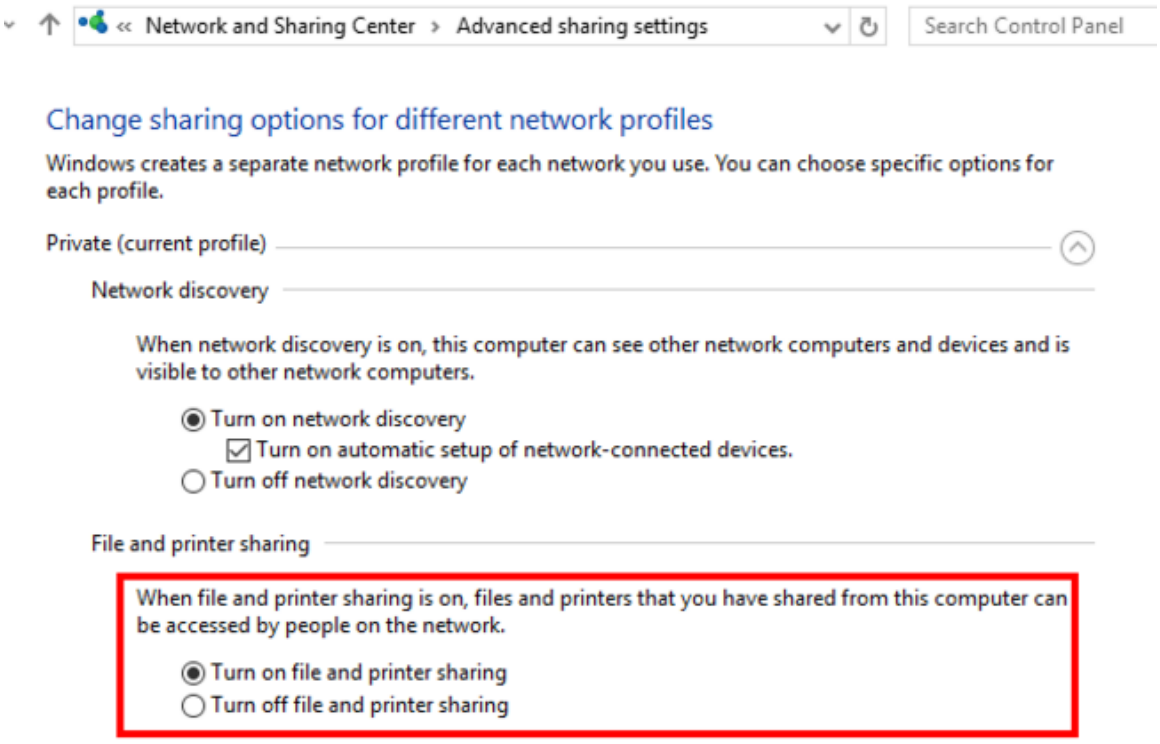
These additional steps are only required for remote agent installation. If the agent is installed manually, these steps are not required.

Note that these steps are not required to manually install the Macrium Agent.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Enable File Sharing

In order to perform the install, file and printer sharing must be turned on. This is found in the Network and Sharing Center -> Advanced sharing settings as shown below.



Enabling Remote Management Users

Outside a domain, users connecting to a computer remotely have reduced privileges. This is part of built-in Windows security measures. The reduced privileges mean that Local Administrator accounts do not have sufficient privileges to install the Macrium Agent when connecting remotely.

To allow remote users to connect with their full Administrator privileges, the following registry entry must be set on the client computer:

Key	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
Name	LocalAccountTokenFilterPolicy
Type	DWORD
Value	1

See https://support.microsoft.com/en-us/kb/951016 for more information on this registry setting.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Deploying Site Manager Agents Using SCCM

Deploying the Macrium Site Manager Agent service to manage your networked computers is easily performed using Site Manager's remote installation feature, however, for some organisations, Microsoft System Center is the preferred method for deploying MSI files. This guide will walk you through the process of deploying the Agent MSI using the Microsoft System Center Configuration Manager.

The Agent .msi is available in two different architectures.:

32 Bit	macrium_agent_x86.msi
64 Bit	macrium_agent_x64.msi

A separate deployment is required for each architecture.

Command Line Switches

There are command line switches that can be passed to install the Agent MSI files.

SILENT_SETTINGS=YES	If not specified or if not equal to **YES**, launch the Agent Configuration Tool after the install
ENABLE_REMOTE_INSTALL=YES	If specified and equal to **YES** enable remote install, see Enabling Remote Installation
NOSHORTCUT=YES	If specified and equal to **YES** the installer will not create a shortcut, if equal to **NO**, shortcuts will be installed
ACCESSTOKEN=*passphrase*	If specified the installer will set the passphrase
SET_ALL=YES	If specified and equal to **YES**, override IP, DNS and NetBIOS if they are empty
SERVER_IP=*192.168.10.42; 192.168.10.43*	If specified and not empty set Site Manager IP in the agent. If SET_ALL=YES and an empty IP is provided, the empty IP will override the current IP
SERVER_DNS=sitemanger1.contoso.local;sitemanger2.contoso.local	If specified and not empty set Site Manager DNS name in the agent. If SET_ALL=YES and an empty DNS is provided, the empty DNS will override the current DNS

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

SERVER_NETBIOS=*SERVER-NETBIOS*	If specified and not empty set Site Manager NetBIOS name in the agent. If SET_ALL=YES and an empty NetBIOS is provided, the empty NetBIOS will override the current NetBIOS
NOCBT=YES	If specified and equal to **YES**, the CBT driver will not be installed
CBT=YES	If specified and equal to **YES**, the CBT driver will be installed

If the shortcut and CBT switches are not specified at all, the shortcut and CBT features will be installed unless an older version of the Site Manager Agent is installed, in which case it will follow the settings of the existing install.

Some platforms cannot run CBT, on these platforms the CBT switch has no effect.

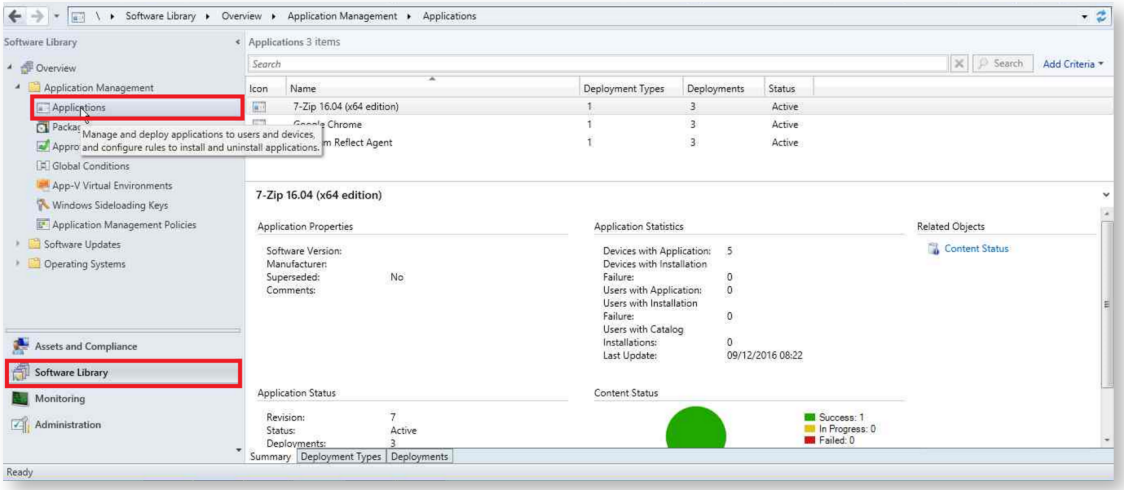
Licensing

Licenses for connected computers are automatically applied when the computer is added to Site Manager. There are no licensing requirements when the Macrium Agent is deployed.

Before you begin: Microsoft System Center Configuration Manager must previously have been installed on Windows Server.

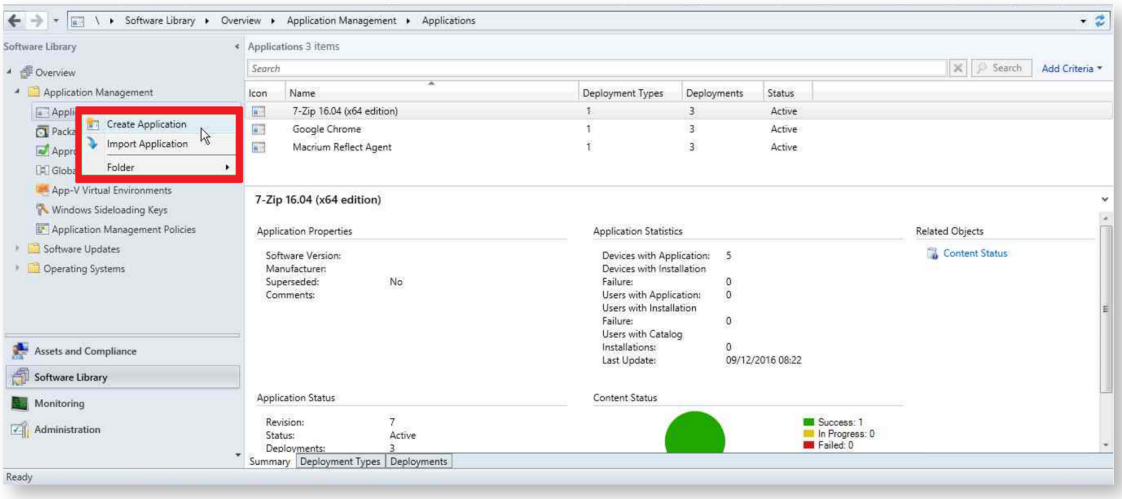
---

1. **Open** SCCM and navigate to '**Software Library**' > '**Applications**' menu on the left hand pane.

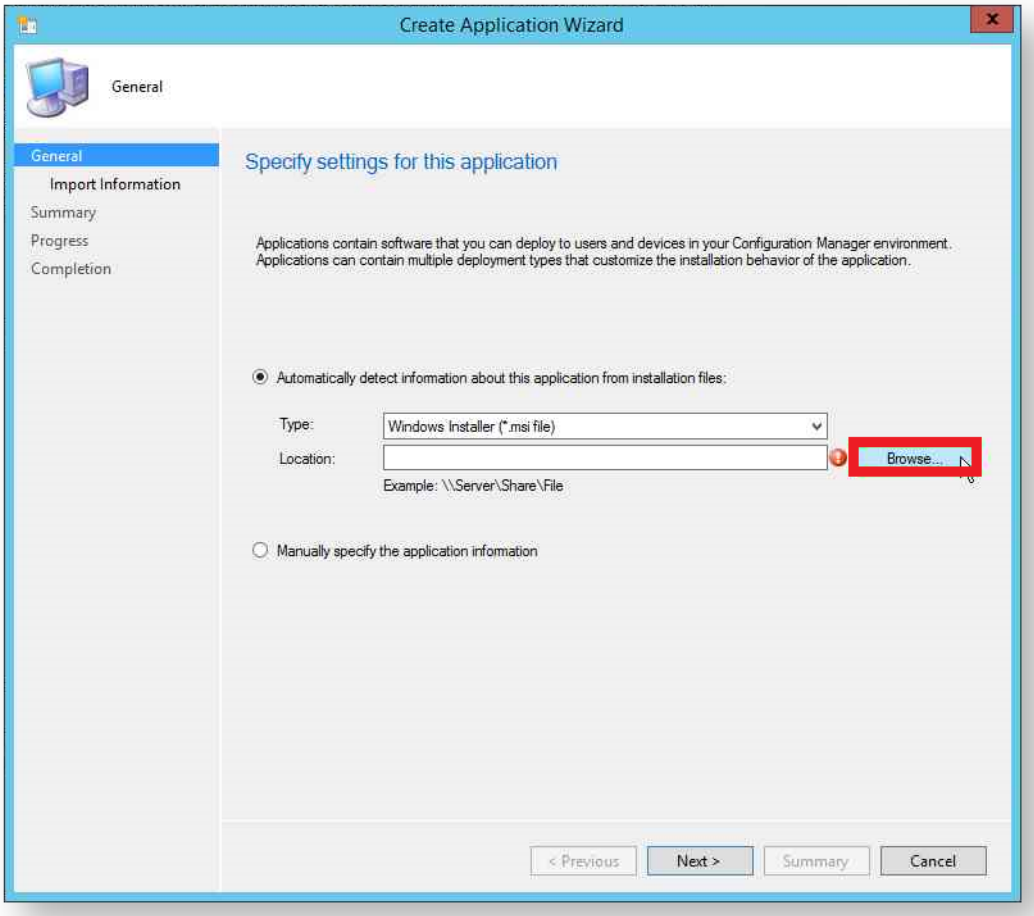


2. **Right click** the '**Applications**' menu and select '**Create Application**'.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

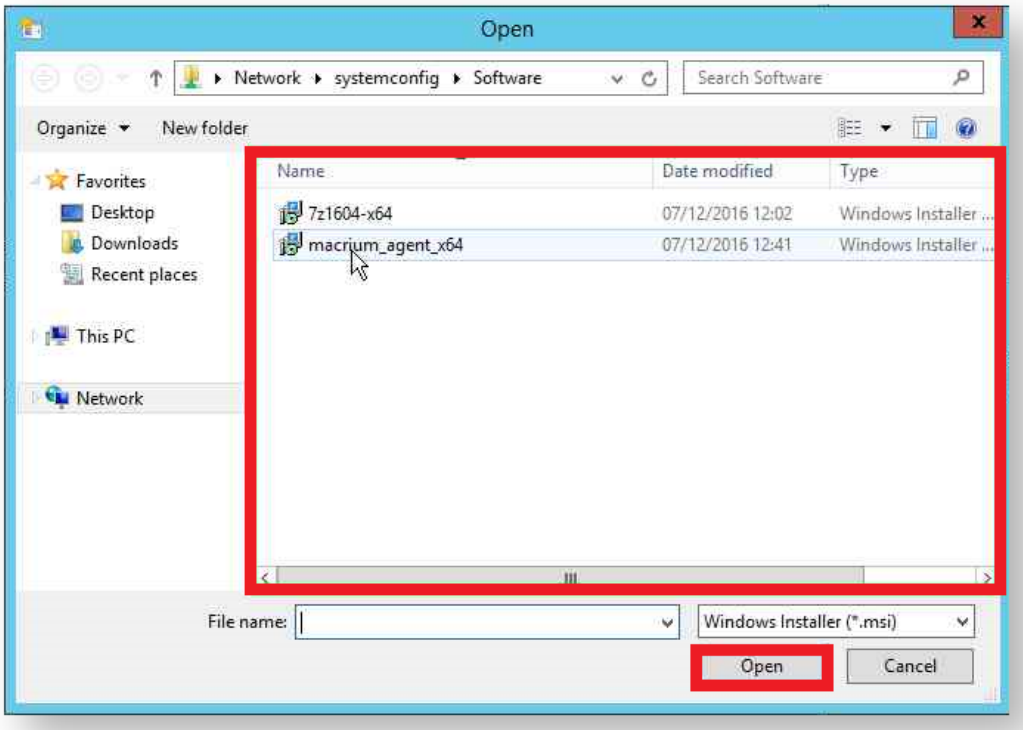


3. In the newly opened wizard **click** the '**Browse...**' button to **add** the **Macrium Agent** to the wizard.



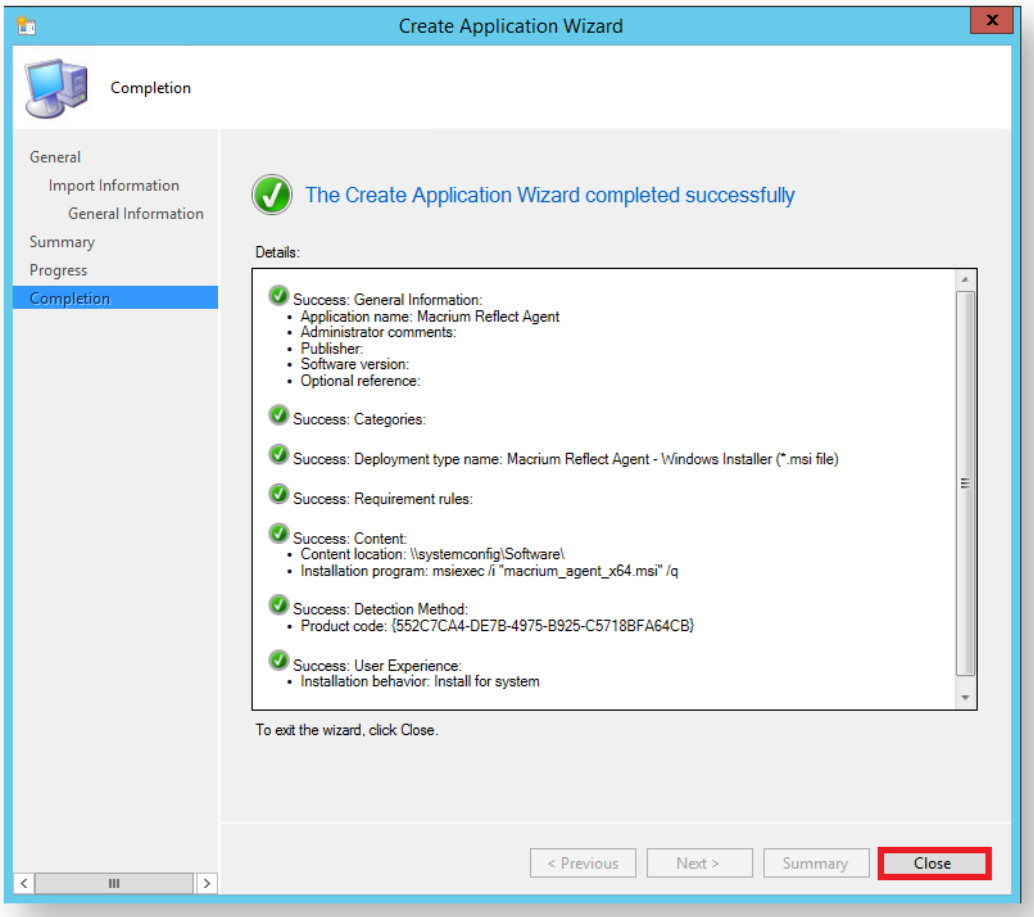
4. Find and select the **Macrium Agent** on your network or local disk then **click** '**Open**'.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



5. **Click** '**Next**' a few more times leaving the fields on each page as **default** until you see the page shown below and **click** '**Close**'.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



6. Once the '**Close**' button is **clicked,** you can start deploying the **Macrium Agent** as per your companies SCCM deployment protocol.

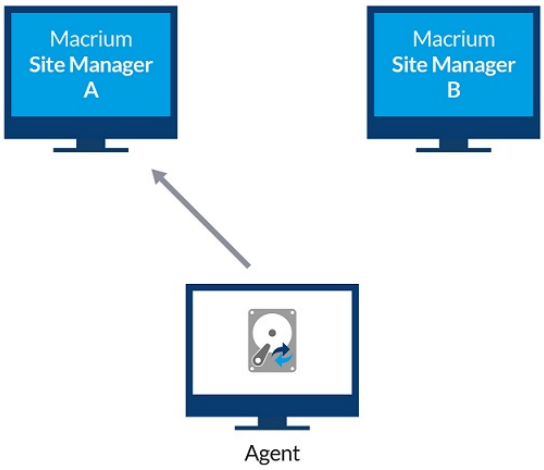
Migrating Site Manager to a new Computer

- Overview
- Automated Agent Migration
- Export and Import Site Manager Configuration
- Manually Migration Migrate a Fully Configured Site Manager

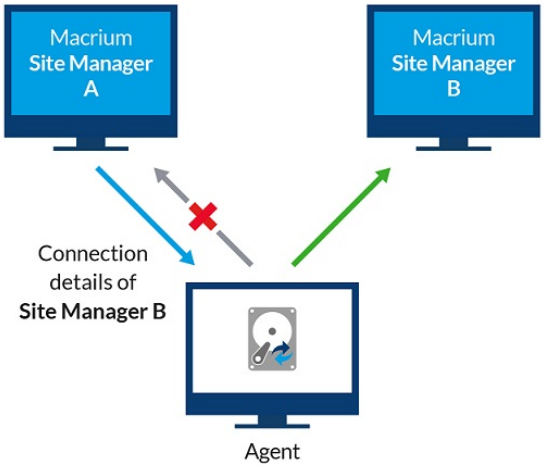
Overview

Site Manager Agents initiate the connection to the Site Manager server which manages them. To move a Site Manager Agent to a new server, the settings in the Agent can be changed on the Agent, or performed using one of the processes listed in this article.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

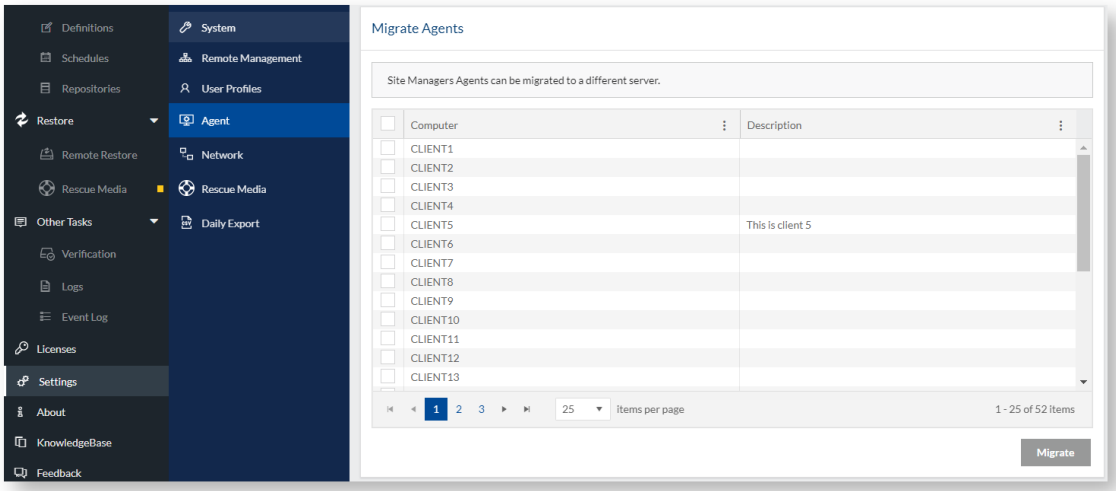


Site Manager A can automate the process of migrating Agents by passing the connection details of Site Manager B to a number of Agents.

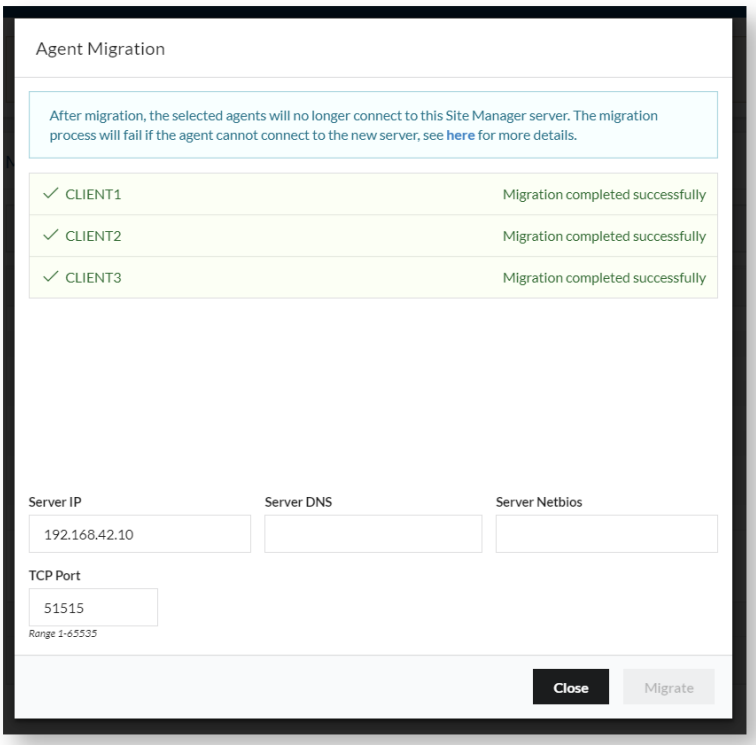


Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Automated Agent Migration



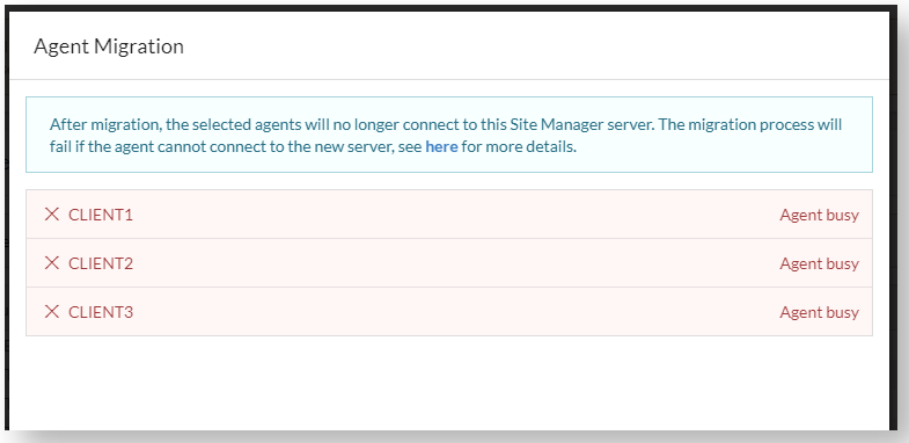
1. In order to migrate an agent from Site Manager A to Site Manager B
2. Go to Settings/Agent page of Site Manager A
3. Select the agents to migrate
4. Click the *Migrate* button
5. Add the connection details for Site Manager B
6. Click the *Migrate* button and wait for the results



Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

If the agent is able to connect to site Manager B, it will report the success and connect to site manager B (the agent will disconnect form Site manager A).

If the agent can't connect to site Manager B, it will report failure. In this case the agents were busy.



Export and Import Site Manager Configuration

Site Manager 7.2 has a configuration import and export function. This should be used instead of the below manual procedure. To use the new mechanism, see Configuration and Security

This article should only be used in cases where an older Site Manager installation is involved or in the case of manual recovery if the Site Manager server hardware can no longer run.

Manually Migration Migrate a Fully Configured Site Manager

1. **Install Site Manager** on a new computer; the download links can be found by clicking here or in trial/license purchase emails. Both the old and new Site Manager installation should be the same version
2. **Remove** any license keys from the old Site Manager installation. The keys must be added to the new Site Manager to register them with the new hardware
3. **Stop** the **' Macrium Remote Management Service'** on the new computer from the **Services** snapin.
   Or run the following command from an elevated command prompt:

   ```
   sc stop MacriumRemoteManagementService
   ```

4. If the **Macrium Agent** is installed on the new server, it should be stopped too. This can be done in the Services UI or by command line:

   ```
   sc stop MacriumAgentService
   ```

5. From your old installation, **copy** the **SiteManager** folder located at '**C:\ProgramData\Macrium**' to the new computer, overwriting the existing folder.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

6. If you are using an SSL certificate to provide an HTTPS interface, ensure that the certificate files are copied to the same path on the new computer. The default self-signed certificates supplied with Site Manager are installed in the ProgramData\SiteManager folder.
7. **Start** the **' Macrium Remote Management Service'** on the new computer from the **Services** snapin.
   Or run the following command from an elevated command prompt

   ```
   sc start MacriumRemoteManagementService
   ```

8. If the **Macrium Agent** is installed, it should be restarted too as above or by using the following command line:

   ```
   sc start MacriumAgentService
   ```

9. Once the service starts, the new Site Manager installation should begin taking over the computers from the old server. The old server should be stopped before this happens. If an agent is in the "Managed by Another Server" state, it may be necessary to manually refresh the agent using the **Refresh** button.
10. If licenses were removed from the old server, add them to the new server.

Dashboard layout and table layouts are stored on a per-user basis. If the new computer uses different local administrator account names to the old, these layout customisations may be lost

MultiSite Integration

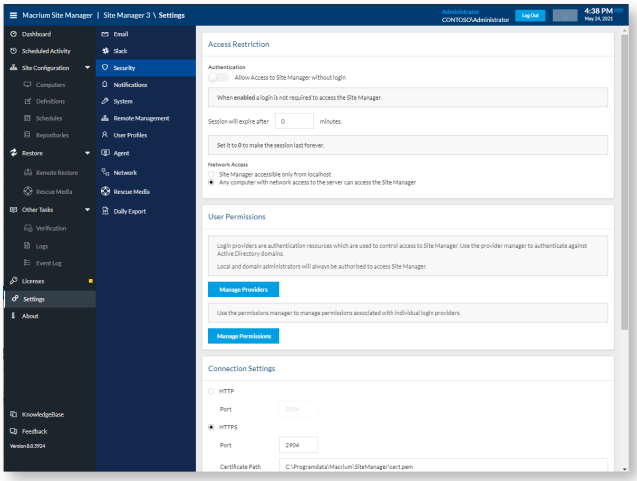
Macrium MultiSite allows multiple Site Manager installations to be monitored and managed from a single online portal. To find out more, visit our website at https://www.macrium.com/multisite

To configure Site Manager for MultiSite integration, the following steps must be followed.

Security Configuration

To ensure that no security issues can arise as a result of enabling MultiSite Integration, the following security options must be set in the **Settings** page under **Security**:

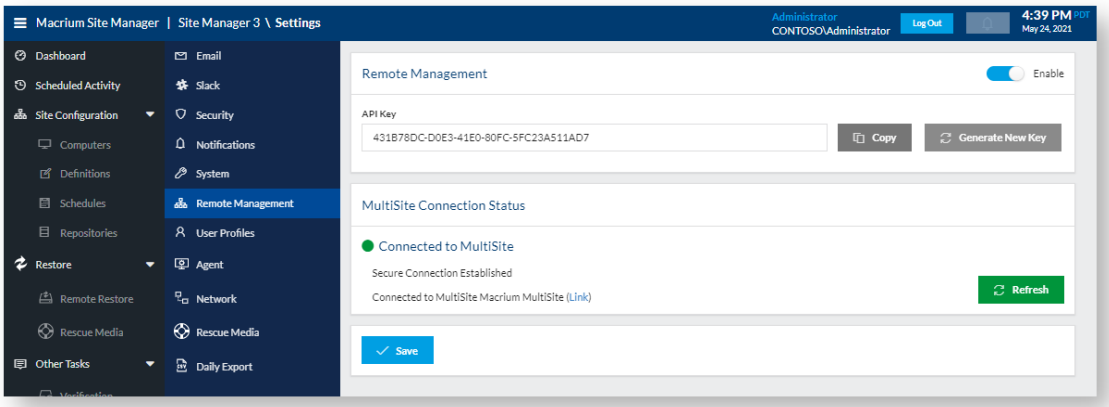
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.



Name	Required Setting
Access Restriction - Allow Access to Site Manager without login	Off - user login must be enabled
Access Restriction - Network Access	Any computer with network access to the server can access Site Manager
Connection Settings	HTTPS communication must be enabled
Connection Settings - Port	Any port may be used

Remote Management

Remote mangement of Site Manager must be enabled in the **Remote Management** section of **Settings**.



The options available are:

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Option	Description
Enable	Toggles Remote Management access on and off
API Key	Security key required by MultiSite to access Site Manager remotely. If this key is changed, MultiSite access will fail until MultiSite is updated with the new key
Copy	Copies the API key to the clipboard
Generate New Key	Generates a new random key. The key is not in effect until **Save** is pressed

All communications between MultiSite and Site Manager use RSA 2048 encryption, no unencrypted data is transferred

Communications Ports and IP Addresses

The MultiSite connection is based on outgoing traffic from the Site Manager installation.

Server	Protocol	Port	IP Addresses	Purpose
tunnel.msadmin.macrium.com	HTTPS	443	40.84.156.200 13.84.162.176 13.65.241.157	To establish an initial connection to MultiSite, Site Manager makes an outgoing HTTPS connection to the Macrium servers.
tunnel.msadmin.macrium.com	SSH	1004	40.84.156.200 13.84.162.176 13.65.241.157	Site Manager uses an outgoing SSH connection to transfer information to MultiSite. Please note that the port used may change in future releases

The IP addresses provided may be changed or added to in future releases. We recommend adding any necessary firewall rules by DNS name if possible.

Agent User Scripting

- Overview
- Setting Up Scripting
  - Running the Script
  - Script output

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

- Viewing Script Results
- Security

Overview

As of version 7.1.3268, a user script may be placed on the agent which the agent will run periodically. This script can produce a user description which is displayed in the computers table of Site Manager and can be used to disable scheduled backups in Site Manager.

The intended use for this script is to provide a mechanism for user scripting to display useful information to the server such as asset IDs and other nonstandard information specific to each computer and to provide a mechanism for the Site Manager administrator to disable backups based on installation specific details. An example of this would be a script which detects that a laptop is connected to the network via a VPN and disables backups until the computer is back in the office.

Setting Up Scripting

The Agent will look for a script at the path **C:\Program Files\Macrium\Agent\Scripts\script.cmd**

This script is executed as a Windows batch file/command script. Powershell scripts, executable files or any other sort of script may be called from this **script.cmd** file.

Running the Script

The Agent will run the script and send the results to the Site Manager server under the following conditions:

- When the Macrium Agent service starts up
- When any file in the **C:\Program Files\Macrium\Agent\Scripts** folder changes
- When any value is written to the **HKEY_LOCAL_MACHINE\SOFTWARE\Macrium\CMCAgent\UserScripts** registry key
- Every 30 minutes

Script activity is logged in the **c:\programdata\Macrium\SiteManager\AgentUserScript.log** file

Script output

The script should produce the following output:

- User description - any text outputted to standard out (e.g. with the 'echo' command) will be shown in Site Manager in the "User Description" column of the Computers table
- Operating Mode - the return code of the script determines the user-set operating mode of the agent. The following

Script Return Value	Operating Mode	Description
0	Normal	The Agent is running normally and all scheduled backups are being run

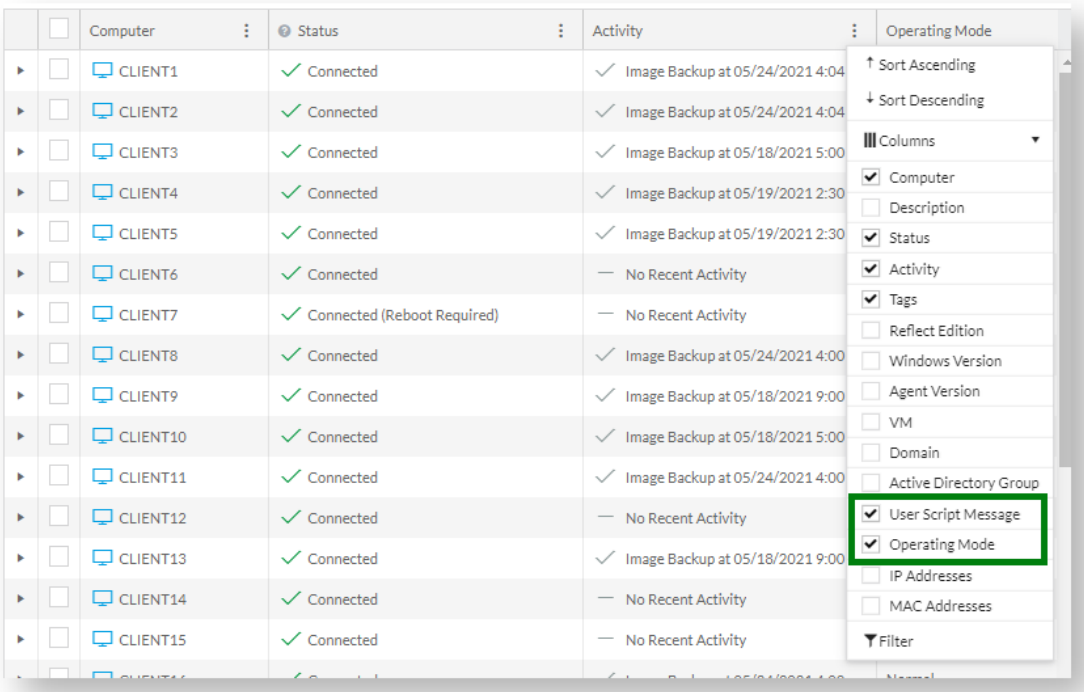
Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Script Return Value	Operating Mode	Description
-1	Ignoring scheduled backups	The Agent should not run backups. When this error code is returned, Site Manager will defer all scheduled backups for the agent until the user script starts returned normal status again. When the agent returns to normal status, any missed backups will be executed immediately as if the computer had been offline and **Defer Missed Backups** was set in the Site Manager schedule. This can be used for computers which move between networks and should not perform backups if they're connected over VPN or WiFi
Any other value	Normal	Any other value is assumed to be an error code in the user script and the script execution is ignored

Viewing Script Results

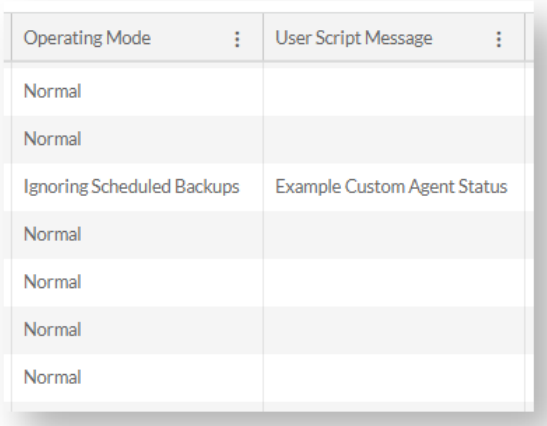
For debugging purposes, script activity is logged in **c:\programdata\Macrium\SiteManager\AgentUserScript.log** on the agent computer.

The results of the script execution can be shown in the Computers table in Site Manager by enabling the "User Script Message" and "Operating Mode" columns which are hidden by default:



Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

These columns will show the script results:



Operating Mode	User Script Message
Normal	
Normal	
Ignoring Scheduled Backups	Example Custom Agent Status
Normal	
Normal	
Normal	
Normal	

This output was produced from the user script below:

```
script.cmd

@echo off
echo Example Custom Agent Status
exit -1
```

Security

For security reasons, scripts must be placed in the **C:\Program Files\Macrium\Agent\Scripts** folder. This folder has write access to **Administrator** users only by default. If the permissions on this folder are manually changed by a system administrator, non-privileged users may be able to set or modify the script being run.

The Agent service runs the script as a non-privileged process using the **Network Service** account, regardless of what user the Agent service is configured to run as. This is to prevent any possibility of a user script being executed with Administrator privileges.

Site Manager Advanced Communications Logging

Advance logging for agents can be enabled for Site Manager by adding the following registry key values.

> This should be done only under the direction of Macrium Support.

This can affect performances as the Site Manager will be logging any interaction with the specified agents.

Remember to remove the added values once done.

1. Run *regedit;*
2. Go to *Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Macrium\Site Manager;*

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

3. Add a string (REG_SZ) value;
4. Rename it to *AgentsToLog;*
5. Set the value to the NetBIOS of the agents separated by ';' e.g. "NETBIOS1;NETBIOS2; NETBIOS3";
6. Add a DWORD value;
7. Rename it to *LogLevel;*
8. Set the value to 3;
9. Restart Site Manager service;

Site Manager Registry Keys

Some advanced options in Site Manager are exposed through setting registry keys on the Site Manager server. The available registry keys are:

Key	HKEY_LOCAL_MACHINE\SOFTWARE\Macrium\Site Manager
Value	Connection Timeout
Type	DWORD
Default	480 (8 minutes)
Affects	Site Manager Server
Description	To avoid NAT routing causing TCP socket disconnection, Site Manager and the Agent will exchange keep alive messages on the interval set in this key. Lowering the number will cause more frequent network traffic, but may be necessary if a NAT router, gateway, switch or other network appliance is set to disconnect sockets more frequently than after 8 minutes idle.

Key	HKEY_LOCAL_MACHINE\SOFTWARE\Macrium\Site Manager
Value	SSL Cipherlist
Type	String (REG_SZ)
Default	TLSv1+HIGH:!SSLv2:!DES:!3DES
Affects	Site Manager Server
Description	

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

	The SSL cipherlist controls which SSL/TLS encryption methods are allowed by the Site Manager's HTTPS management interface. If stricter limits are required for security, any OpenSSL cipherlist as documented on the OpenSSL website may be used. For example, to restrict the web interface to TLS 1.2 and forbid MD5, SHA1 and RC4 hashing, the following string may be used: "TLSv1.2:HIGH:kRSA:!SHA1:!RC4:!MD5:!eNULL:!aNULL:!AES128"

Key	HKEY_LOCAL_MACHINE\SOFTWARE\Macrium\Site Manager
Value	Enable LDAPS
Type	DWORD
Default	1
Affects	Site Manager Server
Description	If set to 0, Site Manager will only attempt unencrypted LDAP requests to Active Directory servers. If set to 1, Site Manager will attempt LDAPS (LDAP over SSL) requests and only fall back to unencrypted requests on error.

Key	HKEY_LOCAL_MACHINE\SOFTWARE\Macrium\Site Manager
Value	LDAPS Port
Type	DWORD
Default	636
Affects	Site Manager Server
Description	The TCP port number to attempt LDAPS queries on.

Key	HKEY_LOCAL_MACHINE\SOFTWARE\Macrium\Site Manager
Value	LDAP Port
Type	DWORD

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Default	389
Affects	Site Manager Server
Description	The TCP port number to attempt LDAP queries on.

Key	HKEY_LOCAL_MACHINE\SOFTWARE\Macrium\Site Manager
Value	Outgoing HTTP Disable
Type	DWORD
Default	0
Affects	Site Manager Server
Description	If set to a non-zero value, this will disable Site Manager's outgoing checks for licenses and updates. This can be useful to set in cases where a Site Manager which cannot contact the internet is experiencing long delays when attempting to add offline keys

Key	HKEY_LOCAL_MACHINE\SOFTWARE\Macrium\Site Manager
Value	Outgoing HTTP Timeout
Type	DWORD
Default	5
Affects	Site Manager Server
Description	By default, there is a 5 second connection timeout on all outgoing HTTP/HTTPS checks from Site Manager. If this is a problem due to slow networking, the timeout can be increased by modifying this registry key

Key	HKEY_LOCAL_MACHINE\SOFTWARE\Macrium\Site Manager
Value	Listen IP Address
Type	String (REG_SZ)

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.

Default	n/a
Affects	Site Manager Server
Description	Site Manager will listen on it's web interface on either the loopback address (127.0.0.1) in restricted mode or on all addresses otherwise. If this registry key is set, the Site Manager web UI will only accept connections from the IP address in this key. This can be useful in advanced deployments where the UI should only be accessible from one network.

Key	HKEY_LOCAL_MACHINE\SOFTWARE\Macrium\Site Manager
Value	Disable Default Admin Access
Type	DWORD
Default	0
Affects	Site Manager Server
Description	By default, Site Manager allows login from any Administrator account on the local computer or on the domain which the local computer is connected to. Setting this registry key to non-zero will disable this behavior and only allow users and groups which have been explicitly allowed access in the settings page of Site Manager access. This key should only be set after initial configuration of Site Manager is completed, to prevent accidental lockout.

Copyright © 2019. Paramount Software UK Ltd. All Rights Reserved.