



# Proactive Systems Management Portal

## Deployment Guide

 Release 1.4

 4 March 2011

---

Dell Inc.  
300 Innovative Way, Nashua, NH 03062

---

## **Copyright © 2007-2010 Dell Inc.**

All rights reserved. Printed in the USA.

At no time may this document be distributed to personnel who have not entered into a Non-Disclosure or Non-Compete agreement with Dell Inc.

## **Trademarks**

Dell and the Dell logo are trademarks of Dell Inc. Microsoft is a registered trademark of Microsoft Corporation in the United States, other countries or both. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and names other than its own. Specifications are subject to change without notice.

For more information about Dell's copyright policies, please see <http://www.dell.com/AUP>.

# Contents

## About This Guide

|                          |    |
|--------------------------|----|
| Audience .....           | ix |
| Conventions .....        | ix |
| Summary of Changes ..... | x  |

## Chapter 1

### Overview

|   |      |
|---|------|
| Overview .....  | 1-1  |
| High-level Architecture .....                                     | 1-2  |
| System Requirements .....   | 1-3  |
| SilverStreak Application Requirements .....                       | 1-3  |
| Operating System .....  | 1-3  |
| Hardware Configuration .....                                      | 1-4  |
| Virtual Machine Configuration .....                               | 1-4  |
| Interoperability .....  | 1-4  |
| Monitored Windows Asset System Requirements .....                 | 1-5  |
| Monitored VMware/Linux Asset System Requirements .....            | 1-5  |
| Monitored Dell PowerVault Storage Asset System Requirements ..... | 1-6  |
| Remote Diagnostics Software Requirements .....                    | 1-6  |
| VMware® vCenter™ Integration .....                                | 1-7  |
| Provisioning Your Account .....                                   | 1-8  |
| Logging Into the Portal .....                                     | 1-10 |
| Quick Start .....   | 1-12 |

## Chapter 2

### Initial Set-up

|   |     |
|---|-----|
| Initial Configuration .....                     | 2-1 |
| Adding Users .....                              | 2-2 |
| Creating a Secondary Contact User Account ..... | 2-2 |
| Creating a Management Domain .....              | 2-4 |

---

|  |      |
|--|------|
| Downloading and Installing SilverStreak .....                          | 2-6  |
| Downloading and Installing SilverStreak from the Dell PSM Portal ..... | 2-6  |
| SilverStreak Configuration .....                                       | 2-8  |
| General .....  | 2-9  |
| Configuration .....  | 2-9  |
| Configuring SilverStreak Credentials .....                             | 2-13 |
| Create an Encryption/Decryption Password .....                         | 2-14 |
| Add Remote Credentials .....   | 2-14 |
| Edit Remote Credentials .....  | 2-18 |
| Delete Remote Credentials .....  | 2-18 |
| Back-up Remote Credentials .....                                       | 2-18 |
| Disaster Recovery .....  | 2-19 |
| Configuring Customer Preferences .....                                 | 2-20 |
| Service Contract Report Notification Options .....                     | 2-20 |
| Remote Diagnostics Settings .....                                      | 2-21 |
| Alerting Options .....   | 2-23 |
| Configuring Monitoring Policies .....                                  | 2-26 |

### **Chapter 3**

#### **Discovery**

|   |     |
|---|-----|
| Discovering Assets .....                | 3-1 |
| Single Device or Range of Devices ..... | 3-3 |
| Importing Devices from a File .....     | 3-4 |
| Device Typing .....                     | 3-5 |
| Verifying Discovery Results .....       | 3-6 |

### **Chapter 4**

#### **Managing Groups and Management Domains**

|                                    |     |
|------------------------------------|-----|
| Group Management .....             | 4-1 |
| Creating a Group .....             | 4-2 |
| Editing a Group .....              | 4-3 |
| Deleting a Group .....             | 4-4 |
| Domain Management .....            | 4-5 |
| Editing a Management Domain .....  | 4-5 |
| Deleting a Management Domain ..... | 4-7 |

---

**Appendix 1**  
**Support and FAQ**

[Support](#) ..... A-1  
[FAQ](#) ..... A-1

**Index**



---

# Figures

|              |  |      |
|--------------|--|------|
| Figure 1-1.  | Dell PSM Portal Architecture .....                 | 1-2  |
| Figure 1-2.  | Dell PSM Portal Self Provisioning Screen .....     | 1-9  |
| Figure 1-3.  | Dell PSM Portal Login Screen .....                 | 1-10 |
| Figure 1-4.  | Home Screen .....                                  | 1-11 |
| Figure 2-1.  | Add User Form .....                                | 2-2  |
| Figure 2-2.  | Registration/Sign In Page .....                    | 2-4  |
| Figure 2-3.  | Add Domain Screen .....                            | 2-5  |
| Figure 2-4.  | SilverStreak Service Account .....                 | 2-7  |
| Figure 2-5.  | Configuration Tab .....                            | 2-10 |
| Figure 2-6.  | Set Password for Remote Credentials Dialogue ..... | 2-14 |
| Figure 2-7.  | Manage Windows Credential Dialogue .....           | 2-15 |
| Figure 2-8.  | Manage SSH Credential Dialogue .....               | 2-17 |
| Figure 2-9.  | Customer Notifications Pane .....                  | 2-20 |
| Figure 2-10. | Remote Diagnostics Pane .....                      | 2-22 |
| Figure 2-11. | Alerts Pane .....                                  | 2-24 |
| Figure 3-1.  | Discovery Wizard .....                             | 3-2  |
| Figure 4-1.  | Add Group Screen .....                             | 4-2  |
| Figure 4-2.  | Edit Group Screen .....                            | 4-3  |
| Figure 4-3.  | Delete Group Screen .....                          | 4-5  |
| Figure 4-4.  | Edit Domain Screen .....                           | 4-6  |
| Figure 4-5.  | Delete Domain Icon .....                           | 4-7  |





---

# About This Guide

The *Dell Proactive Systems Management Portal Deployment Guide* provides you with information that enables you to take full advantage of the Dell Proactive Systems Management Portal's powerful Dell systems management features.

## Audience

The *Dell Proactive Systems Management Portal Deployment Guide* is intended for:

- Users who wish to manage their organisation's network and systems

This guide assumes that you have:

- An understanding of network management

## Conventions

|                           |   |
|---------------------------|---|
| <b>bold text</b>          | Indicates text that you need to enter, or steps in a procedure.<br><br>Example: <b>Enter your password.</b> |
| <i>italic text</i>        | Indicates new terms, menu options, file and directory names and book titles.                                |
| blue text                 | Indicates a hypertext link to another section, document or website.   |
| <code>courier text</code> | Indicates a software or system message.   |

The following conventions are used to attract the attention of the reader:



**Note:** Indicates important information that is essential to the proper configuration or running of the system or system component.

---



**Caution:** Indicates the risk of data loss, equipment damage or system failure.

---



**Tip:** Indicates additional hints or suggestions that may help you to solve problems or that describe alternative ways to perform tasks.

---

## Summary of Changes

The following table describes changes made to this document.

| Release Version         | Date    | Reason   | Details  |
|-------------------------|---------|--|--|
| Release 1.2, revision 1 | 6/4/10  | <ul style="list-style-type: none"><li>Clarity</li><li>Convert to Dell style</li></ul>                | <ul style="list-style-type: none"><li>Updated the steps to add credentials on <a href="#">page 3-3</a>.</li><li>Standardised to Dell Global Services criteria.</li></ul>   |
| Release 1.3             | 18/8/10 | <ul style="list-style-type: none"><li>Clarity</li><li>New features</li><li>Troubleshooting</li></ul> | <ul style="list-style-type: none"><li>Updated:<ul style="list-style-type: none"><li>Service contract expiry notification email description on <a href="#">page 2-21</a>.</li><li>Screens and procedural steps in all chapters.</li><li><a href="#">“SilverStreak Application Requirements”</a> on <a href="#">page 1-3</a>.</li><li><a href="#">“Monitored VMware/Linux Asset System Requirements”</a> on <a href="#">page 1-5</a>.</li></ul></li><li>Added:<ul style="list-style-type: none"><li><a href="#">“Monitored Dell PowerVault Storage Asset System Requirements”</a> on <a href="#">page 1-6</a>.</li><li><a href="#">“Device Typing”</a> on <a href="#">page 3-5</a>.</li><li>New <a href="#">“FAQ”</a> entries.</li></ul></li></ul> |

---

| Release Version | Date   | Reason  | Details   |
|-----------------|--------|---|---|
| Release 1.4     | 4/3/11 | <ul style="list-style-type: none"> <li>Clarity</li> <li>Accuracy, new features</li> </ul> | <ul style="list-style-type: none"> <li>Removed excessive figures, clarified remaining and new figures.</li> <li>Added: <ul style="list-style-type: none"> <li><a href="#">“Remote Diagnostics Software Requirements”</a> on page 1-6.</li> <li><a href="#">“VMware® vCenter™ Integration”</a> on page 1-7.</li> <li>New <a href="#">“FAQ”</a> entries for SLES 11.</li> </ul> </li> <li>Updated: <ul style="list-style-type: none"> <li><a href="#">“System Requirements”</a> on page 1-3.</li> <li><a href="#">“Provisioning Your Account”</a> on page 1-8.</li> <li><a href="#">“Logging Into the Portal”</a> on page 1-10.</li> <li><a href="#">“Adding Users”</a> on page 2-2.</li> <li><a href="#">“Downloading and Installing SilverStreak”</a> on page 2-6.</li> <li><a href="#">“Remote Diagnostics Settings”</a> on page 2-21.</li> <li><a href="#">“Alerting Options”</a> on page 2-23.</li> <li><a href="#">“Configuring Monitoring Policies”</a> on page 2-26.</li> <li><a href="#">“Device Typing”</a> on page 3-5.</li> </ul> </li> </ul> |

---



---

# Chapter 1 Overview

This chapter introduces the Dell Proactive Systems Management Portal and briefly describes the architecture and system requirements, as well as how to log in.

| <b>Chapter Contents</b>   | <b>Page</b> |
|---|-------------|
| • <a href="#">Overview</a>  | 1-1         |
| • <a href="#">High-level Architecture</a>                                     | 1-2         |
| • <a href="#">System Requirements</a>   | 1-3         |
| • <a href="#">SilverStreak Application Requirements</a>                       | 1-3         |
| • <a href="#">Monitored Windows Asset System Requirements</a>                 | 1-5         |
| • <a href="#">Monitored VMware/Linux Asset System Requirements</a>            | 1-5         |
| • <a href="#">Monitored Dell PowerVault Storage Asset System Requirements</a> | 1-6         |
| • <a href="#">Remote Diagnostics Software Requirements</a>                    | 1-6         |
| • <a href="#">VMware® vCenter™ Integration</a>                                | 1-7         |
| • <a href="#">Provisioning Your Account</a>                                   | 1-8         |
| • <a href="#">Logging Into the Portal</a>                                     | 1-10        |
| • <a href="#">Quick Start</a>   | 1-12        |

## Overview

The Dell PSM Portal solution communicates with your Dell systems using SSL encryption on port 443, which is open by default in most environments.

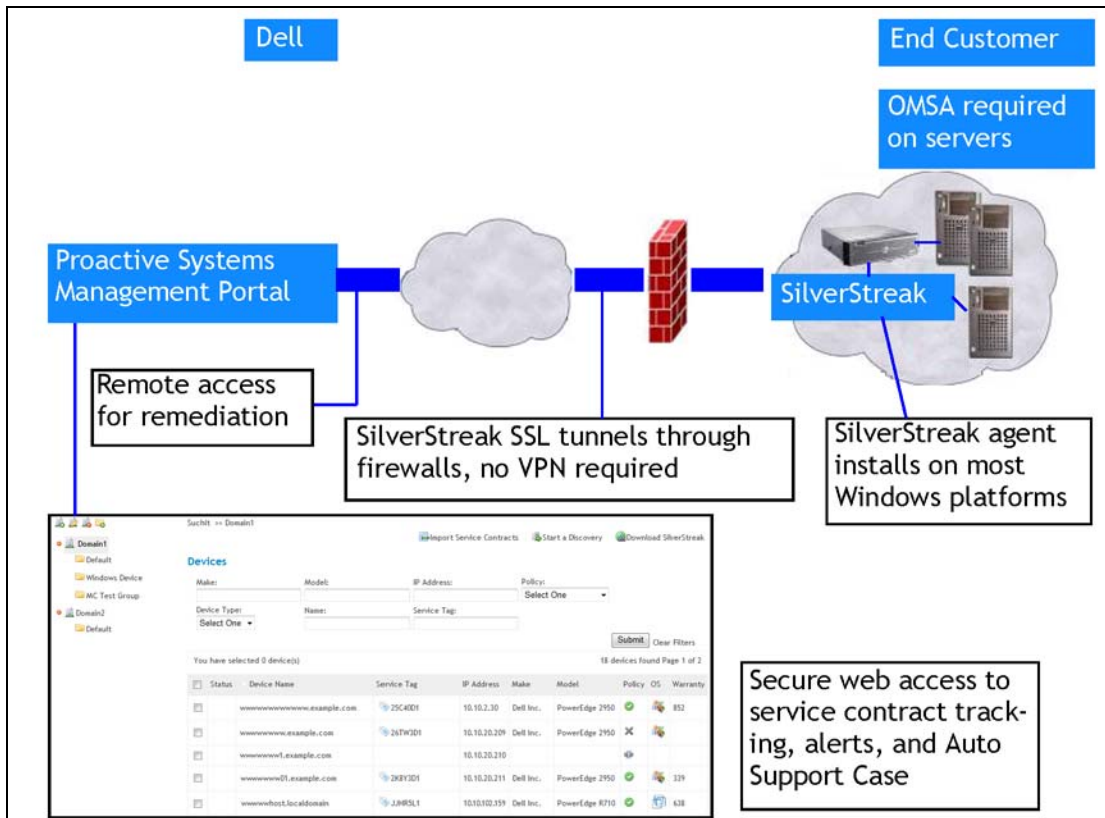
There are no special port requirements for managed and monitored devices on your internal network. The SilverStreak agent, installed upon a Windows server in your environment, monitors Windows event logs and VMware/Linux **/var/log** messages for specific OpenManage events that occur.

Dell does not maintain, and has no visibility to, username/password information used for device discovery and monitoring. Instead, that information is contained and managed by you, on the system hosting SilverStreak. This ensures that your credentials are secure.

## High-level Architecture

Figure 1-1 displays a high-level view of the Dell PSM Portal architecture.

**Figure 1-1. Dell PSM Portal Architecture**



---

## System Requirements

This section describes:

- [SilverStreak Application Requirements](#) (see below)
- [Monitored Windows Asset System Requirements](#) (see [page 1-5](#))
- [Monitored VMware/Linux Asset System Requirements](#) (see [page 1-5](#))
- [Monitored Dell PowerVault Storage Asset System Requirements](#) (see [page 1-6](#))
- [Remote Diagnostics Software Requirements](#) (see [page 1-6](#))

## SilverStreak Application Requirements



---

**Tip:** Dell strongly recommends creating separate Windows credentials:

- A Service Account credential used for running the SilverStreak service
  - A Windows Domain account credential with administrator rights (and proxy authentication if needed)
- 

### Operating System

SilverStreak must be installed on a system running one of the following Windows operating systems, using Administrator privileges.

- Windows Server 2008 R2
- Windows 7 Enterprise or Professional, 32-bit or 64-bit
- Windows Vista Business, Enterprise, or Ultimate 32-bit or 64-bit (Service Pack 1 or higher recommended), with User Access Control (UAC) disabled
- Windows XP Professional 32-bit or 64-bit with Service Pack 1 or higher (Service Pack 2 or higher recommended, with the Microsoft firewall's Startup Type set to Manual)
- Windows 2003 Server 32-bit or 64-bit
- Windows 2000 Professional or Server with any Service Pack (Service Pack 4 recommended)



---

**Tip:** SilverStreak automatically updates to the current version when it connects to an updated Dell PSM Portal application server. To display your current SilverStreak version on the SilverStreak host:

1. Navigate to *Start > All Programs > SilverStreak > SilverStreak Config.*
  2. The SilverStreak version appears in the *General* tab.
-

## Hardware Configuration

The **minimum** recommended hardware configuration for the SilverStreak host, based on the number of assets being monitored, is listed in [Table 1-1](#).

**Table 1-1. Minimum SilverStreak Hardware Requirements**

|                     | 1- 100 Devices    | 101- 500 Devices   | 501- 1,000 Devices |
|---------------------|-------------------|--------------------|--------------------|
| <b>CPU</b>          | 2+ GHz P4         | 3+ GHz P4          | Dual 3+ GHz P4     |
| <b>Memory</b>       | 2 GB              | 4 GB               | 4 GB               |
| <b>Disk</b>         | 80 MB             | 120 MB             | 200 MB             |
| <b>Bandwidth*</b>   | 2 Kbps<br>< 1% T1 | 10 Kbps<br>< 1% T1 | 20 Kbps<br>< 1% T1 |
| <b>System Usage</b> | Shared†           | Dedicated          | Dedicated          |

\* Bandwidth requirements are for SilverStreak only. The bandwidth should be greater if supporting additional traffic.

† Dell recommends that SilverStreak share a system running non-critical applications only.

## Virtual Machine Configuration

If installing within a Virtual Machine, follow the hardware guidelines for OS resource allocation.

## Interoperability

### SNMP

SilverStreak **cannot** reside on a Windows server that also has the Dell OpenManage IT Assistant, Dell Management Console or the Windows SNMP trap collector installed. There is a conflict between SilverStreak's built-in SNMP trap collector and other SNMP monitoring tools.

### VMware® vCenter™

Dell PSM Portal support for VMware® vCenter™ requires SilverStreak version 2.2 or higher. You can start using the enhanced VMware® vCenter™ support as soon as SilverStreak's update has completed.



---

## Monitored Windows Asset System Requirements

---



**Note:** Dell PowerEdge SC servers are not supported.

---

Monitored Windows assets must meet the following requirements:

- Windows Server 2000, 2003 or 2008
- Dell PowerEdge 6th generation server or higher (e.g. 2650, 6600, 4600)
- OpenManage Server Administrator (OMSA) 4.5 or newer installed on the server to be monitored
- Server, RPC, Remote Registry and TCP/IP NetBIOS Helper services running
- NetBIOS over TCP enabled, in order to allow hostname resolution. Otherwise, the asset's IP address will be used as its hostname.

---

## Monitored VMware/Linux Asset System Requirements

---



**Note:** Dell PowerEdge SC servers are not supported.

---

Monitored VMware/Linux assets must meet the following requirements:

- Red Hat Enterprise Linux 3, 4, 5, or 6
- SUSE Linux Enterprise Server 10 or 11 (64-bit only)
- VMware ESX (vSphere) 4.1 and 4.5
- VMware ESXi (vSphere) 4.1 and 4.5
- SSH access to Linux/VMware systems
- Dell PowerEdge 6th generation server or higher (e.g. 2650, 6600, 4600)
- OpenManage Server Administrator (OMSA) 4.5 or newer installed on the server to be monitored
- SNMP installed
- UDP ports 161 and 514 and TCP port 161, open between the monitored system and the SilverStreak host

## Monitored Dell PowerVault Storage Asset System Requirements

The Dell PSM Portal can monitor the following PowerVault storage assets:

- MD3000
- MD3000i
- MD3200i
- MD3220i
- NX2000
- NX3000
- NX3100



**Tip:** Dell Modular Disk Storage Manager (MDSM) must be configured to send SNMP traps to SilverStreak in order for the Dell PSM Portal to monitor Dell PowerVault MD3000, MD3000i, MD3200i and MD3220i devices via traps. See your Dell PowerVault documentation for instructions to specify a trap receiver.

The Dell PSM Portal supports monitoring Dell PowerVault NX2000, NX3000 and NX3100 with Windows server events only. Monitoring via traps is not supported.

---

## Remote Diagnostics Software Requirements

To enable remote diagnostics for Dell Technical Support, ensure that the following software requirements are met:

- **Dell System E-Support Tool (DSET)** — For server devices and Dell PowerVault NX2000, NX3000 and NX3100 storage devices, DSET can run at discovery, upon alert generation and on demand.



**Note:** DSET does not currently run on ESXi devices. Running DSET on ESXi devices will be supported in a future Dell PSM Portal release.

---

- **Lasso** — For Dell PowerVault MD3000, MD3000i, MD3200i and MD3220i storage devices, Lasso can run upon alert generation and on demand.



**Tip:** Because Dell PowerVault NX2000, NX3000 and NX3100 devices are managed as servers, the Dell PSM Portal uses DSET to gather diagnostics information from them, not Lasso.

---

Contact your Dell sales representative to obtain the current versions of these tools.

## VMware® vCenter™ Integration

The Dell PSM Portal enables you to discover, view and monitor VMware® vCenter™-managed ESX and ESXi devices.



**Note:** You must first install the Dell Management Plug-in for VMware® vCenter™ on your vCenter servers to use this feature. Contact your Dell sales representative to obtain it.

You should be aware of the following VMware® vCenter™ integration limitations:

- The Dell PSM Portal cannot detect installations or statuses of Dell Management Plug-in for VMware® vCenter™ instances.
- Alerts cannot be processed without the Dell Management Plug-in for VMware® vCenter™ properly configured and running.
- If the Dell Management Plug-in for VMware® vCenter™ is not properly configured and running, ESX/ESXi devices may appear to be monitored when they are not.
- The Dell PSM Portal can manage a maximum of 250 client ESX/ESXi devices per vCenter Server.

Please bear in mind the following VMware® vCenter™ assets information:

- ESX/ESXi devices identified by vCenter cannot be deleted within the Dell PSM Portal.
- ESX/ESXi devices discovered in prior versions of the Dell PSM Portal system remain, whether or not they are found during a current release rediscovery; any newly-discovered devices are added.
- Device inventory is automatically updated on a daily basis. ESX/ESXi devices

See “Managing ESX/ESXi Devices with the Dell PSM Portal” and “Managing ESX/ESXi Devices with the vCenter Console and Dell PSM Portal” in the *Dell Proactive Systems Management Portal User Guide* for more information.

## Provisioning Your Account

You access the Dell PSM Portal interface with your existing Dell MyAccount credentials. You can manage these credentials and/or create a new account, at <http://ecomm.dell.com/myaccount/login.aspx>.



**Note:** The Dell PSM Portal is only available to Dell ProSupport customers.

Dell MyAccount credentials are required prior to signing up for the Dell PSM Portal service.

---

You **must** have the following items ready before you proceed:

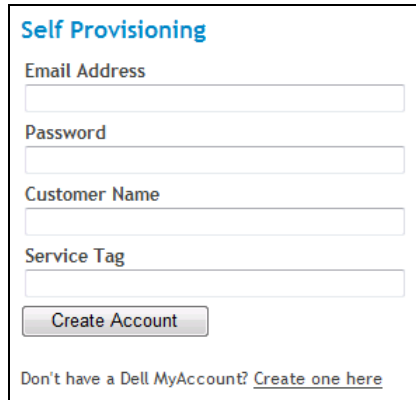
- Your Dell MyAccount or Premier username and password
- A Windows virtual machine or physical server upon which to run the SilverStreak proxy
- Administrative credentials (username and password) for all Dell servers and PowerVault storage devices that you plan to monitor with the Dell PSM Portal
- Dell OpenManage™ Server Administrator (OMSA) installed on the Windows and Linux systems that you plan to monitor with the Dell PSM Portal
- The service tag number of a Dell server or PowerVault storage device covered under an active Dell ProSupport contract

**Procedure:** To Provision Your Dell PSM Portal Account

1. **Open your supported web browser (Internet Explorer 7 or 8 or Firefox) and navigate to <http://www.dell.com/proactive>.**
2. **Click on the *Get Started Now* link.**
3. **Ensure that you have all of the information listed on that page at hand, then click on the *Continue* button.**
4. **Read the end user licensing agreement (EULA) and click on the *Agree* link to continue.**
  - a. **Or click on the *Disagree* link to abandon the operation.**

The Self-Provisioning screen appears. See [Figure 1-2](#) on [page 1-9](#).

Figure 1-2. Dell PSM Portal Self Provisioning Screen



Self Provisioning

Email Address

Password

Customer Name

Service Tag

Create Account

Don't have a Dell MyAccount? [Create one here](#)

5. Enter the following information into the corresponding text fields:
  - a. **Email Address** — The email address that you wish to associate with this account
  - b. **Password** — The password that you wish to associate with the email address
  - c. **Customer Name** — Your company or organisation name
  - d. **Service Tag** — The service tag associated with a Dell server or PowerVault storage device covered under an active Dell ProSupport contract
6. Click on the **Create Account** button.
  - a. Or, if you do not yet have a Dell MyAccount or Premier username and password, click on the **Create one here** link to be redirected to the MyAccount creation page. Once the account is created, repeat from [Step 1](#).

The display refreshes to your newly-created Dell PSM Portal environment, where you are prompted to add secondary alert and support contact users.

An Initial Account Creation email is sent to the configured email address which contains a link to the Dell PSM Portal login page.



**Caution:** You must always use the login page to log into the Dell PSM Portal. Attempting to use the Self Provisioning page to log in will result in an error. If you attempt to use the Registration/Sign In page to log in, the system redirects you to the Login page

If you need additional assistance contact Dell Technical Support in your country and request support for Dell Proactive Systems Management.

## Logging Into the Portal

---



**Note:** You can access the Dell PSM Portal using one of the following Web browsers:

- Microsoft Internet Explorer versions 7 and 8
  - Mozilla Firefox
- 

**Procedure:** To Log into the Dell PSM Portal

1. **Navigate with your Web browser to <http://www.dell.com/proactive>.**
2. **Read the End User Licence Agreement (EULA) and click on the *AGREE* link.**
3. **Select the *Use Existing* radio button, then click on the *Continue* button to display the Login screen.**

See [Figure 1-3](#).

**Figure 1-3. Dell PSM Portal Login Screen**

The screenshot shows a login form with the following elements:

- Title: **Sign In** (in blue text)
- Field 1: **Email Address** (with an input box)
- Field 2: **Password** (with an input box)
- Button: **Sign In** (a rectangular button below the password field)



**Note:** If you enter incorrect login credentials 6 consecutive times your account is locked. Please contact Dell Technical Support to reactivate your account.

---

4. **Enter your email address and password, then click on the *Sign In* button.**
  - a. **If your username or password is incorrect, you will be prompted to re-enter.**
  - b. **If you have forgotten your password, click on the *Forgot Password* link.**



**Note:** If you do not yet have a Dell MyAccount login, create one in the create a new account section, at <http://ecomm.dell.com/myaccount/login.aspx>.





If you have a Dell MyAccount login but have not yet provisioned your Dell PSM Portal account, follow the steps in “[To Provision Your Dell PSM Portal Account](#)” on [page 1-8](#).

---

The Home screen displays. See [Figure 1-4](#).

**Figure 1-4. Home Screen**

RisingStar

| Domains                 |          |  |           |  |   |
|-------------------------|----------|--|-----------|--|---|
| Domain Name             | Groups   | Primary Contact  | Devices   | Open Alerts  |   |
| <a href="#">RSV1</a>    | 2        | <a href="mailto:dummy@example.com">dummy@example.com</a> | 30        |  30 |  <a href="#">Start a Discovery</a>     |
| <a href="#">Storage</a> | 1        | <a href="mailto:dummy@example.com">dummy@example.com</a> | 6         |  |  <a href="#">Start a Discovery</a>     |
| <a href="#">Fred</a>    | 1        | <a href="mailto:dummy@example.com">dummy@example.com</a> | 0         |  |  <a href="#">Download SilverStreak</a> |
| <b>Totals</b>           | <b>4</b> |  | <b>36</b> | <b>30</b>  |   |

| Discoveries Started in the Past Week |                  |                                   |                                   |          |
|--------------------------------------|------------------|-----------------------------------|-----------------------------------|----------|
| Status                               | IP Address/Range | Started                           | Completed                         | Progress |
| Complete                             | 10.9.102.26      | Wednesday, July 14, 2010 11:38 AM | Wednesday, July 14, 2010 12:09 PM | 100      |



**Tip:** All informational screens in the Dell PSM Portal contain breadcrumbs or visual cues to where the current screen is situated in the user interface, below the main navigation bar.

Email addresses and action links are live hypertext links, enabling you to immediately send an email, open a screen (such as *Open Alerts*) or perform an action (such as *Start a Discovery*).

## Quick Start

Once you are logged into the Dell PSM Portal, you can begin the “[Initial Configuration](#)” (see [page 2-1](#)). The following procedures, completed in order, will quickly configure Dell PSM Portal management of your Dell systems:

1. [Adding Users](#) (see [page 2-2](#))
2. [Creating a Management Domain](#) (see [page 2-4](#))
3. [Downloading and Installing SilverStreak](#) (see [page 2-6](#))
4. [Configuring SilverStreak Credentials](#) (see [page 2-13](#))
5. [Discovering Assets](#) (see [page 3-1](#))



---

# Chapter 2

## Initial Set-up

This chapter describes the initial set-up procedures that enable you to efficiently monitor your infrastructure with the Dell Proactive Systems Management Portal.

| Chapter Contents  | Page |
|---|------|
| • <a href="#">Initial Configuration</a>                   | 2-1  |
| • <a href="#">Adding Users</a>                            | 2-2  |
| • <a href="#">Creating a Management Domain</a>            | 2-4  |
| • <a href="#">Downloading and Installing SilverStreak</a> | 2-6  |
| • <a href="#">SilverStreak Configuration</a>              | 2-8  |
| • <a href="#">Configuring SilverStreak Credentials</a>    | 2-13 |
| • <a href="#">Configuring Customer Preferences</a>        | 2-20 |
| • <a href="#">Configuring Monitoring Policies</a>         | 2-26 |

## Initial Configuration

Perform the steps in the following sections, *in the specified order*, to configure the Dell PSM Portal.

## Adding Users

### Creating a Secondary Contact User Account



**Caution:** You **must** configure a secondary contact user **before performing any further configuration**. This user should be an organisational contact who is responsible for systems administration and monitoring.

This user account is required for these critical functions:

- Providing Dell with a back-up support contact
- Receiving alert notifications.

*If the primary user for your Dell PSM Portal account is no longer available, please contact Dell Technical Support to request a primary user change to another Dell MyAccount or Premier user. **Only Dell personnel can change the primary user for any Dell PSM Portal account.***

---

**Procedure:** To Create an Alert and Support Contact User Account

1. **Log into the Dell PSM Portal.**
2. **Select *Preferences*.**
3. **Select the *User Management* tab to display the User Management screen.**
4. **Click on the *Add User* icon.**

The Add User form displays. See [Figure 2-1](#).

**Figure 2-1. Add User Form**

The screenshot shows a web form titled "Add User Form". It contains the following fields and controls:

- Email Address:** A text input field containing "dummy@example.com".
- Role:** A dropdown menu with "User" selected.
- Country:** A dropdown menu with "United States" selected.
- Language:** A dropdown menu with "English" selected.
- Buttons:** A "Cancel" button with a red stop sign icon and a "Submit" button.

5. **Enter the user's *Email Address*.**
6. **Select the user's *Role* from the drop-down.**
  - **User** - has rights to manage devices, asset groups and alerts

- **Site Administrator** - has User rights, plus the ability to add, modify and delete users
7. Select the user's **Country** from the drop-down.
  8. Select the user's **Language** from the drop-down.
  9. Click on the **Submit** button.
    - a. Or click on the **Cancel** icon to abandon the operation.



**Note:** If you attempt to add an email address that has already been added, a prompt will ask you to supply a different address.

---

The browser refreshes to the User Management screen, which now displays the new user. Once their Dell PSM Portal account is created, the new user will receive a confirmation email, which includes a “welcome” message containing the primary user who created the secondary account and Dell MyAccount set-up instructions.

10. **The new user must then create a Dell MyAccount login, for the email address configured above, at the URL contained in the account confirmation email.**

Once the user's Dell MyAccount has been created, they can advance to the next procedure.

**Procedure:** To Enable User Access to the Dell PSM Portal

---



**Tip:** This procedure is performed by the new user to:

- Create their Dell MyAccount login
  - Enable their Dell PSM Portal access
- 

1. **Open your supported web browser (Internet Explorer 7 or 8, or Firefox) and navigate to <http://www.dell.com/proactive>.**
2. **Click on the *Get Started Now* link.**
3. **Ensure that you have all of the information listed on that page at hand, then click on the *Continue* button.**
4. **Read the end user licensing agreement (EULA) and click on the *Agree* link to continue.**
  - a. **Or click on the *Disagree* link to abandon the operation.**

The Registration/Sign In page displays. See [Figure 2-2](#) on [page 2-4](#).

**Figure 2-2. Registration/Sign In Page**



Registration / Sign In

Email Address

Password

Sign In

[Forgot Password](#) | [Register](#)

5. Enter the following information into the corresponding text fields:
  - a. **Email Address** — The email address that you wish to associate with this account
  - b. **Password** — The password that you wish to associate with the email address
6. Click on the **Sign In** button.
  - a. Or if you do not yet have a Dell MyAccount or Premier username and password, click on the **Register** link to be redirected to the MyAccount creation page. When the account is created, repeat Steps 1 through 6.

An Account Creation email will be sent to your configured email address which will contain a link to the Dell PSM Portal Login page. If you attempt to use the Registration/Sign In page to log in, the system redirects you to the Login page.

## Creating a Management Domain

A Management Domain in the Dell Proactive Systems Management Portal represents a site or network that can be monitored by a single SilverStreak agent. For each Management Domain you install only one SilverStreak.



**Tip:** For more granular control of monitoring and alerts, you can configure groups within a Management Domain.

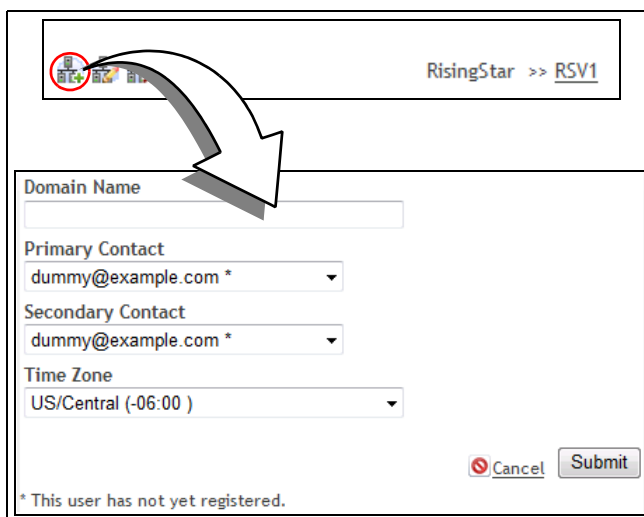
---

**Procedure:** To Create a Management Domain

1. **Log into the Dell PSM Portal.**
2. **Select *Assets* to display the *Assets* screen.**

If no Management Domains are configured, a warning message appears.
3. **Click on the *Add Domain* icon in the upper left-hand corner.**

The Add Domain form displays. See [Figure 2-3](#) on [page 2-5](#).

**Figure 2-3. Add Domain Screen**

RisingStar >> RSV1

Domain Name

Primary Contact  
dummy@example.com \*

Secondary Contact  
dummy@example.com \*

Time Zone  
US/Central (-06:00 )

Cancel Submit

\* This user has not yet registered.

4. Provide the following information in the Add Domain form:
  - a. Enter the *Domain Name*.
  - b. Select the *Primary Contact* from the drop-down.
  - c. Select the *Secondary Contact* from the drop-down.



**Note:** The primary and secondary domain contacts are used for receiving service contract alerts. See ["Configuring Customer Preferences"](#) on page 2-20.

- d. Select the *Time Zone* from the drop-down.



**Tip:** You can click in the drop-down to highlight the existing time zone name, then start typing the new time zone's name. The first matching time zone is selected. You can then scroll down the list to select the exact time zone you require.

5. Click on the *Submit* button.
  - a. Or click on the *Cancel* button to abandon the operation.

Once the Management Domain is created, you can see it listed in a tree view on the left side of the Assets screen.



**Note:** The Management Domain's initial status is *Not Connected*. This is expected, as the SilverStreak for this domain has not been configured.

---

## Downloading and Installing SilverStreak

You must create a Management Domain before SilverStreak can be downloaded, installed and configured. See "[Creating a Management Domain](#)" on [page 2-4](#).



**Tip:** SilverStreak software should be installed on a server or other computer that is operational at all times and **must** be able to send HTTPS (SSL) traffic through your company's firewall for communications back to Dell.

---

SilverStreak can only be installed when logged into the computer with Administrator rights. You can use either local Administrator credentials or a Windows domain administrator account.

To configure the SilverStreak, you will also require an account that allows access through any proxy server that your company may use.



**Note:** To enable the monitoring of systems in your network, you must have accounts that have Administrator rights to **each monitored system**. You can use multiple accounts, with Administrator rights to different systems.

---

## Downloading and Installing SilverStreak from the Dell PSM Portal



**Tip:** Because each SilverStreak installer package is customised for the specific domain that you select, you must perform this procedure once for each Management Domain. You cannot re-use a single SilverStreak installer package for multiple Management Domains.

---

**Procedure:** To Download the SilverStreak Installer

1. **Log into the Dell PSM Portal from the computer upon which SilverStreak will be installed.**
2. **Select Assets.**
3. **Select a Management Domain from the tree listing on the left side of the Assets screen.**
4. **Click on the *Download SilverStreak* link.**

The Download SilverStreak dialogue displays.



**Tip:** If the Download SilverStreak dialogue does not display, see the [FAQ](#) section for possible solutions.

5. **When prompted, click on the Download button.**
  - a. **Or click on the Cancel button to abandon the operation.**
6. **When prompted, click on the *Run* button to extract and run the SilverStreak Install Wizard application.**  
The splash dialogue displays.
7. **Click on the *Next* button to proceed to the Licence Agreement.**
8. **Read the agreement, then select the *I agree...* radio button.**
9. **Click on the *Next* button to proceed to the SilverStreak Service Account dialogue.**

See [Figure 2-4](#).

- a. **If you do not agree to the agreement, select the *I disagree...* radio button, then click on the *Cancel* button to exit the installation process.**

**Figure 2-4. SilverStreak Service Account**

10. **Enter the username and password of an account with local system or Windows domain Administrator privileges.**

**11. Click on the *Next* button.**

If you installed SilverStreak using an account that is not explicitly defined as a member of the host's local Administrator group, you will see an Account Error message dialogue, indicating that the installer is unable to verify the account.



**Note:** This occurs even if the account is part of a global group that is granted local Administrator group privileges.

---

- a. **Correct the credentials in order to continue the installation. The account must be explicitly defined as a member of the host's local Administrator group.**
  - b. **Or click on the *Yes* button to cancel the installation.**
- 



**Note:** If your credentials are incorrect, you will have to uninstall, then reinstall SilverStreak to correct them.

---

**12. Click on the *Install* button to install SilverStreak.**

**13. When SilverStreak has finished installing, click on the *Finish* button to exit the wizard.**

## SilverStreak Configuration

You can change basic SilverStreak configuration parameters using the SilverStreak Configuration utility. You can also use this utility to add, edit or delete locally-stored credentials that are used for device discovery and monitoring. See "[Configuring SilverStreak Credentials](#)" on [page 2-13](#).



**Note:** Changes made using this utility do not take effect until either of these buttons are selected:

- *Apply* (applies changes and leaves the screen open)
  - *OK* (applies changes and closes the screen)
- 

**Procedure:** To Modify the SilverStreak Configuration

**1. In the Windows task bar click on *Start* > *Programs* > *SilverStreak* > *SilverStreak Config*.**

The SilverStreak Configuration utility consists of three tabbed panes:

- [General](#) (see [page 2-9](#))
- [Configuration](#) (see [page 2-9](#))



- Updates (Does not apply to the Dell PSM Portal)



**Tip:** Many networks require the configuration of local HTTP proxy credentials before SilverStreak can successfully communicate with the Dell PSM Portal server over SSL. See “[HTTP Proxy Configuration](#)” on [page 2-11](#) for instructions.

---

## General

In the General pane you can:

- Stop and start the SilverStreak service



**Note:** The SilverStreak service starts automatically, unless there is a problem with your SilverStreak service credentials. See “[Configuring SilverStreak Credentials](#)” on [page 2-13](#).

- View SilverStreak status and connection information



**Note:** The Credentials button will initially be inactive until successful communication with the Dell PSM Portal server has been established. This may take anywhere from 2 to 10 minutes. See “[Configuring SilverStreak Credentials](#)” on [page 2-13](#) for more information about configuring SilverStreak credentials.

---

**Procedure:** To Start the SilverStreak Service

1. **Click on the Start button.**
  - a. **If the SilverStreak service does not start correctly, you may need to modify your SilverStreak service credentials or the Configuration.**  
See “[Configuring SilverStreak Credentials](#)” on [page 2-13](#).

**Procedure:** To Stop the SilverStreak Service

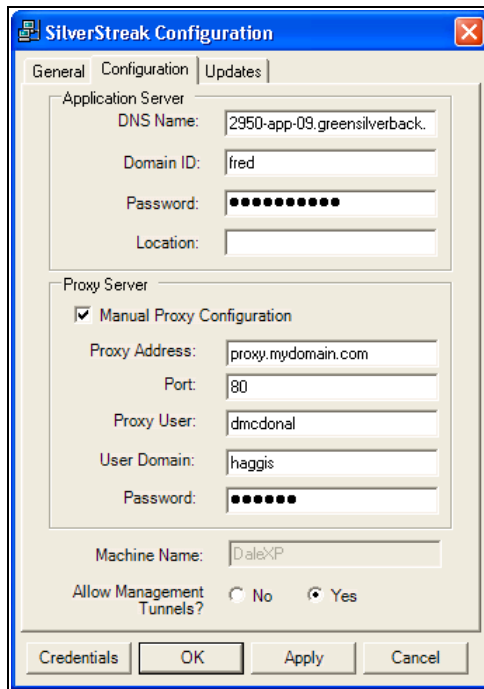
1. **Click on the Stop button.**

## Configuration

**Procedure:** To Change the SilverStreak Configuration

1. **Click on the Configuration tab.**  
See [Figure 2-5](#) on [page 2-10](#).

Figure 2-5. Configuration Tab



In the Configuration pane you can view and/or modify:

### Host Configuration

- View the SilverStreak host Machine Name
- Allow or disallow Management Tunnels (SilverStreak Remote Access Sessions)



**Caution:** To ensure proper monitoring operations, make sure that the *Allow Management Tunnels* option is configured to **No**.

---

## Dell RIM Server Configuration

---



**Caution:** The Dell RIM Server configuration, Domain ID and password information are populated automatically. **Do not change this information without first contacting Dell PSM Portal [Support](#).**

---

**Procedure:** To Change the Dell RIM Server Configuration

1. **Stop the SilverStreak service by clicking on the *Stop SilverStreak Service* button in the SilverStreak Configuration utility's [General](#) tab.**
2. **Enter the Dell PSM Portal application server's *DNS Name* to point SilverStreak to a different Dell PSM Portal server.**

Using the Dell PSM Portal server's DNS name rather than its IP address ensures that SilverStreak will continue to operate normally in the unlikely event of a Dell PSM Portal server failover to a different host.

3. **Enter the *Domain ID* (remote Management Domain) that SilverStreak monitors.**

The Domain ID is a reference to the internal Management Domain ID within the Dell RIM server. It is not user-visible in the Dell PSM Portal and does not reference anything within your local network.

4. **Enter the *Password*.**

This is required if you change the Domain ID. Ensure that you have the correct password; otherwise, SilverStreak will be unable to monitor the Management Domain.

5. **Enter an optional *Location*.**

This field is provided as an organisational convenience, and is not mandatory.

6. **Click on the *Apply* button to commit your changes.**
  - a. **Or click on the *Cancel* button to abandon the operation.**
7. **Click on the *Start SilverStreak Service* button in the SilverStreak Configuration utility's [General](#) tab.**

### HTTP Proxy Configuration

If your network uses an HTTP proxy server to communicate to the Internet, you must provide the correct proxy information, including the user name, password and domain information.

**Procedure:** To Configure SilverStreak to Use an HTTP Proxy Server

**1. Configure your Web browser to use the proxy server.**



**Note:** SilverStreak identifies the proxy server using these settings. You must always set these in your Web browser **before** modifying SilverStreak's proxy configuration.

---

**a. In Internet Explorer:**

- Open Internet Explorer and then navigate to *Tools > Internet Options*.
- Click on the *Connection* tab and then click on the *LAN Settings* button.
- Select the *Use a proxy server* tick box and then enter the HTTP proxy server's IP address and port.
- Click on the *OK* button to dismiss the LAN Settings dialogue and then click on the *OK* button to dismiss the Internet Options dialogue.

**b. In Firefox:**

- Navigate to *Tools > Options > Advanced*.
- Click on the *Network* tab, then click on the *Settings* button.
- Select the *Manual proxy configuration* radio button and then enter the HTTP proxy server's IP address and port.
- Click on the *OK* button to dismiss the Networks tab and then click on the *OK* button to dismiss the Options dialogue.

2. **Stop the SilverStreak service by clicking on the *Stop SilverStreak Service* button in the SilverStreak Configuration utility's [General](#) tab.**
3. **Click on the *Configuration* tab in the SilverStreak Configuration utility.**
4. **Select the *Manual Proxy Configuration* tick box to activate the Proxy Server configuration fields.**
5. **Enter the following information into the respective fields:**
  - a. *Proxy Address* — The IP address of the HTTP proxy server
  - b. *Port* — The proxy server's HTTP port number (defaults to port 80)
  - c. *Proxy User* — Your Windows domain username
  - d. *User Domain* — The name of the Windows domain to which your user belongs
  - e. *Password* — Your Windows domain password
6. **Click on the *Apply* button to save your changes.**

- a. Or click on the *Cancel* button to discard your changes and dismiss the SilverStreak Configuration utility.
7. Click on the *Start SilverStreak Service* button in the SilverStreak Configuration utility's [General](#) tab.
8. Validate that SilverStreak is connecting to the Dell PSM Portal server properly.
9. If the connection fails, re-examine your settings and make any needed corrections.

## Configuring SilverStreak Credentials

SilverStreak enables you to remotely monitor and manage your managed infrastructure without any of the credentials leaving your premises. All usernames and passwords are kept on your SilverStreaks.

SilverStreak credentials are encrypted using a 1024-bit, 3DES public key. They cannot be accessed in any way other than via the SilverStreak configuration tool.



**Caution: Do not attempt to edit the credentials XML file with any tool other than the SilverStreak Credentials dialog!** Doing so will corrupt the credentials, causing the monitoring of devices that reference the credentials to fail once the credentials have synchronised with the Dell PSM Portal application server.

**Procedure:** To Manage SilverStreak Credentials

1. In the Windows task bar click on *Start > Programs > SilverStreak > SilverStreak Config*.
2. Click on the *Credentials* button to display the Remote Credentials dialogue window.
3. Click on the *Credentials* button.
  - a. If this is the first time that you have used remote SilverStreak credentials, the Set Password for Remote Credentials dialogue will display.  
See [Figure 2-6](#) on [page 2-14](#).
  - b. If you have already set an encryption/decryption password, the SilverStreak Credentials dialogue will display.

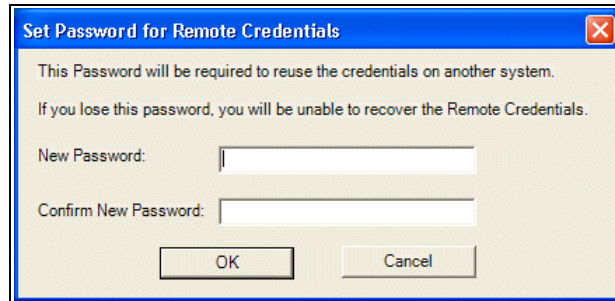
You can perform the following credentials operations directly on the SilverStreak host computer:

- [Create an Encryption/Decryption Password](#) (see [page 2-14](#))
- [Add Remote Credentials](#) (see [page 2-14](#))
- [Edit Remote Credentials](#) (see [page 2-18](#))

- [Delete Remote Credentials](#) (see [page 2-18](#))
- [Back-up Remote Credentials](#) (see [page 2-18](#))
- [Disaster Recovery](#) (see [page 2-19](#))

## Create an Encryption/Decryption Password

**Figure 2-6. Set Password for Remote Credentials Dialogue**



This dialogue enables you to set an encryption/decryption password to protect your credentials using a 1024-bit, 3DES public key.

**Procedure:** To Create an Encryption/Decryption Password

**1. Enter a password into the *New Password* field.**

Should you take the current SilverStreak offline and then install SilverStreak on a different computer, this password is required in order for you to reuse your SilverStreak credentials on the new SilverStreak.

**2. Re-enter the password into the *Confirm Password* field, then click on the *OK* button to display the SilverStreak Credentials dialogue.**

**3. Continue to “[Add Remote Credentials](#)” below.**

## Add Remote Credentials

**Procedure:** To Add Remote Credentials

**1. In the SilverStreak Credentials dialogue, click on the *Add* button to display the Manage Credential dialogue.**

See [Figure 2-7](#) on [page 2-15](#).



**Note:** Although you can configure Intel® vPro™ and Navisphere™ credentials in the SilverStreak Credentials dialogue, they are not currently used or supported by the Dell Proactive Systems Management Portal.

---

**Figure 2-7. Manage Windows Credential Dialogue**

The screenshot shows a 'Manage Credential' dialog box. At the top, there is a 'Credential Type' dropdown menu currently set to 'Windows', with a '\* Required' label to its right. Below this is a tab labeled 'Windows'. The main content area contains several input fields: 'Name' (with a '\*' required), 'Description' (a large text area), 'Windows Domain', 'User Name' (with a '\*' required), 'Password', and 'Confirm Password'. At the bottom of the dialog are 'Add' and 'Cancel' buttons.

The Manage Credential dialogue defaults to Windows. You can select a different type from the *Credential Type* drop-down.

**2. Enter a Name for the credential.**

The maximum size of this field is 40 characters.

**3. Optionally, enter a Description for the credential.**

You can enter a description of the credential, up to a maximum of 1000 characters.

You can also enter HTML links here in the format "http//: <target>", "https//: <target>" or "mailto: <email\_address>". The quotation marks are mandatory for HTML links.

**4. Enter the required authentication information for the selected credential type:**

- [Windows](#) (see [page 2-16](#))
- [SNMP](#) (see [page 2-16](#))

- [SSH](#) (see [page 2-17](#))



**Note:** VMware/Linux systems require both [SNMP](#) and [SSH](#) credentials. Dell PowerVault MD3000, MD3000i, MD3200i and MD3220i storage devices require [SNMP](#) credentials. Dell PowerVault NX2000, NX3000 and NX3100 storage devices require [Windows](#) credentials.

---

### **Windows**

- If applicable, enter the name of the *Windows Domain* to which the device belongs.
- Enter the username of an Administrator account for the device into the *Username* field.
- Enter the Administrator account *Password* for the device.
- Confirm the password by retyping it into the *Confirm Password* field.



**Tip:** If SilverStreak has been installed and is running using a Windows domain administrator account, it may be necessary to use Kerberos-formatted usernames (e.g. <username>@<domain.FQDN>)\* instead of NTLM-formatted usernames (e.g. <domain>\<username>) when creating Windows credentials.

---

\* FQDN = Fully Qualified Domain Name

### **SNMP**

- Enter the SNMP device's *Read Community String*.  
The SNMP Read community string defines the relationship between an SNMP server and its client systems. The community string functions as a client access control password to the server.



## SSH

Figure 2-8. Manage SSH Credential Dialogue

The screenshot shows a 'Manage Credential' dialog box with a blue title bar. The 'Credential Type' dropdown menu is set to 'SSH'. Below the dropdown, there is a tab labeled 'SSH'. The main area of the dialog contains several input fields: 'Name', 'Description', 'User Name', 'Password', and 'Confirm Password'. Below these fields is a checkbox labeled 'Run As'. Underneath the checkbox are three more input fields: 'Run-As User Name', 'Run-As Password', and 'Run-As Confirm Password'. At the bottom of the dialog, there are two buttons: 'Add' and 'Cancel'.

- Enter the username of a valid user account for the device into the *Username* field.
  - Enter the account's Password into the *Password* field.
  - Confirm the password by retyping it into the *Confirm* field.
  - Enter the username of a valid, root-level user account for the device into the *Run-As Username* field.
  - Enter the account's password into the *Run-As Password* field.
  - Confirm the password by retyping it into the *Confirm Run-As Password* field.
5. Click on the **Add** button to save your work.
- a. Or click on the **Cancel** button to abandon the operation without making any changes.

The display refreshes to the SilverStreak Credentials dialogue, which now includes the newly-added credential.

## Edit Remote Credentials

---



**Note:** You cannot edit a SilverStreak credential's name.

---

**Procedure:** To Edit Remote Credentials

1. **Click on the *Credentials* button to display the SilverStreak Credentials dialogue.**  
See [Figure 2-7](#) on [page 2-15](#).
2. **Select the credential that you wish to edit.**
3. **Click on the *Edit* icon to display the Manage Credential dialogue.**  
The dialogue is pre-populated with the selected credential's information.
4. **Proceed to [Step 3](#).**  
See [page 2-15](#).

## Delete Remote Credentials

**Procedure:** To Delete Remote Credentials

1. **Click on the *Credentials* button to display the SilverStreak Credentials dialogue.**  
See [Figure 2-7](#) on [page 2-15](#).
2. **Select the credential that you wish to delete, then click on the *Delete* icon.**  
A new dialogue appears, asking you to confirm the deletion.
3. **Click on the *OK* button to confirm the deletion.**
  - a. **Or click on the *Cancel* button to abandon the deletion.**The display refreshes to the SilverStreak Credentials dialogue, which will now not include the deleted credential.

## Back-up Remote Credentials

To guard against an extended service disruption and to aid disaster recovery in the event of hardware or software failure on the SilverStreak host computer, the best practice is to back-up and store your SilverStreak credentials to a secure location. The Dell PSM Portal provides an easy way for you to accomplish this.

---

**Procedure:** To Back Up Remote Credentials

1. **Click on the *Credentials* button to display the SilverStreak Credentials dialogue.**

See [Figure 2-7](#) on [page 2-15](#).

2. **In the SilverStreak Credentials dialogue, click on the *Back-up* button.**

A *Save As* dialogue appears, prompting you to save the credentials XML file to the default location on the SilverStreak host computer.



**Tip:** Dell strongly recommends that you choose a another location, on a different secure computer, in the event of a hardware or software failure on the SilverStreak host computer.

---

3. **Browse to the desired location, then click on the *Save* button.**

Your SilverStreak credentials are now backed up.

## Disaster Recovery

Although unlikely, it is possible that the encryption/decryption password could become corrupted. If that happens, the following dialogue will display when you click on the SilverStreak Configuration utility's *Credentials* button.

You have two possible courses of action:

- [Reset the Encryption/Decryption Password](#) (see below)
- [Erase and Recreate All SilverStreak Credentials](#) (see below)

### ***Reset the Encryption/Decryption Password***

**Procedure:** To Reset the Encryption/Decryption Password

1. **Click on the *Reset Password* button to display the Set Password dialogue.**
2. **Start again at Step 1 of “[Create an Encryption/Decryption Password](#)” on [page 2-14](#).**

### ***Erase and Recreate All SilverStreak Credentials***

**Procedure:** To Erase and Recreate All SilverStreak Credentials

1. **Click on the *Erase Credentials* button. A confirmation dialogue appears.**
2. **Click on the *OK* button. An information dialogue appears**
3. **Click on the *OK* button to dismiss the dialogue.**

4. **Start again at Step 1 of “Reset the Encryption/Decryption Password” on page 2-19.**

You can now return to the Dell Proactive Systems Management Portal.

## Configuring Customer Preferences

The Dell PSM Portal Preference pane allows you to:

- Create and modify user accounts (see Chapter 2, “User Management”, in the *Dell Proactive Systems Management Portal User Guide*)
- Change [Service Contract Report Notification Options](#) (see below)
- Change managed device [Remote Diagnostics Settings](#) (see [page 2-21](#))
- Change [Alerting Options](#) (see [page 2-23](#))

### Service Contract Report Notification Options

You can customise notification options on a per-customer basis.



**Tip:** You may receive a service contract expiry email if a service contract, that will automatically renew at a different service level, is due to expire. You can safely ignore that email, as your service contract will automatically renew at the predetermined service level.

---

**Procedure:** To Customise Service Contract Expiry Notices by Customer

1. **Select *Preferences*, then select the *Notifications* tab.**

See [Figure 2-9](#).

**Figure 2-9. Customer Notifications Pane**

RisingStar

### Service Contract Expirations

Do you wish to receive notifications of service contract expirations by email?

Yes  No

How far in advance would you like to receive these notifications?

2 Months

Optionally provide the email address of your Dell Channel partner to receive a copy of these notifications

Submit

2. **Click on the *Yes* radio button.**

---

3. **Select the service contract expiry notifications *interval* from the *drop-down*.**

You can choose any notification interval from one (1) month to six (6) months in advance. The default setting is two (2) months in advance, which sends you a monthly report on service contracts that are due to expire within the next two months.



**Note:** If this option is enabled, both the primary and secondary contacts for each Management Domain will receive reports for their respective domains.

The service contract expiry notification email is not sent immediately - it is sent once per month, in the first week of each month. You can retrieve the same data on demand using the Service Contract Report. See "Viewing the Service Contract Report" in the *Dell Proactive Systems Management Portal User Guide*.

---

4. **Optionally, you can enter your Dell channel partner's *email address* if you want them to receive the notifications as well.**



**Tip:** If the channel partner's email address later changes, you must change it in the *Preferences > Notifications* tab. Otherwise the channel partner will not receive notifications.

---

5. **Click on the *Submit* button.**

## Remote Diagnostics Settings

You can use the following remote diagnostics tools with the Dell PSM Portal:

- Dell **System E-Support Tool (DSET)** — For server devices and Dell PowerVault NX2000, NX3000 and NX3100 storage devices, DSET can run at discovery, upon alert generation and on demand.
- **Lasso** — For Dell PowerVault MD3000, MD3000i, MD3200i and MD3220i storage devices, Lasso can run upon alert generation and on demand.



**Tip:** Because Dell PowerVault NX2000, NX3000 and NX3100 devices are managed as servers, the Dell PSM Portal uses DSET to gather diagnostics information from them, not Lasso.

---

You can customise settings for these tools in three ways:

- By Customer
- By Management Domain
- By Group

You must first perform the following tasks in order for the Dell PSM Portal to run Lasso diagnostics:

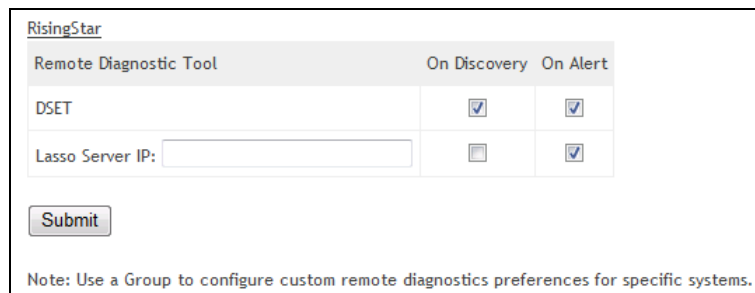
- Enter the Lasso server's IP address in the *Preferences > Remote Diagnostics* screen.
  - If you attempt to run Lasso without first performing this task, the Dell PSM Portal displays the *Preferences > Remote Diagnostics* screen.
- Discover the Dell Modular Disk Storage Manager (MDSM) host. This is the device upon which Lasso is run.

**Procedure:** To Automatically Execute DSET or Lasso upon Discovery and/or Alert Generation:

1. **Select the organisation for which you wish to change remote diagnostics settings:**
  - a. **For a Customer, select *Preferences*, then select the *Remote Diagnostics* tab.**
  - b. **For a Management Domain, select *Preferences*, then select the *Remote Diagnostics* tab, then select the domain icon in the tree view.**
  - c. **For a Group, select *Preferences*, then select the *Remote Diagnostics* tab, then select the group icon in the tree view.**

See [Figure 2-10](#).

**Figure 2-10. Remote Diagnostics Pane**



| Remote Diagnostic Tool                | On Discovery                        | On Alert                            |
|---------------------------------------|-------------------------------------|-------------------------------------|
| DSET                                  | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Lasso Server IP: <input type="text"/> | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |

Note: Use a Group to configure custom remote diagnostics preferences for specific systems.



**Tip:** DSET will automatically execute against successfully-discovered server assets. If you do not want that to occur, you must change that setting **prior to discovering devices**.

2. **In the form table's DSET row, ensure that the *On Discovery* and *On Alert* tick boxes are selected.**

The default setting is *Enabled*. You can toggle the tick boxes on and off to change DSET behaviour. This allows DSET to generate a report upon device discovery and upon receipt of a hardware alert.

---

This report is automatically uploaded to Dell Technical Support.

3. **In the form table's Lasso row:**
  - a. **Enter the Lasso server's IP address into the *Lasso Server IP* field.**
  - b. **Ensure that the *On Alert* tick box is selected.**

The default setting is *Enabled*. You can toggle the tick box on and off to change Lasso behaviour. This will allow Lasso to generate a report upon receipt of a storage hardware alert.

This report is automatically uploaded to Dell Technical Support and is not viewable from the Dell PSM Portal.



**Note:** Dell Technical Support will proactively review these reports *unless the Auto Support Case policy is disabled for a managed device*. See "[Configuring Monitoring Policies](#)" on [page 2-26](#).

If you have disabled the Auto Support Case policy you can manually open a case by clicking on either the *Support Chat* or *Support Email* buttons or by calling Dell Technical Support. See "[Support](#)" in [Appendix 1](#).

---

4. **For a Customer, click on the *Submit* button to commit your changes.**
5. **For a Management Domain, click on the *Override Customer Settings* button to display the Remote Diagnostics panel.**
  - a. **Make your changes.**
  - b. **Click on the *Submit* button to commit your changes.**
  - c. **Or click on the *Revert to Customer Settings* button to abort the operation.**
6. **For a Group, click on the *Override Domain Settings* button to display the Remote Diagnostics panel.**
  - a. **Make your changes.**
  - b. **Click on the *Submit* button to commit your changes.**
  - c. **Or click on the *Revert to Domain Settings* button to abort the operation.**

## Alerting Options

You can customise your Email Policy filtering preferences, Auto-Support Case Policy alerting preferences, and Critical Alert escalation rules to suite your organisational requirements.



**Note:** When new alerts are generated upon devices with existing Auto Support Case alerts, the new alerts are appended to the existing cases. No new cases are created and generated notification emails for the new alerts indicate the associated case numbers. When a case is closed, any appended alerts are also closed.

**Procedure:** To Change Email Policy Filtering Options

**1. Select the organisation for which you wish to change alerting options:**

- For a Customer, select *Preferences*, then select the *Alerts* tab.
- For a Management Domain, select *Preferences*, then select the *Alerts* tab, then select the domain icon in the tree view.
- For a Group, select *Preferences*, then select the *Alerts* tab, then select the group icon in the tree view.

The Alerts panel displays. See [Figure 2-11](#).

**Figure 2-11. Alerts Pane**

**Email Policy Filtering Preferences**

Critical  Major  Minor

**Auto Support Case Policy Notification Preferences**

Mission Critical Systems

Contact me by  
 Email  Phone

Phone Notification Schedule  
9:00 AM to 6:00 PM US/Central (-06:00)

Enterprise-Wide Contract Systems

Contact me by  
 Email  Phone

Phone Notification Schedule  
9:00 AM to 6:00 PM US/Central (-06:00)

Phone notifications include an automated email at the time of the alert. Dell Tech Support will contact you by phone during your scheduled notification hours.

**Critical Alert Escalation Rules**

Send escalation email for all critical alerts (add up to 10 email addresses)

[Add](#)



- 
2. Select the **Email Policy Filtering Preferences** tick boxes that correspond to each alert criticality for which you wish to be notified by the Email Policy:
    - **Critical** — Receive alert notifications for critical alerts
    - **Major** — Receive alert notifications for major alerts
    - **Minor** — Receive alert notifications for minor alerts
  3. Select one or both of the following **Auto-Support Case Policy contract types**:
    - **ProSupport Mission Critical Systems** — Receive alert notifications for Dell ProSupport Mission Critical Systems
    - **ProSupport Enterprise-Wide Contract Systems** — Receive alert notifications for Dell ProSupport Enterprise-Wide Contract Systems



**Note:** Both contract types are selected by default.

---

4. Select the **Contact me by** radio button that corresponds to your preferred **Auto Support Case Alerts contact mode**:
  - **Email** — Receive alert notifications via the email address configured for your user account. No further action is required.
  - **Phone** — Receive alert notifications via a telephone number that you specify:
    - Enter your preferred telephone number into the *Phone* text field.
    - Select your preferred daily *Phone Notification Schedule* start/end hours and time zone from the drop-downs.



**Note:** If the notification schedule start time is later than the end time, notifications will be enabled overnight.

---

5. Enter any **Critical Alert Escalation Rules** email addresses to which you want emails sent for critical alerts only, then click on the **Add button**.

You may enter up to ten (10) email addresses.
6. **Commit your changes**:
  - a. For a Customer, click on the **Submit** button.
  - b. For a Management Domain, click on the **Override Customer Settings** button.
  - c. For a Group, click on the **Override Domain Settings** button.

## Configuring Monitoring Policies

Dell provides several Monitoring Policies that you can use to perform proactive monitoring and alert notification on your managed devices.



**Note:** Devices covered by Dell ProSupport for IT and Dell ProSupport for End User contracts can only use the *Email* contact type for Auto Support Cases.

---

You can configure a policy for devices in two ways:

- For a single device, or several devices, in a single operation from the Assets screen (see below)
- 



**Tip:** Applying a Monitoring Policy to more than 200 devices in a single operation can take some time and may even cause the operation to time out.

---

- For a single device from the Device Details screen (see [page 2-27](#))

**Procedure:** To Configure Device Monitoring Policies from the Assets Screen

1. **Select *Assets* to display the Assets screen.**
2. **Select the tick box(es) which correspond to the device(s) for which you wish to configure the policy.**

An *update polices* to drop-down list appears above the assets list.

3. **Select the *policy* from the drop-down list. You can select from:**
  - a. ***Auto Support Case*** — Automatically turns any alerts generated for managed assets into Dell Technical Support cases. You will receive an email notification with the case number.
  - b. ***Email*** — Automatically sends email about any alerts generated for managed assets to the primary and secondary contacts. Dell Technical Support cases are **not** automatically generated.
  - c. ***Ignore*** — No Monitoring Policies manage the assets, no alerts are generated and Dell Technical Support cases are **not** automatically generated. Emails will **not** be sent to the primary or secondary contacts. Dell recommends its use during scheduled maintenance windows for managed devices.
  - d. ***Unmanaged*** — Treats managed assets as if they were unmanaged. **No** alerts or cases are created. Dell recommends its use for assets that are not mission-critical, such as test or development devices. Service contract tracking **is** available for unmanaged devices.

---

The policy is now configured for each selected device.



**Note:** Auto Support Case is available for systems covered by Dell ProSupport for IT, Dell ProSupport for End User, Dell ProSupport Mission Critical and Dell ProSupport Enterprise-Wide contracts.

---

**Procedure:** To Configure Device Monitoring Policies from the Details Screen

1. **Select *Assets* to display the *Assets* screen.**
2. **Click on the *Device Name*.**  
The details of the selected asset display.
3. **Select the *Policy* tab.**
4. **Select the *radio button* next to the name of the Monitoring Policy that you wish to apply to the asset. You can select from:**
  - a. ***Auto Support Case*** — Automatically turns any alerts generated for managed assets into Dell Technical Support cases. You will receive an email notification with the case number.
  - b. ***Email*** — Automatically sends email about any alerts generated for managed assets to the primary and secondary contacts. Dell Technical Support cases are **not** automatically generated.
  - c. ***Ignore*** — No Monitoring Policies manage the assets, no alerts are generated and Dell Technical Support cases are **not** automatically generated. Emails will **not** be sent to the primary or secondary contacts. Dell recommends its use during scheduled maintenance windows for managed devices.
  - d. ***Unmanaged*** — Treats managed assets as if they were unmanaged. **No** alerts or cases are created. Dell recommends its use for assets that are not mission-critical, such as test or development devices. Service contract tracking **is** available for unmanaged devices.



**Note:** Auto Support Case is available for systems covered by Dell ProSupport for IT, Dell ProSupport for End User, Dell ProSupport Mission Critical and Dell ProSupport Enterprise-Wide contracts.

---

5. **Click on the *Apply Policy* button.**

The policy is now configured for the selected device.



---

# Chapter 3 Discovery

This chapter describes the Dell Proactive Systems Management Portal discovery process.

| Chapter Contents                                    | Page |
|---|------|
| • <a href="#">Discovering Assets</a>                | 3-1  |
| • <a href="#">Single Device or Range of Devices</a> | 3-3  |
| • <a href="#">Importing Devices from a File</a>     | 3-4  |
| • <a href="#">Device Typing</a>                     | 3-5  |
| • <a href="#">Verifying Discovery Results</a>       | 3-6  |

## Discovering Assets



**Tip:** SilverStreak must be downloaded and configured prior to discovering assets. See [“Downloading and Installing SilverStreak”](#) on page 2-6, [“SilverStreak Configuration”](#) on page 2-8 and [“Configuring SilverStreak Credentials”](#) on page 2-13 for more information.

The appropriate diagnostics tool (Dell System E-Support Tool [DSET] or Lasso) will be executed automatically on any device that is successfully discovered and managed. To change this setting, see [“Configuring Customer Preferences”](#) on page 2-20 **prior to device discovery**.

**Procedure:** To Start the Discovery Wizard

1. **Log into the Dell PSM Portal.**
2. **Select Assets.**
3. **Select a Management Domain from the tree listing on the left side of the Assets screen.**

#### 4. Click on the Start a *Discovery* icon to display the Discovery Wizard.



**Note:** If the Management Domain's SilverStreak is not configured, or is not working correctly, asset discovery for that domain will fail. You will see an error dialogue. You must correct the problem before re-attempting discovery.

**Figure 3-1. Discovery Wizard**

RisingStar >> RSV1

Discovery - RSV1 (Connected)

**Enter a Single IP Address**

[+Add](#)

**Enter a Range of IP Addresses**

to   
[+Add](#)

**Import**

To browse for an import file, click on the Browse button. Only .txt and .csv files, with one IP Address per line, are currently supported. Only valid IP Addresses will appear in the summary.

Filename  [Browse...](#) [Upload](#)

**Summary**

Review the information below before initiating discovery. If any information is incorrect, correct it before continuing. Discovery cannot be canceled once started.

**Select Credentials**

Define pre-existing authentication information that the Dell Managed Services Platform may need in order to access and monitor the devices.

Select All Credentials

MyDell.remote

IBM.remote

Public.remote

[Cancel](#) [Finish](#)

You can discover devices in two ways:

- [Single Device or Range of Devices](#) (see below)
- [Importing Devices from a File](#) (see [page 3-4](#))

---

## Single Device or Range of Devices

**Procedure:** To Discover One Device or a Range of Devices



**Caution:** Since discovering very large IP address ranges is time-consuming, Dell strongly encourages you to discover large ranges in several smaller stages. In addition, since the Dell PSM Portal is a server-only management system, you must avoid discovering desktop or laptop systems. This can serve as a guideline to dividing your IP address ranges into smaller stages for discovery.

1. **For a single asset, enter the asset's IP address in the *Enter a Single IP Address* text field.**
2. **For a range of assets, enter the starting and ending IP addresses in the *Enter a Range of IP Addresses* text field.**

A range discovery is a one-time scan of the entered IP address range.
3. **Click on the corresponding *Add* button.**

The IP address(es) you entered are displayed in the Summary table.
4. **Review the entries in the Summary table to ensure that they are correct.**
  - a. **If they are correct, continue to [Step 5](#).**
  - b. **If there are errors, click on the *Remove* icon, then go back to [Step 1](#).**
5. **Select the credentials that you want to use to discover the devices by ticking the *Select Credentials* tick boxes.**
  - a. **If you make a mistake, deselect the unwanted credentials.**



**Caution:** Multiple credentials can be used for device discovery. Ensure that the credentials you choose correspond to the device or range of devices and have Windows domain (or LDAP, NIS or the equivalent for Linux environments) administrator permissions, which are required to perform proper discovery.

If you discover devices using credentials that do not have the proper permissions, the credentials may succeed in logging into the devices but may not have the proper permissions to access the Windows Event Logs or syslogs. The devices will then display in the Assets screen but will not be profiled correctly.

If you encounter this issue:

1. Select the devices in the Assets screen.
2. Assign the proper credentials. See "Changing Credentials" in the *Dell Proactive Systems Management Portal User Guide*.

**6. Click on the *Finish* button to display a discovery initiation dialogue.**

Once you read and understand the dialogue text, you can click on the **X** icon to dismiss. The discovery will continue.

**a. Or click on the *Cancel* button to abandon the operation.**



**Tip:** Discovery can take some time. You can safely close your Web browser and do other tasks in the meantime before proceeding.

---

**7. Continue to “[Verifying Discovery Results](#)” on page 3-6.**

## Importing Devices from a File

**Procedure:** To Import Devices from a File



**Caution:** Since the Dell PSM Portal is a server-only management system, you must avoid discovering desktop or laptop systems. This can serve as a guideline to dividing your IP address ranges into smaller stages for import and discovery.

---

This feature enables you to import devices from a text file in either *.txt* or *.csv* format. Import files must contain only one column, with one IP address per line.

- 1. Click on the *Browse* button to display a Windows Explorer file selection dialogue.**
- 2. Browse to the appropriate file and then click on the *Open* button.**
- 3. Click on the *Upload* button.**

The IP addresses contained within the file are displayed in the Summary table.

- 4. Review the entries in the Summary table to ensure that they are correct.**
  - a. If they are correct, continue to [Step 5](#).**
  - b. If there are errors, click on the *Remove* icon, fix the errors in the import file, then go back to [Step 2](#).**
- 5. Select the credentials that you want to use to discover the devices by ticking the *Select Credentials* tick boxes.**
- 6. Click on the *Finish* button to display the discovery initiation dialogue.**
  - a. Or click on the *Cancel* button to abandon the operation**



---

## 7. Continue to “Verifying Discovery Results” on page 3-6.

---



**Tip:** Discovery can take some time. You can safely close your Web browser and do other tasks before proceeding to “Verifying Discovery Results” on page 3-6.

---

## Device Typing

Each device discovered by the Dell PSM Portal is automatically assigned a device type, reflected in the Assets screen’s OS column. See [Table 3-1](#) for currently-supported device types.

---



**Tip:** Each disk array in a Dell PowerVault SAN is classified as a separate storage device, with its own service tag. In addition, each Dell PowerVault SAN has two (2) physical network interfaces. These interfaces can be assigned IP addresses on different subnets; however, only the first discovered interface will be managed and reported upon, to eliminate duplicate alerts. The second will be ignored.

---

**Table 3-1: Device Types**

| System/OS                                  | Device Type/Icon | Icon |
|--|------------------|------|
| Windows Server                             | Server           |      |
| Linux Server                               | Server           |      |
| VMware® vCenter™ Server                    | Server           |      |
| VMware® vCenter™ Discovered Device         | Server           |      |
| ESX/ESXi Server                            | Server           |      |
| Dell PowerVault MD3xxx Series              | Storage          |      |
| Dell PowerVault NX2000, NX3000 and NX3100* | Storage          |      |

\* Dell PowerVault NX2000, NX3000 and NX3100 devices are discovered and classified in the Dell PSM Portal as storage devices, but managed as Windows servers. See “[Monitored Dell PowerVault Storage Asset System Requirements](#)” on page 1-6.

## Verifying Discovery Results

Once asset discovery has been initiated, you should ensure that the results are what you expect.

**Procedure:** To Verify Discovery Results

1. **Select *Home* to display the Dashboard.**
2. **Once the discovery operation is complete, select *Assets* to refresh the list of discovered devices.**

This list does not automatically refresh.



**Note:** If the assets do not appear at this point, or if they appear with incomplete make/model/service tag information and/or have credentials issues (indicated by a key icon), see "[FAQ](#)" for information and assistance.

Discovery is 100% complete when the Dell PSM Portal finishes gathering the service tag numbers for all discovered devices.

---

---

# Chapter 4

## Managing Groups and Management Domains

This chapter describes how to manage asset groups and Management Domains, using the Dell Proactive Systems Management Portal.

| Chapter Contents                               | Page |
|--|------|
| • <a href="#">Group Management</a>             | 4-1  |
| • <a href="#">Creating a Group</a>             | 4-2  |
| • <a href="#">Editing a Group</a>              | 4-3  |
| • <a href="#">Deleting a Group</a>             | 4-4  |
| • <a href="#">Domain Management</a>            | 4-5  |
| • <a href="#">Editing a Management Domain</a>  | 4-5  |
| • <a href="#">Deleting a Management Domain</a> | 4-7  |

### Group Management

You can use groups to assign different technical contacts for different devices. Technical contacts will receive alerts on monitored systems. For example, you could have groups with different administrators, such as:

- Windows Servers
- Linux Servers
- Dell PowerVault Storage Devices
- Production Servers
- Test Servers



**Note:** Using groups is optional; you can leave all devices in the Default group if that makes sense for your environment.

---

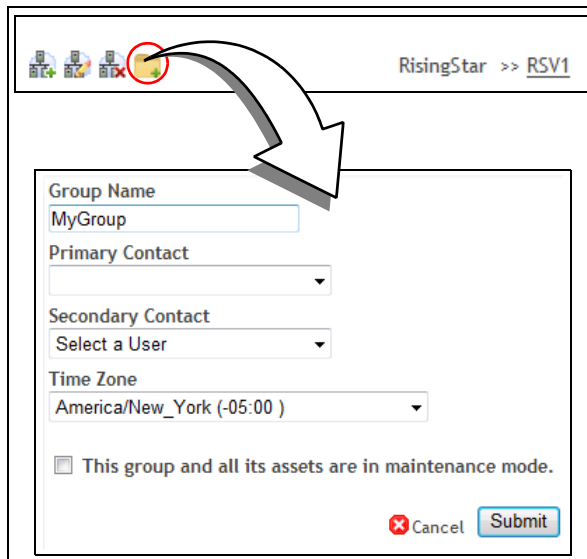
## Creating a Group

**Procedure:** To Create a Group

1. Select **Assets**, then select the group's parent Management Domain by selecting the domain's icon.
2. Click on the **Add Group** icon.

The Add Group screen displays. See [Figure 4-1](#).

**Figure 4-1.** Add Group Screen



The screenshot shows the 'Add Group' screen in the RisingStar portal. At the top right, it says 'RisingStar >> RSV1'. Below this is a toolbar with several icons; the 'Add Group' icon (a green plus sign) is circled in red, and a large white arrow points from it to the form below. The form has the following fields:

- Group Name:** A text input field containing 'MyGroup'.
- Primary Contact:** A dropdown menu.
- Secondary Contact:** A dropdown menu with the text 'Select a User'.
- Time Zone:** A dropdown menu with 'America/New\_York (-05:00)' selected.
- This group and all its assets are in maintenance mode.
- Buttons for 'Cancel' (with a red X icon) and 'Submit'.

3. Enter the **Group Name**.
4. Select the group's **Primary Contact** from the drop-down.
5. Select the group's **Secondary Contact** from the drop-down.



**Tip:** You can select any existing users as the primary and secondary group contacts. They don't have to be the parent Management Domain contacts.

---

6. Select the group's **Time Zone** from the drop-down.



**Tip:** You can click in the drop-down to highlight the existing time zone name, then start typing the new time zone's name. The first matching time zone is selected. You can then scroll down the list to select the exact time zone you require.

---

7. To temporarily suspend alert email notifications and Auto Support Case generation for all assets in the group, select the ***This group and all its assets are in maintenance mode*** tick box.

See “Maintenance Mode” in the *Dell Proactive Systems Management Portal User Guide* for more information about maintenance mode.

8. Click on the ***Submit*** button.
  - a. Or click on the ***Cancel*** button to abandon the operation.

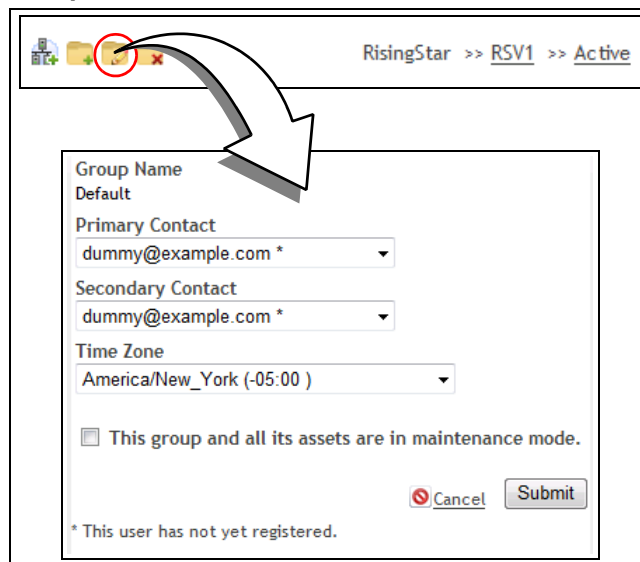
## Editing a Group

**Procedure:** To Edit a Group

1. Select ***Assets***, then select the group’s icon from the tree view.
2. Click on the ***Edit Group*** icon.

The Edit Group screen displays. See [Figure 4-2](#).

**Figure 4-2. Edit Group Screen**



RisingStar >> RSV1 >> Active

Group Name  
Default

Primary Contact  
dummy@example.com \*

Secondary Contact  
dummy@example.com \*

Time Zone  
America/New\_York (-05:00 )

This group and all its assets are in maintenance mode.

\* This user has not yet registered.

3. Enter the ***Group Name***.
4. Select the group’s ***Primary Contact*** from the drop-down.

**5. Select the group's *Secondary Contact* from the drop-down.**



**Tip:** You can select any existing users as the primary and secondary group contacts. They don't have to be the parent Management Domain contacts.

Users who have not logged into their accounts are indicated by asterisks ( \* ) next to their email addresses.

---

**6. Select the group's *Time Zone* from the drop-down.**



**Tip:** You can click in the drop-down to highlight the existing time zone name, then start typing the new time zone's name. The first matching time zone is selected. You can then scroll down the list to select the exact time zone you require.

---

- 7. To temporarily suspend alert email notifications and Auto Support Case generation for all assets in the group, select the *This group and all its assets are in maintenance mode* tick box.**
  - 8. Click on the *Submit* button.**
    - a. Or click on the *Cancel* button to abandon the operation.**
- 



**Tip:** You can also put a single device into maintenance mode. For information on how to put a single device into maintenance mode, see "Maintenance Mode" in the *Dell Proactive Systems Management Portal User Guide*.

---

## Deleting a Group

When you delete a group, all its contained assets are moved to the Default group. Those assets will continue to be monitored, but no further alerts are emailed to the former group's contact users. Instead, alerts will be emailed to the parent Management Domain contacts and the Default group contacts.

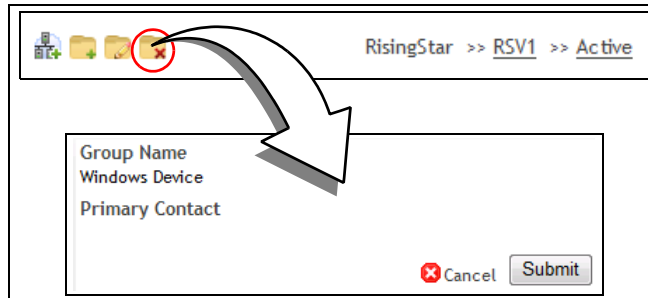
**Procedure:** To Delete a Group

- 1. Select *Assets*, then select the group's icon from the tree view.**
- 2. Click on the *Delete Group* icon.**

A dialogue window appears, prompting you to confirm the deletion.
- 3. Click on the *OK* button to dismiss the dialogue and continue the group deletion.**
  - a. Or click on the *Cancel* button to dismiss the dialogue and abandon the operation.**

The Delete Group screen displays. See [Figure 4-3](#).

**Figure 4-3. Delete Group Screen**



4. Click on the *Submit* button.
  - a. Or click on the *Cancel* button to abandon the operation.

## Domain Management

For information about creating a Management Domain, see [“Creating a Management Domain”](#) on [page 2-4](#).

### Editing a Management Domain

**Procedure:** To Edit a Management Domain

1. Select *Assets*, then select the Management Domain’s icon from the tree view.
2. Click on the *Edit Domain* icon.

The Edit Domain screen displays. See [Figure 4-4](#) on [page 4-6](#).

**Figure 4-4. Edit Domain Screen**

RisingStar >> RSV1

Domain Name  
RSVI

Primary Contact  
dummy@example.com \*

Secondary Contact  
dummy@example.com \*

Time Zone  
US/Central (-06:00 )

Cancel Submit

\* This user has not yet registered.

3. Enter the *Domain Name*.
4. Select the Management Domain's *Primary Management Contact* from the drop-down.
5. Select the Management Domain's *Secondary Management Contact* from the drop-down.



**Note:** The primary and secondary domain contacts are used for receiving service contract alerts. See [“Configuring Customer Preferences”](#) on [page 2-20](#).

Users who have not logged into their accounts are indicated by asterisks ( \* ) next to their email addresses.

---

6. Select the Management Domain's *Time Zone* from the drop-down.



**Tip:** You can click in the drop-down to highlight the existing time zone name, then start typing the new time zone's name. The first matching time zone is selected. You can then scroll down the list to select the exact time zone you require.

---

7. Click on the *Submit* button.
  - a. Or click on the *Cancel* button to abandon the operation.



---

## Deleting a Management Domain

When you delete a Management Domain, all of its contained assets and groups are also deleted. Those assets will no longer be managed.



**Caution:** When you delete an asset, all alerts associated with that asset are also deleted. This is an irrevocable action.

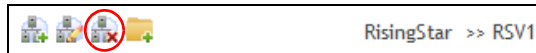
---

**Procedure:** To Delete a Management Domain

1. Select **Assets**, then select the **Management Domain's** icon from the tree view.
2. Click on the **Delete Domain** icon.

See [Figure 4-5](#).

**Figure 4-5.** Delete Domain Icon



A dialogue window appears, prompting you to confirm the deletion.

3. Click on the **OK** button to delete the domain.
  - a. Or click on the **Cancel** button to dismiss the dialogue and abandon the operation.

An informational dialogue window appears.

4. Click on the **OK** button to dismiss the dialogue window and return to the **Assets** screen.



---

# Appendix 1

## Support and FAQ

This chapter describes the currently-known anomalies and considerations for Dell Remote Infrastructure Monitoring software Release 1.4.

| Chapter Contents          | Page |
|---------------------------|------|
| • <a href="#">Support</a> | A-1  |
| • <a href="#">FAQ</a>     | A-1  |

## Support

If you require support for the Dell Proactive Systems Management Portal or SilverStreak, please contact Dell at the links below.

- For eSupport assistance with a device alert:
  - [http://support.dell.com/support/topics/global.aspx/support/chat/hardware\\_chat?c=us&l=en&s=gen](http://support.dell.com/support/topics/global.aspx/support/chat/hardware_chat?c=us&l=en&s=gen)
- For a listing of Dell Technical Support telephone numbers:
  - [http://www.dell.com/content/topics/global.aspx/services/prosupport/regional\\_contacts?c=us&l=en&s=gen](http://www.dell.com/content/topics/global.aspx/services/prosupport/regional_contacts?c=us&l=en&s=gen)

## FAQ

**Q.** I cannot log into the Dell PSM Portal.

**A.** You must enable cookies in your web browser.

***From Internet Explorer:***

1. Select **Tools > Internet Options** and then click on the **Privacy** tab.

2. Move the slider to the *Medium* security setting.
3. To enable cookies for the Dell PSM Portal, click on the *Sites* button.
4. Enter one of the following wildcard URLs into the text box:
  - \*.us.dell.com
  - \*.dell.com
5. Click on the *Allow* button, then click on the *OK* button to dismiss the *Trusted Sites* window.
6. Click on the *OK* button to dismiss the *Internet Options* window.

***From Firefox:***

1. Select *Tools > Options* and then click on the *Privacy* tab.
2. To enable cookies for the Dell PSM Portal, select the *Accept cookies from sites* tickbox, then click on the *Exceptions* button.
3. Enter one of the following wildcard URLs into the text box:
  - \*.us.dell.com
  - \*.dell.com
4. Click on the *Allow* button, then click on the *Close* button to dismiss the *Privacy* window
5. Click on the *OK* button to dismiss the *Options* window.

**Q.** Some Dell PSM Portal pages do not display properly in Internet Explorer.

- A.** Internet Explorer should be set to save encrypted pages to disk in order for some Dell PSM Portal user interface pages to display properly.
1. From Internet Explorer, click on *Tools > Internet Options* and then click on the *Advanced* tab.
  2. Scroll down until you see the "Do not save encrypted files to disk" option.
  3. Clear the tickbox and then click on the *Apply* button.
  4. Click on the *OK* button to dismiss the *Internet Options* window.

**Q.** I cannot download SilverStreak from Internet Explorer.

- A.** You must enable file downloads within Internet Explorer.
1. From Internet Explorer, click on *Tools > Internet Options* and then click on the *Security* tab.
  2. Click on the *Trusted Sites* icon, then click on the *Custom level...* button.

3. Scroll down until you see the “Downloads > Automatic prompting for file downloads” option.
4. Select the *Enable* radio button, then click on the *OK* button to dismiss the Security Settings window.
5. Click on the *Apply* button, then click on the *OK* button to dismiss the Internet Options window.

**Q.** I cannot download SilverStreak, even when both the Dell Remote Infrastructure Monitoring and Dell PSM Portal servers’ URLs are in my browser’s Trusted Sites.

**A.** Enter a wildcard URL to Trusted Sites.

***From Internet Explorer:***

1. Select *Tools > Internet Options* and then click on the *Security* tab.
2. Click on the *Trusted Sites* icon, then click on the *Sites* button.
3. Enter one of the following wildcard URLs into the text box:
  - \*.us.dell.com
  - \*.dell.com
4. Click on the *Add* button, then click on the *Close* button to dismiss the Trusted Sites window.
5. Click on the *OK* button to dismiss the Internet Options window.

***From Firefox:***

1. Click on *Tools > Options* and then click on the *Privacy* icon.
2. Click on the *Exceptions* button.
3. Enter one of the following wildcard URLs into the text box:
  - \*.us.dell.com
  - \*.dell.com
4. Click on the *Allow* button, then click on the *Close* button to dismiss the Privacy window
5. Click on the *OK* button to dismiss the Options window.

**Q.** When I click on a button, nothing happens.

**A.** Certain tasks in the Dell PSM Portal user interface require pop-up windows to be displayed in the web browser. You must disable any pop-up blocking software on your browser client before performing such tasks.

**From Internet Explorer:**

1. Select *Tools > Pop-up Blocker > Turn Off Pop-up Blocker*.

**From Firefox:**

1. Click on *Tools > Options* and then click on the *Content* icon.
2. Deselect the *Block pop-up windows* tickbox, then click on the *OK* button to dismiss the Options window.

Q. When I click on a button, I see error messages.

A. You must enable JavaScript in your web browser.

**From Internet Explorer:**

1. Select *Tools > Internet Options* and then click on the *Security* tab.
2. Click on the *Custom Level* button.
3. Scroll down until you see the "Scripting > Active scripting" option.
4. Select the *Enable* radio button, then click on the *OK* button to dismiss the Security Settings window.
5. Click on the *Apply* button, then click on the *OK* button to dismiss the Internet Options window.

**From Firefox:**

1. Click on *Tools > Options* and then click on the *Content* icon.
2. Select the *Enable JavaScript* tickbox, then click on the *OK* button to dismiss the Options window.

Q. Can I manage devices that are located in different parts of the world with the Dell PSM Portal?

A. Yes. The best practice is to use dedicated Management Domains for each supported region (e.g. Europe, North America). See "[Creating a Management Domain](#)" on [page 2-4](#) for more information about creating Management Domains.



**Tip:** Service contract information is unavailable for managed devices that are located in unsupported regions (e.g. Asia).

---

- Q.** Can I discover devices that are already managed with Dell Management Console (DMC)?
- A.** Yes, by following this procedure:
- 1. Navigate to *Reports > Inventory > Discovered Devices* in the DMC console.**
  - 2. Export the Discovered Devices report to a text or CSV file.**
  - 3. Remove any extra data columns from the file. It must contain only one column, with one IP address per line.**
  - 4. Import the text or CSV file.**
- See “[Importing Devices from a File](#)” on [page 3-4](#).

**Q.** I’m unable to discover my assets. What’s wrong?

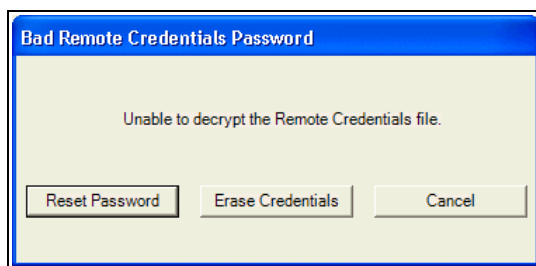
**A.** You may not have downloaded and configured SilverStreak properly.

Follow the steps in “[Downloading and Installing SilverStreak](#)” on [page 2-6](#).



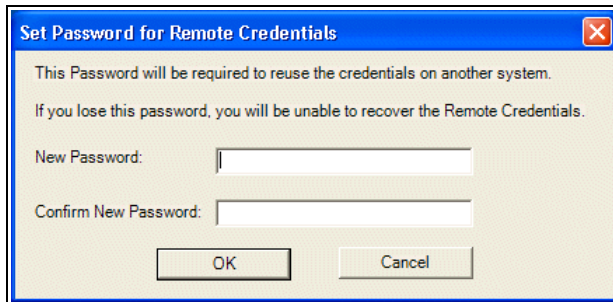
**Tip:** If you have already downloaded SilverStreak, you may need to uninstall it using *Start > Control Panel > Add/Remove Programs* and then re-install it.

- Q.** Discovery appeared to run successfully, but assets were not discovered, or contained incomplete information. What happened?
- A.** The credentials in SilverStreak may be incorrect. See “[Configuring SilverStreak Credentials](#)” on [page 2-13](#) on for help.
- Q.** I clicked on the *Credentials* button on the SilverStreak Configuration application and I received a “Bad Remote Credentials Password” error (see below). What should I do?



- A.** Follow this procedure:
- 1. Click on the *Erase Credentials* button and confirm this choice.**

2. Click on the **Reset Password** button. You will see the following window:



3. Enter a password of your choosing.

This password is used to encrypt the credentials file located in the SilverStreak install directory. If you forget this password, you will have to erase the credentials and reconfigure your discovery credentials. See [“Configuring SilverStreak Credentials”](#) on [page 2-13](#).

4. Click on the **OK** button.

The Credentials window will appear. At this point, you can add a new credential. See [“Add Remote Credentials”](#) on [page 2-14](#).

**Q.** What version of OpenManage Server Administrator is supported?

**A.** OMSA 4.5 or greater.

**Q.** What files are modified on my VMware/Linux and Windows systems by DSET?

**A.** See your DSET documentation for further information.

**Q.** What files does Dell Proactive Systems Management Portal modify or monitor on my VMWare/Linux systems when they are discovered?

**A.** The Dell PSM Portal monitors the system log file on most configurations as follows:

- The `/etc/syslog.conf` file is modified to give SilverStreak access to system logs at discovery time.
- The `/var/log/messages` file is monitored for OpenManage events once the device has been discovered and is being managed by the Email or Ignore policies.

**Q.** I am unable to monitor my SLES 11 servers. Why?

**A.** Make the following changes to your SLES 11 server configuration:



- To the `/etc/syslog-ng/syslog-ng.conf` file:

```
Destination logserver { udp("<SilverStreak_IP_address>" port(514)); };  
Log { source(src); destination(logserver); };
```

- To the `sshd_conf` file:

```
ChallengeResponseAuthentication no  
GSSAPIAuthentication yes  
GSSAPICleanupCredentials yes  
PasswordAuthentication yes
```

- Q.** What files does Dell Proactive Systems Management Portal modify or monitor on my Windows systems when they are discovered?
- A.** No files are modified on your Windows systems by Dell Proactive Systems Management Portal. Windows Event Logs are monitored for Windows events once the device has been discovered, and is being managed by the Email or Ignore policies.
- Q.** I received a service contract expiry notification email for a service contract that will automatically renew at a different service level. What should I do?
- A.** You can safely ignore that email, as your service contract will automatically renew at the predetermined service level.



## A

- Account
  - Provisioning Your, [1-8](#)
- Add
  - Assets, [3-1](#)
    - single device or a range of devices, [3-3](#)
  - Devices, [3-1](#)
  - Encryption/Decryption Password, [2-14](#)
  - Group, [4-2](#)
  - Management Domain, [2-4](#)
  - Secondary Contact User, [2-2](#)
  - Users, [2-2](#)
- Adding
  - Assets, [3-1](#)
    - importing devices from a file, [3-4](#)
    - single device or a range of devices, [3-3](#)
  - Devices, [3-1](#)
  - Encryption/Decryption Password, [2-14](#)
  - Group, [4-2](#)
  - Management Domain, [2-4](#)
  - Secondary Contact User, [2-2](#)
  - Users, [2-2](#)
- Alerting Options
  - Configuring
    - customer preferences, [2-23](#)
- Architecture
  - High-level, [1-2](#)
- Assets
  - Add, [3-1](#)
  - Adding, [3-1](#)
    - importing devices from a file, [3-4](#)
    - single device or a range of devices, [3-3](#)
  - Discover, [3-1](#)
  - Discovering, [3-1](#)
    - importing devices from a file, [3-4](#)
    - single device or a range of devices, [3-3](#)
- Auto-support Case
  - Configuring Monitoring Policies, [2-26](#), [2-27](#)

## B

- Browsers, Web
  - Supported
    - Firefox, [1-10](#)
    - Internet Explorer 6 and 7, [1-10](#)

## C

- Change
  - Primary Contact User, [2-2](#)
- Changing
  - Primary Contact User, [2-2](#)
- Configuration
  - Dell RIM Server, [2-11](#)
  - Proxy Server, [2-11](#)
  - SilverStreak, [2-8](#)
- Configure
  - Service Contract Expiry Notice
    - frequency
      - not immediate, [2-21](#)
  - Service Contract Report Notification Options
    - by customer, [2-20](#)
  - SLES 11 Servers, [A-6](#)
- Configuring
  - Customer Preferences, [2-20](#)
    - alerting options, [2-23](#)
    - remote diagnostic settings, [2-21](#)
    - service contract report notification options, [2-20](#)
  - Monitoring Policies, [2-26](#)
    - auto support case, [2-26](#), [2-27](#)
    - email alerts, [2-26](#), [2-27](#)
    - ignore, [2-26](#), [2-27](#)
    - unmanaged, [2-26](#), [2-27](#)
  - Service Contract Expiry Notice
    - frequency
      - not immediate, [2-21](#)
  - Service Contract Report Notification Options, [2-20](#)
    - by customer, [2-20](#)
  - SLES 11 Servers, [A-6](#)

- Creating
  - Encryption/Decryption Password, [2-14](#)
  - Group, [4-2](#)
  - Management Domain, [2-4](#)
  - Secondary Contact User, [2-2](#)
  - Users, [2-2](#)
- Credentials
  - SilverStreak, [2-13](#)
- Customer Preferences
  - Alerting Options
    - configuring, [2-23](#)
  - Configuring, [2-20](#)
  - Remote Diagnostic Settings
    - configuring, [2-21](#)
  - Service Contract Report Notification Options
    - configuring, [2-20](#)

## D

- Delete
  - Group, [4-4](#)
  - Management Domain, [4-7](#)
- Deleting
  - Group, [4-4](#)
  - Management Domain, [4-7](#)
- Dell
  - Modular Disk Storage Manager (MDSM)
    - required for SNMP traps monitoring
      - Dell PowerVault MD3000, [1-6](#)
      - Dell PowerVault MD3000i, [1-6](#)
      - Dell PowerVault MD3200i, [1-6](#)
      - Dell PowerVault MD3220i, [1-6](#)
    - required to run Lasso, [2-22](#)
  - MyAccount
    - Required, [1-8](#)
  - PowerVault Storage Devices
    - System Requirements, [1-6](#)
  - RIM Server
    - Configuration, [2-11](#)

- Device
  - Typing
    - during discovery, [3-5](#)

- Devices
  - Add, [3-1](#)
  - Adding, [3-1](#)
  - Discover, [3-1](#)
  - Discovering, [3-1](#)
  - Typing
    - during discovery, [3-5](#)

- Discover
  - Assets, [3-1](#)

- Dell Modular Disk Storage Manager (MDSM)
  - Server
    - required to run Lasso, [2-22](#)
  - Devices, [3-1](#)
- Discovering
  - Assets, [3-1](#)
    - importing devices from a file, [3-4](#)
    - single device or a range of devices, [3-3](#)
  - Dell Modular Disk Storage Manager (MDSM)
    - server
      - required to run Lasso, [2-22](#)
    - Devices, [3-1](#)
- Discovery
  - Complete when All Device Service Tags are Collected, [3-6](#)
  - Device Typing, [3-5](#)
  - Results
    - verifying, [3-6](#)
- Domain Management, [4-5](#)
- Domain:
  - Manage, [4-5](#)
  - Managing, [4-5](#)
- Downloading and Installing SilverStreak, [2-6](#)
- Downloading SilverStreak, [2-6](#)

## E

- Edit
  - Group, [4-3](#)
  - Management Domain, [4-5](#)
- Editing
  - Group, [4-3](#)
  - Management Domain, [4-5](#)
- Email Alerts
  - Configuring Monitoring Policies, [2-26](#), [2-27](#)
- Encryption/Decryption Password
  - Add, [2-14](#)
  - Adding, [2-14](#)
  - Creating, [2-14](#)

## F

- FAQ, [A-1](#)
- Firefox
  - Supported Web Browsers, [1-10](#)

## G

- Group

---

- Add, [4-2](#)
- Adding, [4-2](#)
- Creating, [4-2](#)
- Delete, [4-4](#)
- Deleting, [4-4](#)
- Edit, [4-3](#)
- Editing, [4-3](#)
- Manage, [4-1](#)
- Management, [4-1](#)

- Groups
  - Managing, [4-1](#)

## H

- Hardware Configuration
  - Requirements, [1-4](#)
- High-level Architecture, [1-2](#)

## I

- Ignore
  - Configuring Monitoring Policies, [2-26](#), [2-27](#)
- Importing
  - Assets
    - from a file, [3-4](#)
    - single device or a range of devices, [3-4](#)

- Install SilverStreak, [2-6](#)
- Installing SilverStreak, [2-6](#)
- Integration
  - VMware® vCenter™, [1-7](#)

- Internet Explorer
  - Supported Web Browsers, [1-10](#)

- Interoperability
  - Requirements, [1-4](#)
    - SNMP, [1-4](#)
    - VMware® vCenter™, [1-4](#)

## L

- Logging Into the Portal, [1-10](#)

## M

- Manage
  - Domain: , [4-5](#)
  - Group, [4-1](#)
- Management Domain
  - Add, [2-4](#)
  - Adding, [2-4](#)

- Creating, [2-4](#)
- Delete, [4-7](#)
- Deleting, [4-7](#)
- Edit, [4-5](#)
- Editing, [4-5](#)
- Managing
  - Domain: , [4-5](#)
  - Groups, [4-1](#)
- Modular Disk Storage Manager (MDSM)
  - Required for SNMP Traps Monitoring
    - Dell PowerVault MD3000, [1-6](#)
    - Dell PowerVault MD3000i, [1-6](#)
    - Dell PowerVault MD3200i, [1-6](#)
    - Dell PowerVault MD3220i, [1-6](#)
  - Required to Run Lasso, [2-22](#)

- Monitoring Policies
  - Configuring, [2-26](#)
    - auto support case, [2-26](#), [2-27](#)
    - email alerts, [2-26](#), [2-27](#)
    - ignore, [2-26](#), [2-27](#)
    - unmanaged, [2-26](#), [2-27](#)

- MyAccount
  - Dell
    - required, [1-8](#)

## O

- Operating System
  - Requirements, [1-3](#)
- Overview, [1-1](#)

## P

- Password
  - Encryption/Decryption
    - Adding, [2-14](#)
    - Creating, [2-14](#)
- Portal
  - Logging In, [1-10](#)
- Preferences
  - Alerting Options
    - configuring, [2-23](#)
  - Customer
    - configuring, [2-20](#)
  - Remote Diagnostic Settings
    - configuring, [2-21](#)
  - Service Contract Report Notification Options
    - configuring, [2-20](#)
- Primary Contact User
  - Change, [2-2](#)

Changing, [2-2](#)  
Provisioning Your Account, [1-8](#)  
Proxy Server  
Configuration, [2-11](#)

## Q

Quick Start, [1-12](#)

## R

Remote Diagnostic Settings  
Configuring  
customer preferences, [2-21](#)  
Remote Diagnostics  
Requirements, [1-6](#)  
Requirements  
System, [1-3](#)  
hardware configuration, [1-4](#)  
interoperability, [1-4](#)  
operating system, [1-3](#)  
remote diagnostics, [1-6](#)  
SNMP, [1-4](#)  
virtual machine configuration, [1-4](#)  
VMware® vCenter™, [1-4](#), [1-7](#)

## S

Secondary Contact User  
Add, [2-2](#)  
Adding, [2-2](#)  
Creating, [2-2](#)  
Server  
Dell RIM  
configuration, [2-11](#)  
Service Contract Expiry Notice  
Configure  
by customer, [2-20](#)  
Configuring  
by customer, [2-20](#)  
frequency not immediate, [2-21](#)  
Service Contract Report Notification Options  
Configuring  
customer preferences, [2-20](#)  
SilverStreak  
Configuration, [2-8](#)  
Credentials, [2-13](#)  
Downloading, [2-6](#)  
Install, [2-6](#)  
Installing, [2-6](#)

SLES 11 Servers  
Configure, [A-6](#)  
Configuring, [A-6](#)  
Support, [A-1](#)  
System Requirements, [1-3](#)  
Dell PowerVault Storage Devices, [1-6](#)  
Hardware Configuration, [1-4](#)  
Interoperability, [1-4](#)  
SNMP, [1-4](#)  
VMware® vCenter™, [1-4](#)  
Operating System, [1-3](#)  
Remote Diagnostics, [1-6](#)  
Virtual Machine Configuration, [1-4](#)  
VMware® vCenter™, [1-7](#)  
VMware/Linux Servers, [1-5](#)  
Windows Servers, [1-5](#)

## T

Traps  
Monitoring Requirements  
not supported  
Dell PowerVault NX2000, [1-6](#)  
Dell PowerVault NX3000, [1-6](#)  
Dell PowerVault NX3100, [1-6](#)  
supported  
Dell PowerVault MD3000, [1-6](#)  
Dell PowerVault MD3000i, [1-6](#)  
Dell PowerVault MD3200i, [1-6](#)  
Dell PowerVault MD3220i, [1-6](#)

Troubleshooting, [A-1](#)

## Type

Device  
during discovery, [3-5](#)  
Devices  
during discovery, [3-5](#)

## Typing

Device  
during discovery, [3-5](#)  
Devices  
during discovery, [3-5](#)

## U

Unmanaged  
Configuring Monitoring Policies, [2-26](#), [2-27](#)  
User  
Primary Contact  
Changing, [2-2](#)  
Secondary Contact  
Adding, [2-2](#)

---

Creating, [2-2](#)

Users

Add, [2-2](#)

Adding, [2-2](#)

Creating, [2-2](#)

## V

Verifying Discovery Results, [3-6](#)

Virtual Machine Configuration

Requirements, [1-4](#)

VMware® vCenter™

Integration, [1-7](#)

Interoperability

system requirements, [1-4](#)

Requirements, [1-7](#)

VMware/Linux Servers

System Requirements, [1-5](#)

## W

Web Browsers

Supported

Firefox, [1-10](#)

Internet Explorer 6 and 7, [1-10](#)

Windows Servers

System Requirements, [1-5](#)



300 Innovative Way  
Nashua, NH 03062  
800-379-6538 tel  
603-589-5855 fax  
[www.dell.com](http://www.dell.com)