ECHOplatform Quick Start Partner Guide

Getting Started with Barracuda's MSP ECHOplatform Backup and Recovery Solutions

Version 3.9

Barracuda MSP

ECHOplatform Quick Start Partner Guide

Revision History

Status	Changes	Date
Final.	Updated Backup Agent Requirements.	August 2020.

Copyright © 2020 Barracuda Networks, Inc. All rights reserved.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Table of Contents

Table of Figures v
Introduction 1
Audience 1
About This Quick Start Guide 1
Backup Agent Requirements 2
Related Documentation 3
Barracuda Technical Support 4
Chapter 1. Setting Your Preferences 5
Logging in 5
Changing Your Password 6
Branding Your Portal 8
Viewing or Editing Contact and Billing Information 17
Creating Portal User Accounts for Employees 19
Managing Portal Time-Out for Employees 23
Creating Accounts for Customers 24
Adding Computers to Accounts 27
Creating an Account Billing Plan 29
Managing Billing 32
Chapter 2. Installing the Software 35
About Software Installation 35
Downloading the Backup Agent Software 35
About the Custom Backup Installer 36
Creating a Custom Backup Installer 36
About the Backup Agent Software 39
Recover Previous Installation 39
Move Account to This Computer 39
Recovery Mode 39
Installing the Backup Agent Software 39
Deploying the Backup Agent Software with RMM Tool 47

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Chapter 3. Initial Seed 49
About Initial Seeds 49
Initial Seed Requirements 49
Creating the Initial Seed 49
Special Considerations 50
Initial Seed Recommendations 50
Chapter 4. Home Dashboard 51
About the Home Dashboard 51
Group Selection Menu 52
Include Recurring Interval-Based Backups Option 52
Last Updated Summary 52
Backups Finished 53
Backup Status Icons 53
Status Display Filters 54
Expanded View 54
Actual Time or Elapsed Time Display 55
Backup Status Sorted by Accounts and Filters 57
Backup Status Display 57
Backup Status Details 58
Navigation Links 59
Account Link 59
Status Reason Link 59
Computer ID Link 60
Manually Restart Backup Link 60
Viewing Activity Logs from the Home Dashboard Expanded View 60
Running Backup Sets from the Home Dashboard 62
Chapter 5. Backup Types, Templates, and Reports 63
Backup Types 63
File and Folder Backup 63
Hyper-V Standard & Hyper-V Rapid Recovery 63

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

VMware Standard & VMware QuickSpin 63
Exchange Information Store 63
Exchange Mailbox Level 64
SQL Server 64
System State 64
Physical Imaging Standard & Physical Imaging Rapid Recovery 64
Templates 64
Reports 64
Chapter 6. Barracuda Essentials 65
Email-Borne Threat Protection 65
Archiving for Compliance 65
Real-Time Analysis 65
Chapter 7. Barracuda Appliances 67
Fast and Easy Installation 67
High Performance 67
Other Deployment Options 67
Chapter 8. Barracuda Content Shield 69
Robust DNS Filtering 69
Real-time Threat Intelligence 69
Centralized Management & Comprehensive Reporting 69
Policy Enforcement 70
Chapter 9. Accessing Resources and Marketing Materials 71
Accessing Marketing Materials 72
Chapter 10. Contacting Partner Support 73
How and When to Contact Partner Support 73
Common Things You Can Check 73
Preparing for Support 73
Glossary 75

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Table of Figures

Figure 1. Group Selection Drop-down Menu. 52
Figure 2. Include Recurring Interval-Based Backups Option. 52
Figure 3. Last Updated Summary. 52
Figure 4. Backup Time Periods. 53
Figure 5. Ratio Example. 53
Figure 6. Filters Affect Drop-down Menu. 54
Figure 7. Expand All Option. 54
Figure 8. Before Status Filter Is Applied. 55
Figure 9. After Status Filter Is Applied. 55
Figure 10. Actual Time and Elapsed Time Features. 56
Figure 11. Elapsed Time Display. 56
Figure 12. Actual Time Display. 56
Figure 13. Graphic Status Sorted by Accounts and Filtered by Status. 57
Figure 14. Backup Status. 58
Figure 15. Account Link. 59
Figure 16. Status Reason Link. 59
Figure 17. Computer ID Link. 60
Figure 18. Manually Backup Restart Link. 60

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Introduction

This section includes the following topics:

- Audience
- About This Quick Start Guide
- Backup Agent Requirements
- Related Documentation
- Barracuda Technical Support

Audience

The audience for this document is IT professionals and partners who provide clients with cloud backup and recovery support using Barracuda.

About This Quick Start Guide

Barracuda continues building on the strategy of expanding the breadth of backup and data protection support as well as expanding the recoverability of data for small businesses.

This Quick Start Guide provides the following chapters:

- Setting Your Preferences
- Installing the Software
- Initial Seed
- Home Dashboard
- Backup Types, Templates, and Reports
- Barracuda Essentials
- Barracuda Appliances
- Accessing Resources and Marketing Materials
- Contacting Partner Support

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Backup Agent Requirements

The following table provides the requirements for running the Backup Agent software.

Backup Agent Requirements	
Supported Operating Systems • Microsoft Windows 8.1 (8 is not supported) • Microsoft Windows 10 (Anniversary Update or newer) • Microsoft Windows Server 2012 Server (Standard Edition) • Microsoft Windows Server 2012 R2 (Standard Edition) • Microsoft Windows Server 2012 R2 Essentials • Microsoft Windows Server 2016 (Standard Edition) • Microsoft Windows Server 2019 (Standard Edition) **Physical Imaging and BMR Supported Operating Systems** • Microsoft Windows 8.1 • Microsoft Windows 10 • Microsoft Windows Server 2012 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 R2 Essentials • Microsoft Windows Server 2016 (Standard Edition) • Microsoft Windows Server 2019 (Standard Edition) **BMR Support** • **Hard Disk Controllers** — SCSI — IDE — SATA • **Boot Types/Disk Partition Styles** — MBR — GPT • **Supported File Systems (for backup source)**	**Minimum Requirements for File and Folder Backups** • 2 GHz dual-core CPU • 1 GB of total RAM (500 MB free RAM during backup, restore, or delete operation) • Free disk space equaling twice the size of your largest protected file (not required for VM backups) • Broadband Internet Connection • MS.NET Framework 4.8 **Minimum Requirements for Exchange, SQL, Imaging, VMware, and Hyper-V Backups** • 2GHz quad-core CPU • 4 GB of Total RAM (1 GB free RAM during backup, restore, or delete operation) • Free disk space equaling twice the size of your largest protected file (not required for VM backups) • Broadband Internet Connection • MS.NET Framework 4.8 (to allow backup/restore/delete management from the web) **Exchange** • Microsoft Exchange 2010 (when installed on Windows Server 2012 Standard edition; does not support DAG or clustered environments) • Microsoft Exchange 2013 (when installed on Windows Server 2012 Standard edition; does not support DAG or clustered environments) • Microsoft Exchange 2016 • Microsoft Exchange 2019

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Backup Agent Requirements	
— NTFS (Unless it is a System volume that is part of the Boot Volumes group.) • **Supported Backup Destinations** — 512-byte sector disks — 4K native sector disks **Web Portal Requirements** • Chrome (most recent version) • Edge (most recent version) • Internet Explorer (most recent version) • Firefox (most recent version)	**SQL** • Microsoft SQL Server 2012 Standard • Microsoft SQL Server 2014 Standard • Microsoft SQL Server 2016 Standard • Microsoft SQL Server 2017 Standard • Microsoft SQL Server 2019 Standard **Note**: SQL Databases running in Full recovery mode do not have their transaction logs truncated. **Virtual Machines** • VMware ESXi/vCenter 5.5, 6.0, 6.5, 6.7, 7.0 (with TLS 1.0 or TLS 1.2) - All supported versions require a VMware Essentials license or higher. Includes support for clustered environments. VDDK 7.0 is not supported. • Hyper-V 2012, 2012 R2, 2016, 2019 **Note**: Clustered environments are not supported.

Related Documentation

The following documentation is available:

- *ECHOplatform Backup and Restore Reference Guide* – provides details on how to perform backups and restores for each backup type.
- *Barracuda MSP Best Practices Partner Guide* - provides details on best practices for performing backups and restores.
- *Barracuda Backup Services User Guide* - -provides information about Barracuda data backup and security services
- *ECHOplatform - Autotask Integration Guide* - provides information about setting up Autotask integration with the Backup Agent.
- *ECHOplatform - ConnectWise Integration Guide* - provides information about setting up ConnectWise integration with the Backup Agent.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Barracuda Technical Support

Technical Support is available 8 AM to 9 PM (EST).

Phone: 800-569-0155, option 1 or 617-948-5300

Email: support@barracudamsp.com

You also can use the live chat service 8 AM to 6 PM (EST).

Click the following link:

Link: http://www.barracudamsp.com/support/contact.php

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Chapter 1. **Setting Your Preferences**

This section includes the following topics:

- Logging in
- Changing your password
- Branding your portal
- Viewing or editing contact and billing information
- Creating portal user accounts for employees
- Managing portal time-out for employees
- Creating accounts for customers
- Adding computers to accounts
- Creating an account billing plan
- Managing billing

Logging in

Once you become a Barracuda Partner, you can log in with your username and password

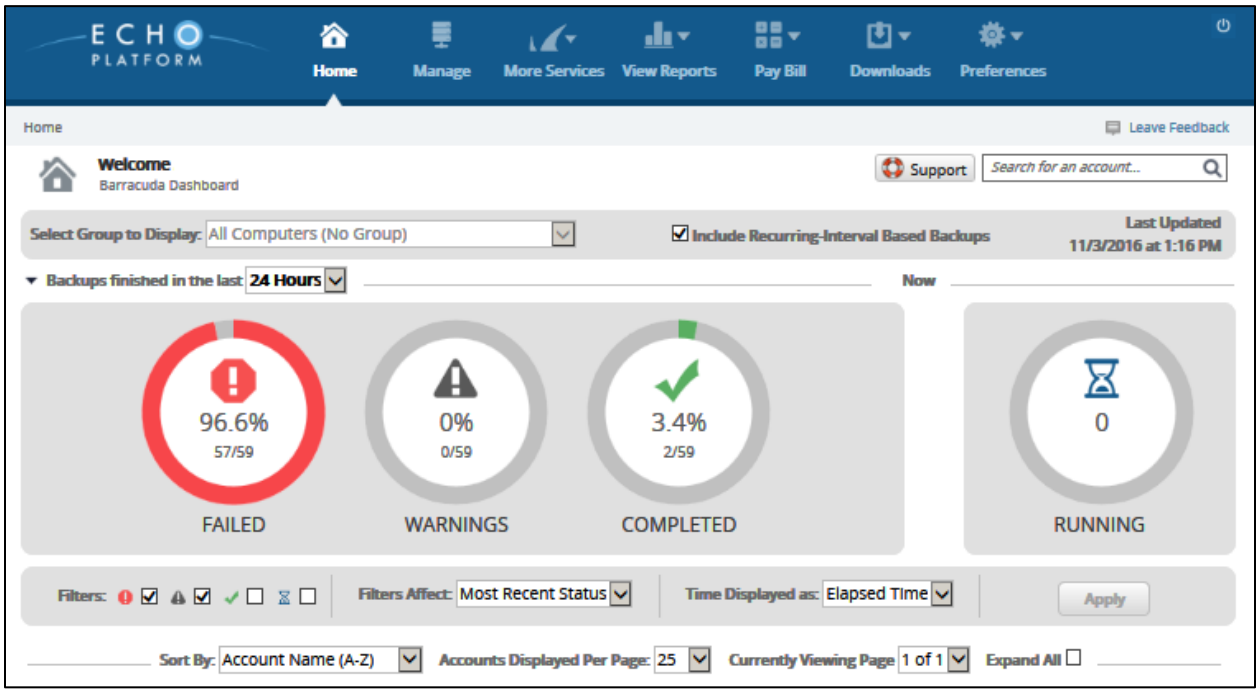
Navigate to https://manage.barracudamsp.com.

The login screen is displayed.

Enter your username and password, and then click **Sign In**.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

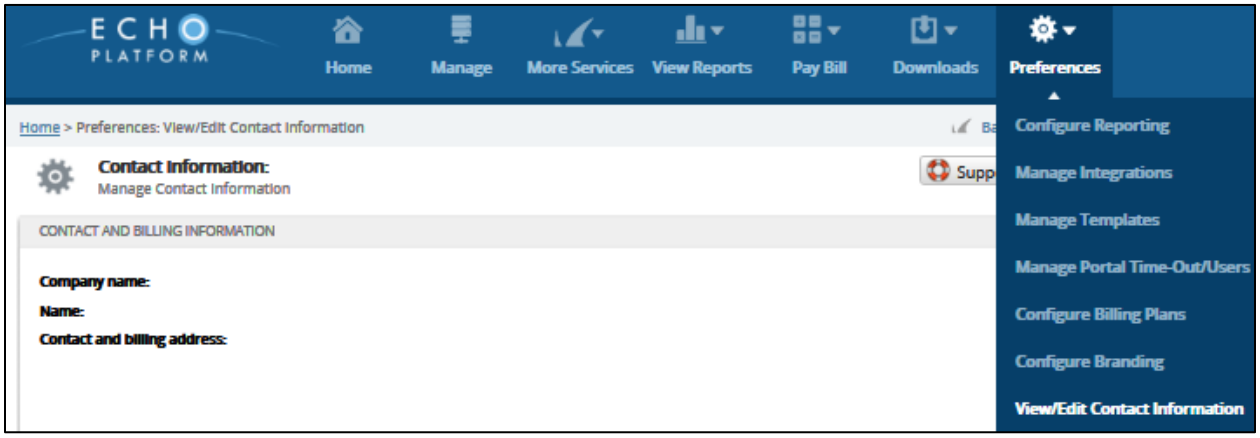
The Home Dashboard is displayed.



Changing Your Password

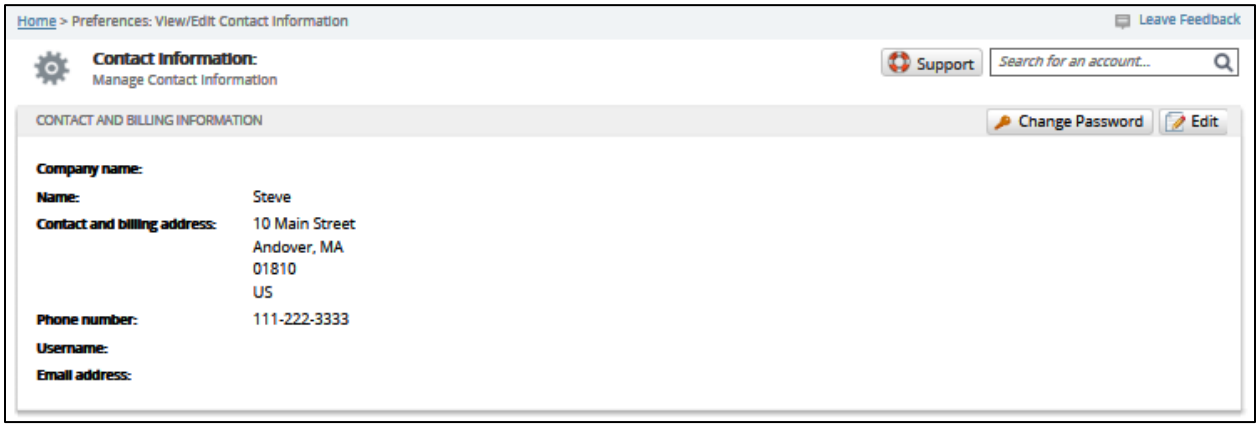
To change your password, perform the following steps.

1. At the ECHOplatform ribbon, click **Preferences**, **View/Edit Contact Information**.



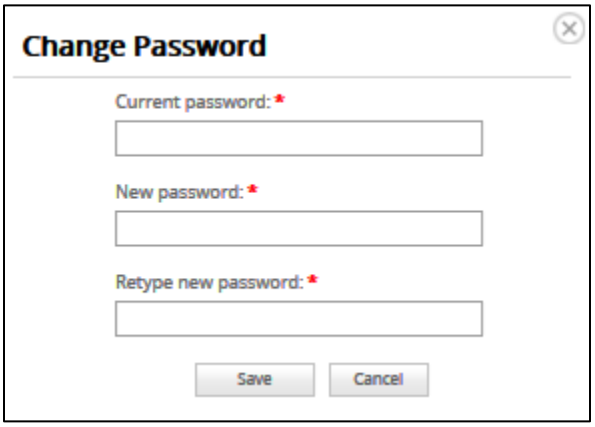
This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

The contact information for your account is displayed.



2. Click the **Change Password** button.

The Change Password pop-up is displayed.



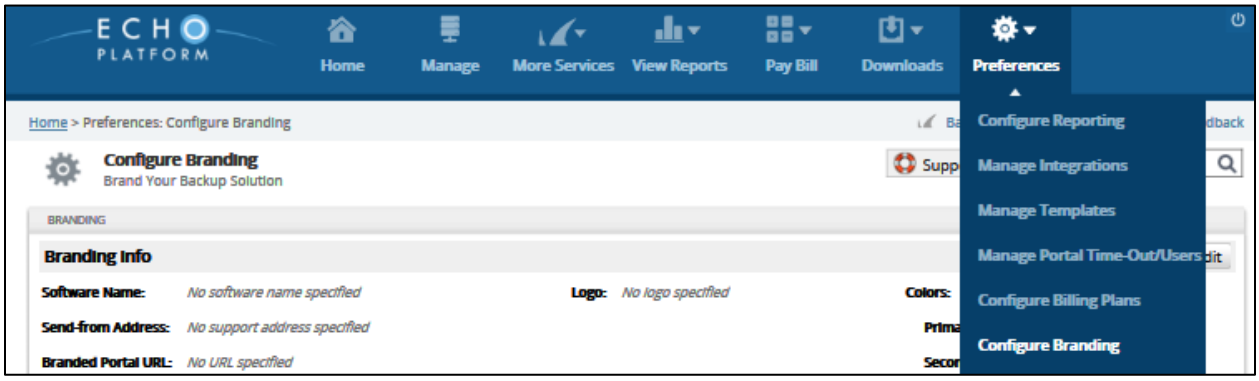
3. Make your changes, and then click **Save**.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Branding Your Portal

To brand your portal, perform the following steps.

1. At the ECHOplatform ribbon, click **Preferences**, **Configure Branding**.

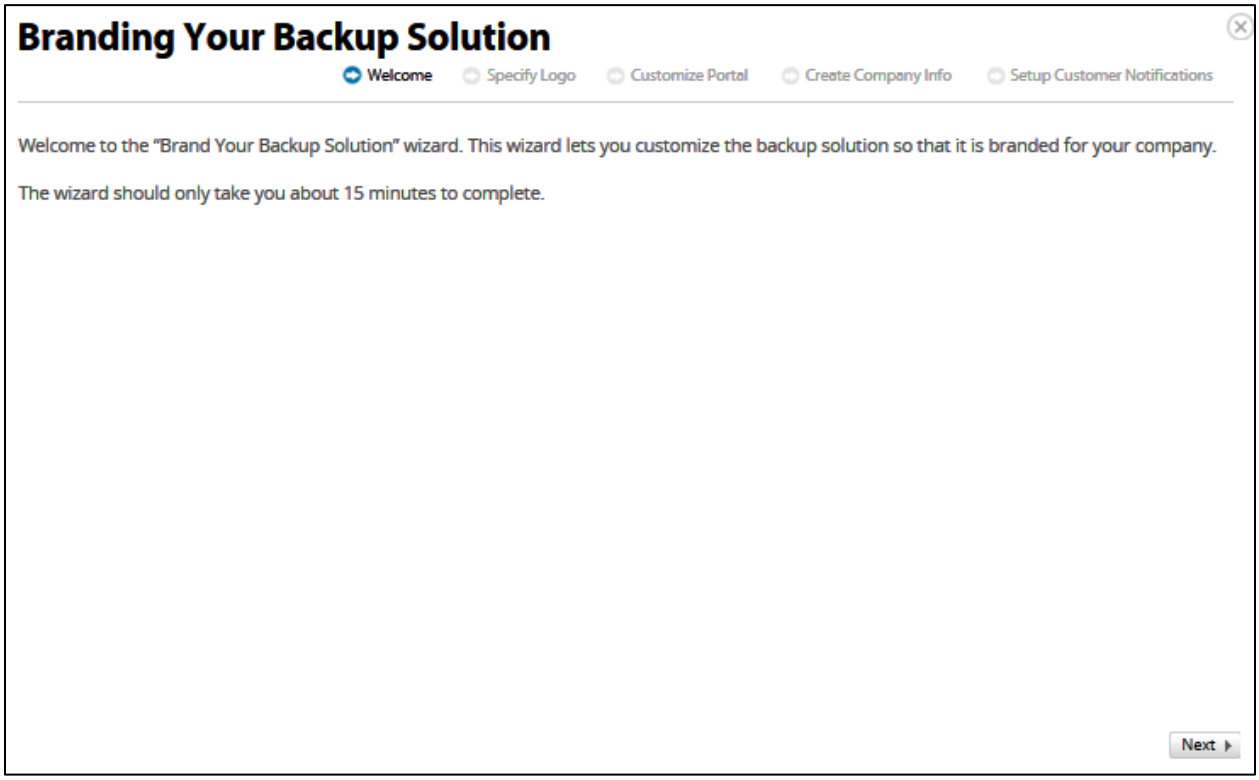


The Configure Branding page is displayed.

2. Click the **Edit** button.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

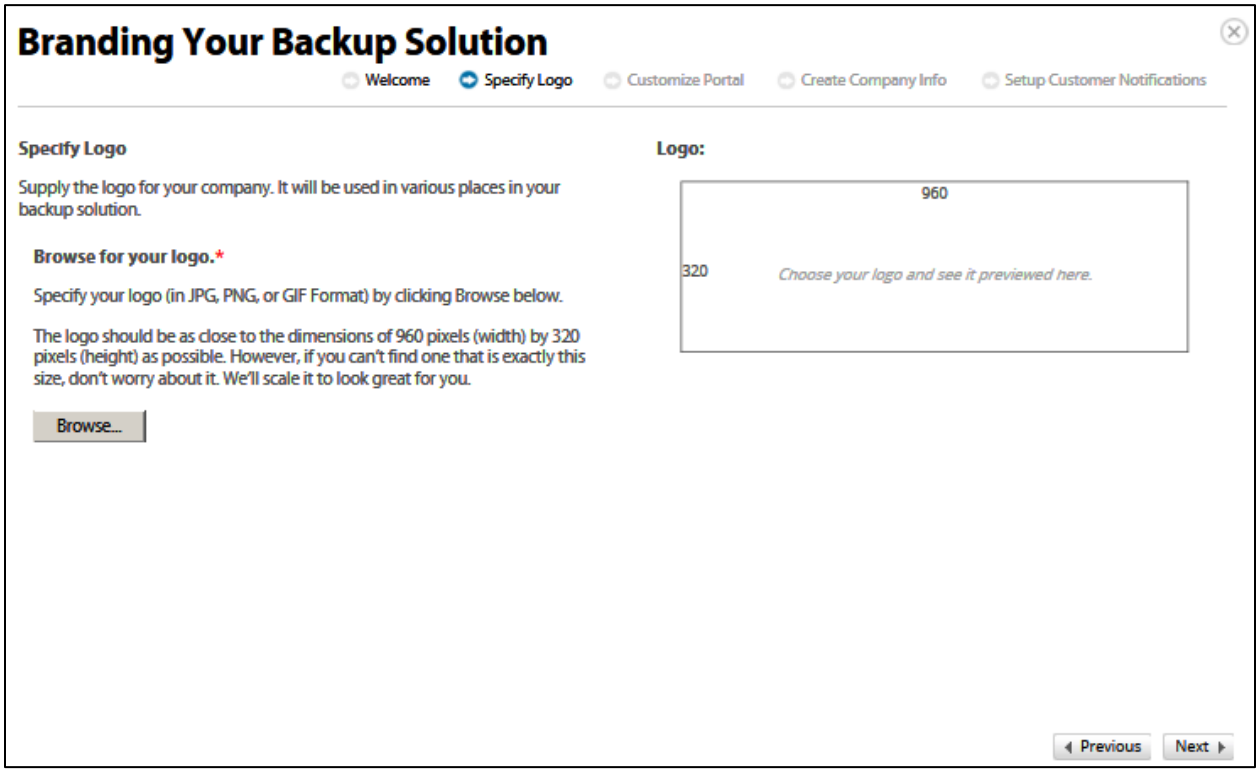
The Welcome page is displayed.



3. Click **Next**.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

The Specify Logo page is displayed.

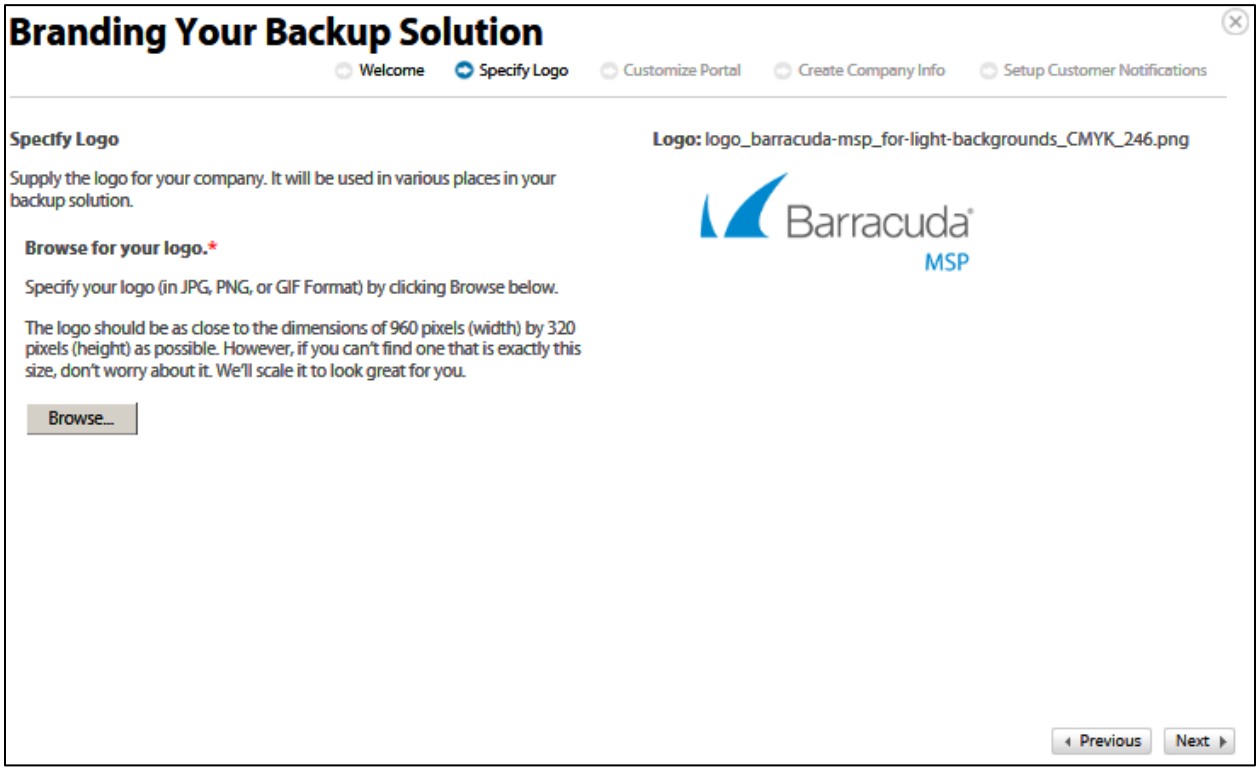


4. Click the **Browse** button to select your company logo.

Note: Specify your logo in JPG, PNG, or GIF Format. The logo needs to be as close to the dimensions of 960 pixels (width) by 320 pixels (height) as possible. However, if you cannot find one that is exactly this size, it can be automatically scaled.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

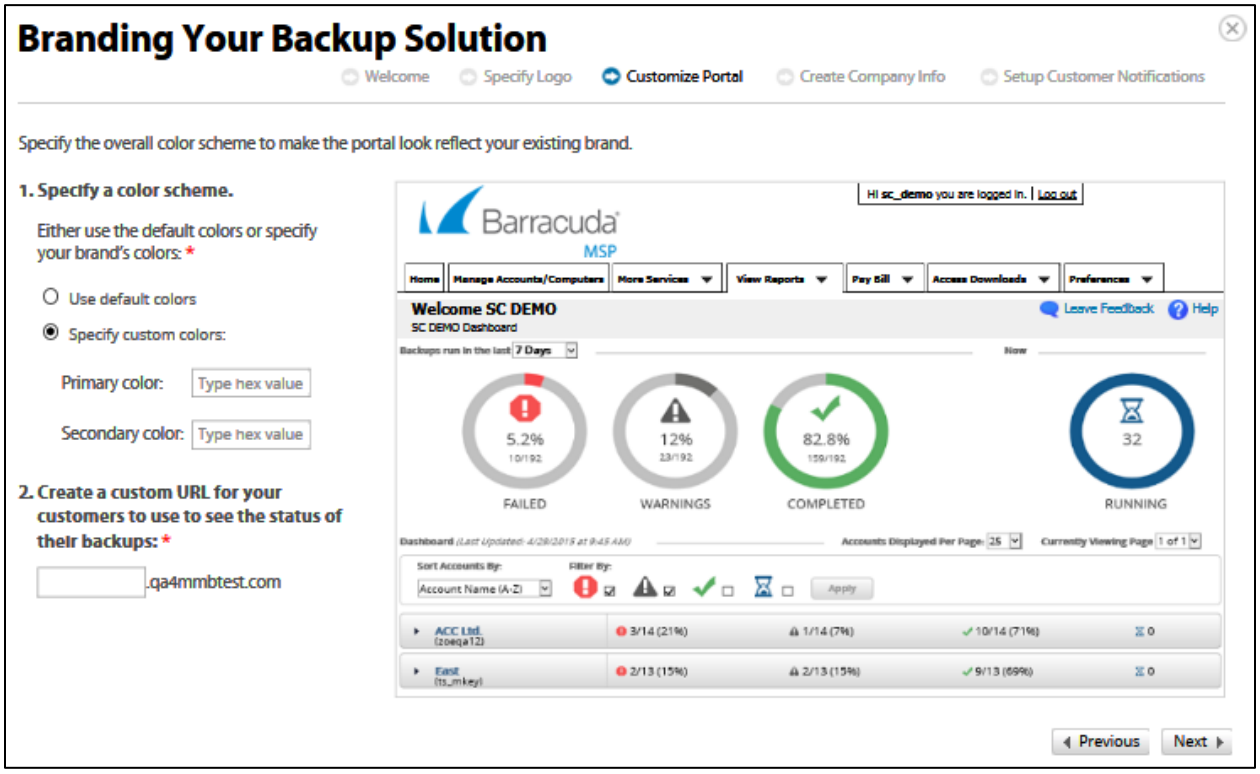
The logo is displayed in the right-side panel, as shown in the example below.



5. Click **Next**.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

The Customized Portal page is displayed.



6. Specify the overall color scheme to make the portal reflect your existing brand.

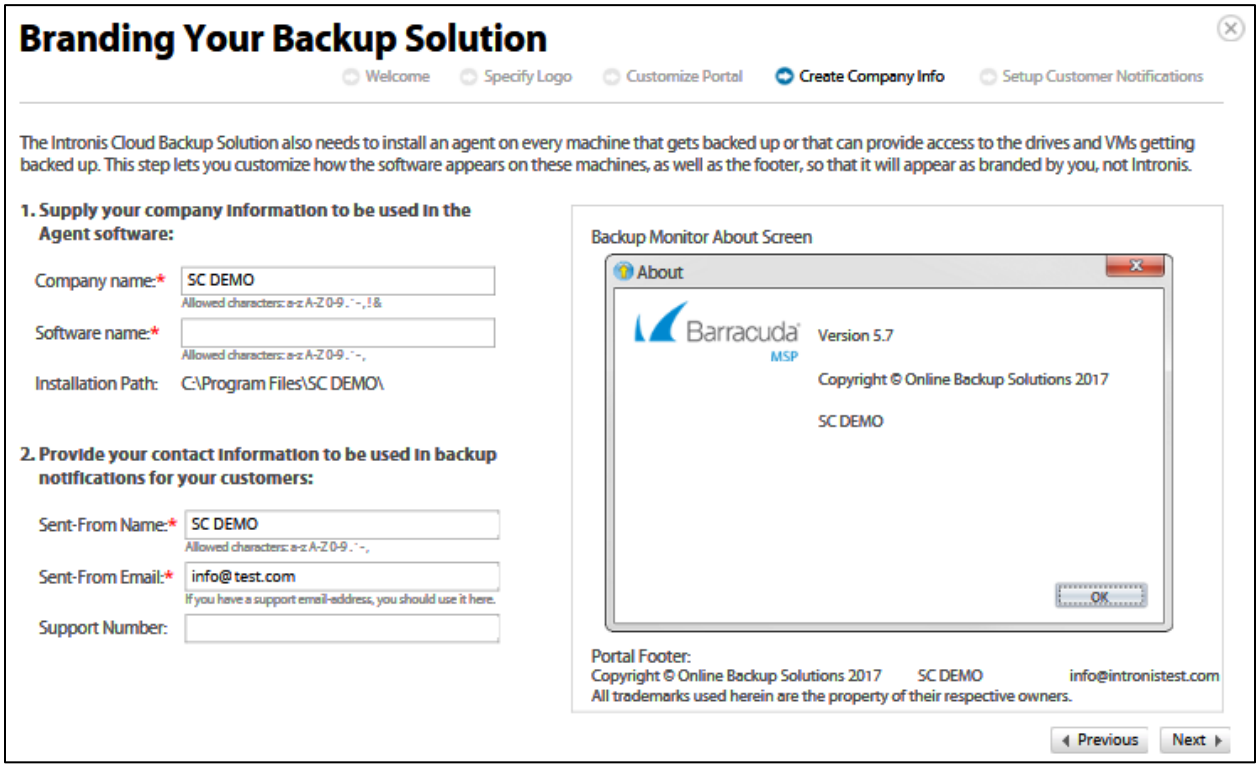
   You have the options of using the default colors or specifying custom colors by clicking the relevant radio buttons.

7. Create a custom URL for your customers to display the status of their backups by typing it into the text box, and then click **Next**.

   Requirement: The URL must be formatted as *x.managemybackups.com*.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

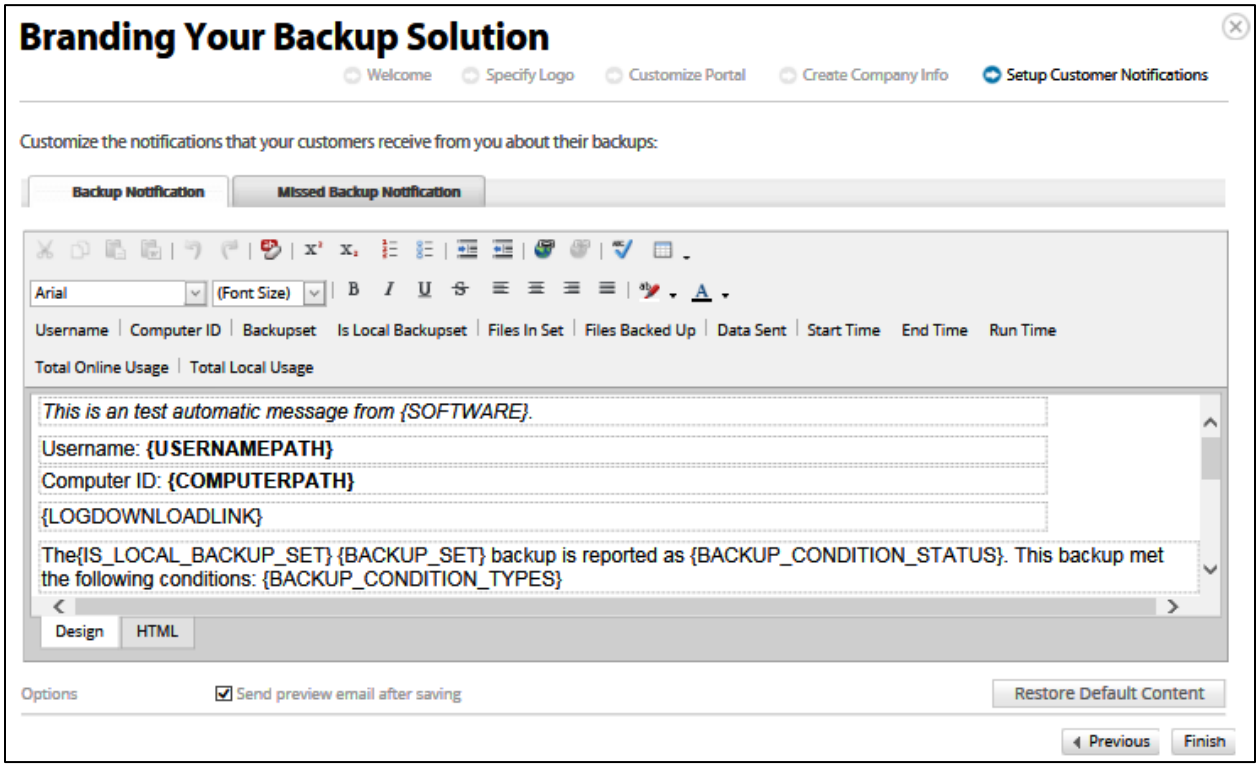
The Create Company Info page is displayed.



8. In the first section, supply your company information to be used in the Agent software, and then select an Installation Path.
9. In the second section, provide your contact information to be used in backup notifications for your customers.
10. Enter a support number to be displayed on the portal and on emails so your customers can call you for support, and then click **Next**.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

The Setup Customer Notifications page is displayed.

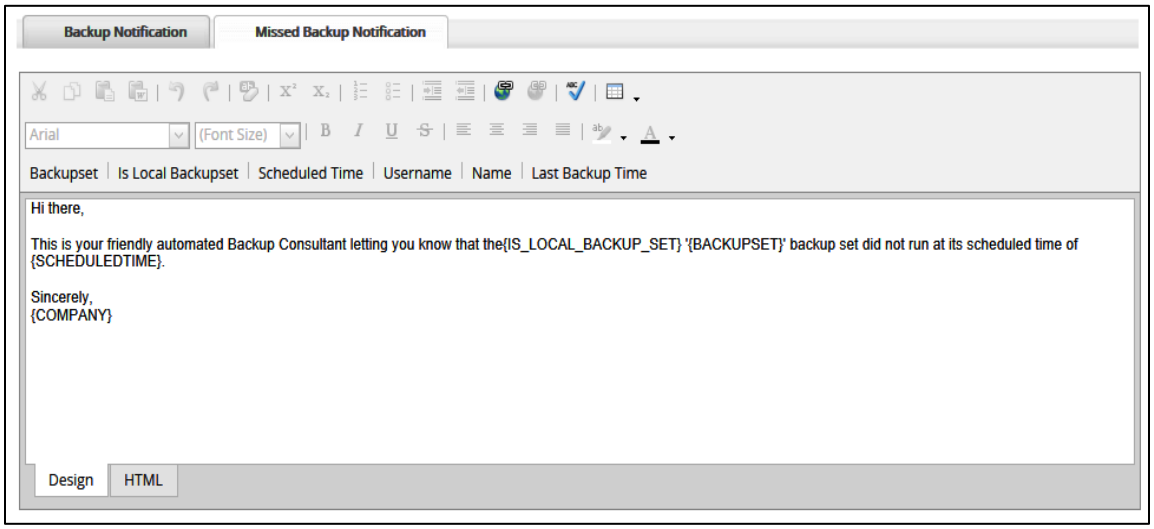


11. Customize the text and macros for the notifications that your customers receive from you about their backups by typing information in the relevant fields.

The Design or HTML buttons are provided to meet your preference.

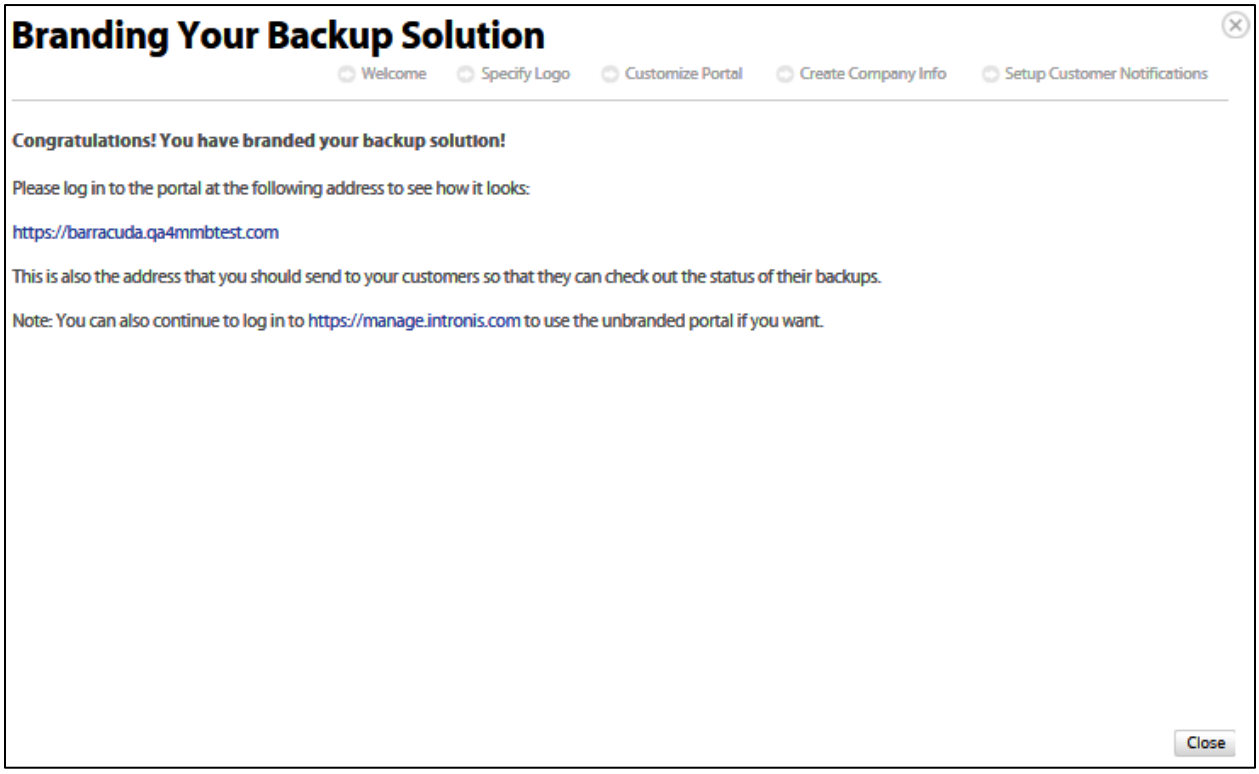
This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

12. Click the **Missed Backup Notification** tab to customize the status message, as shown below.



13. When satisfied, click **Finish**.

The Completion page is displayed.



This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

14. Clink the link provided.

    The Log in page is displayed.

15. Log in to the portal at the address link provided to view your branded solution.

    Note: This is the address that is sent to your customers so that they can review the status of their backups.

16. When satisfied, return to the Setup Customer Notification page, and click **Close**.

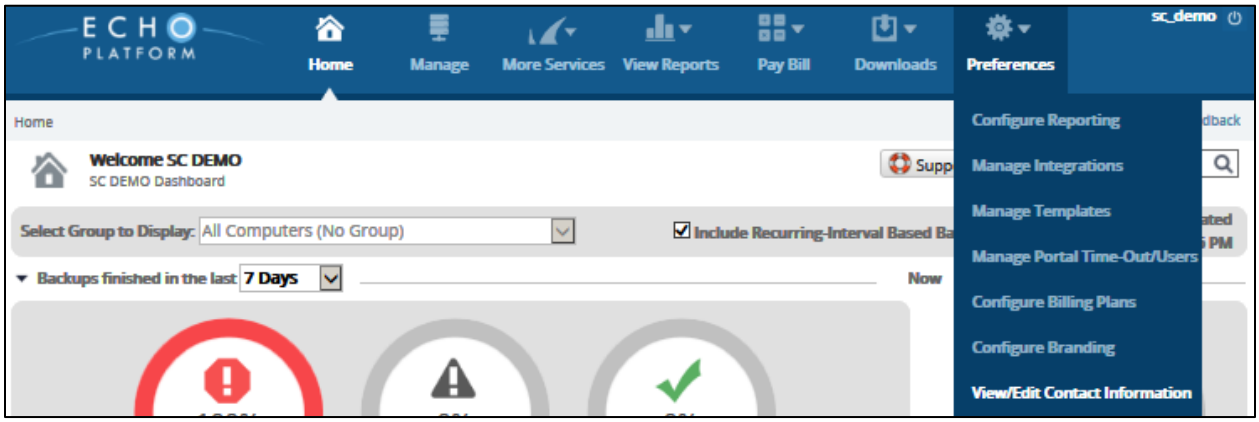
    The Configure Branding page displays your edits.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Viewing or Editing Contact and Billing Information

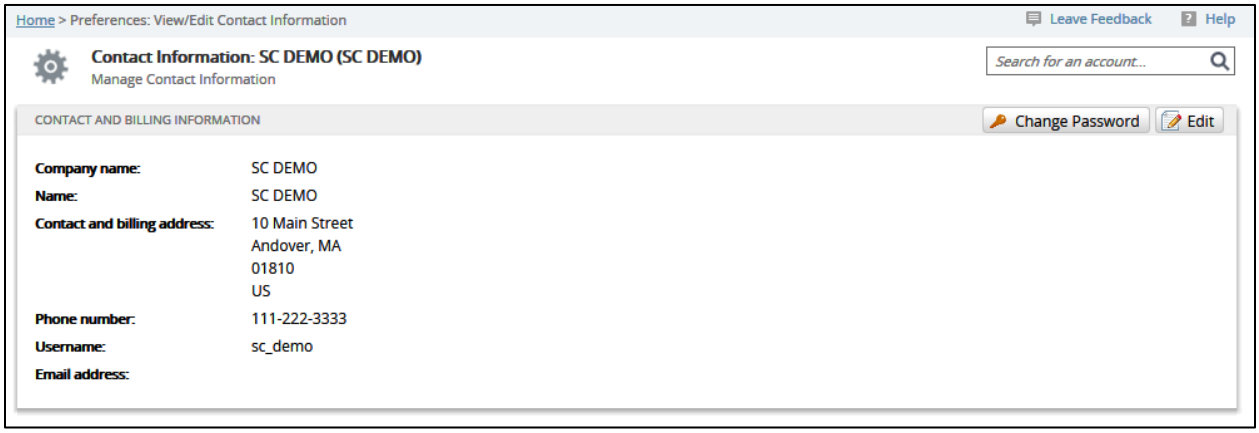
To view or edit your contact and billing information, perform the following steps.

1. At the ECHOplatform ribbon, click **Preferences, View Contact Information**.



2. Select **View/Edit Contact Information**.

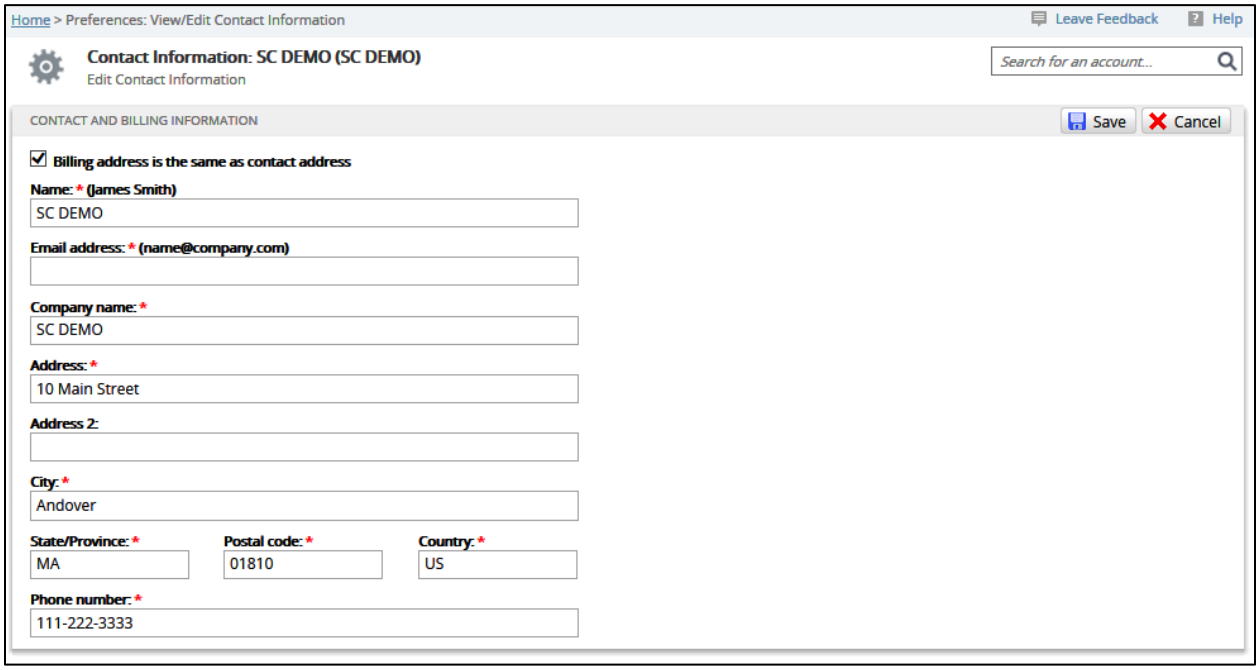
The contact information for your account is displayed.



3. To make any changes, click the **Edit** button.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

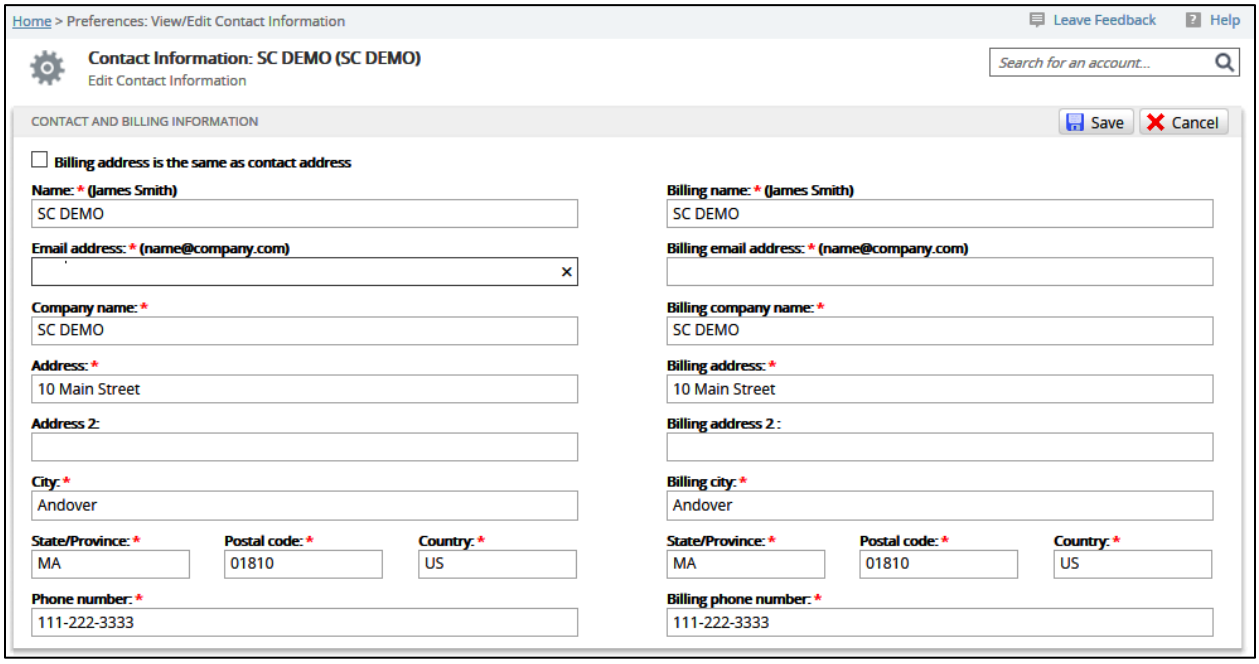
The contact information fields are displayed.



4. If your contact and billing information are different, clear the **Billing address is the same as contact address** check box.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

The billing information fields are displayed so you can edit them separately.

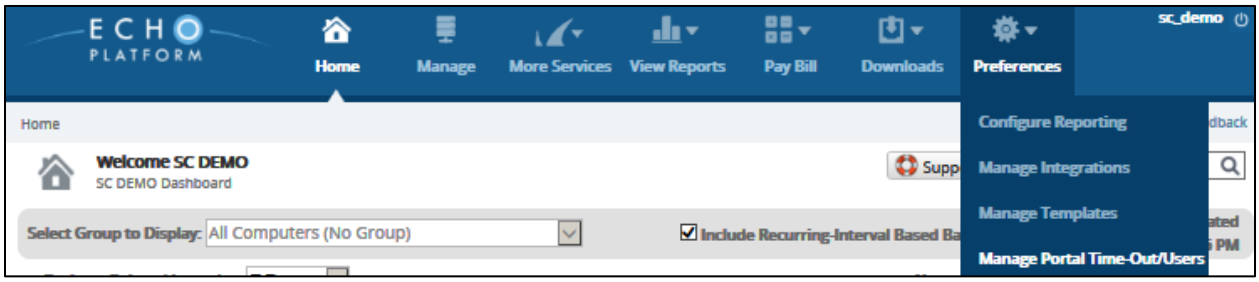


5. Make your edits, and then click **Save**.

Creating Portal User Accounts for Employees

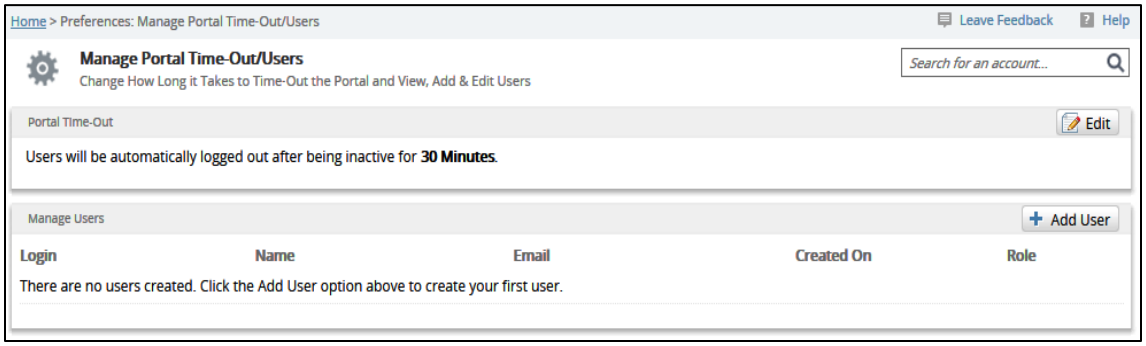
To create portal user accounts for your employees, perform the following steps.

1. At the ECHOplatform ribbon, click **Preferences, Manage Portal Time-Out/Users**.



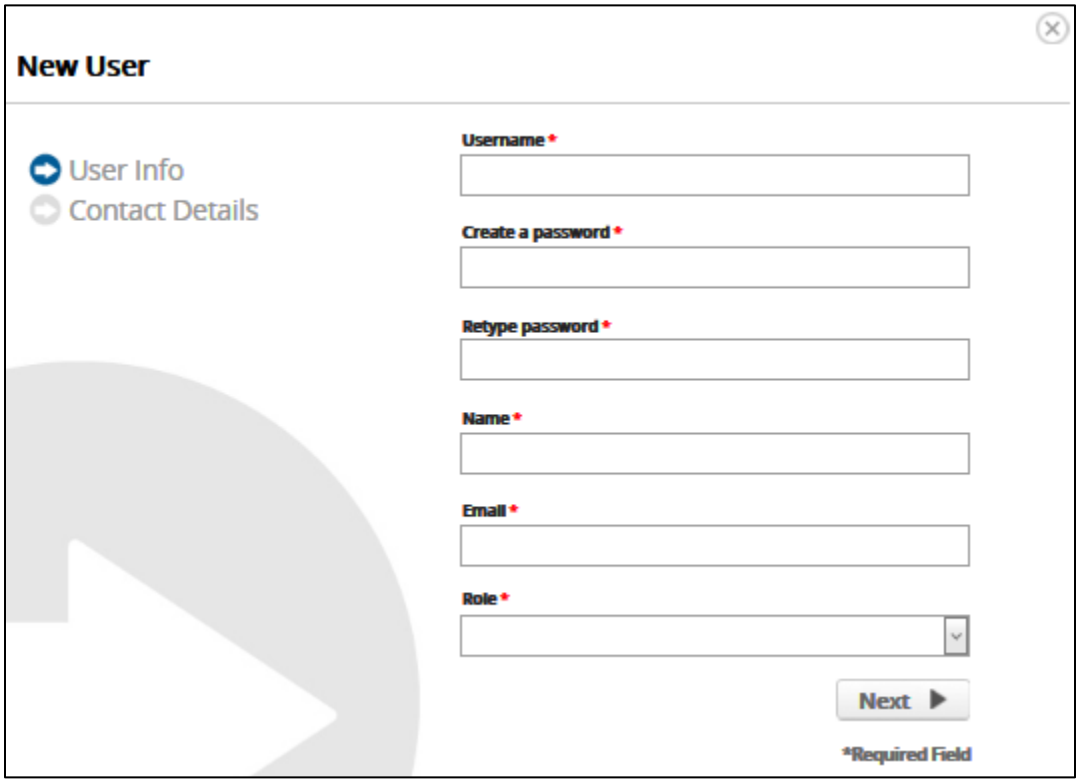
This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

The Manage Portal Time-Out/Users page is displayed.



2. Click the **Add User** button.

The New User form is displayed.

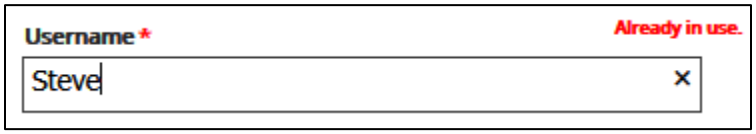


3. Complete the fields.

a. Type a unique Username.

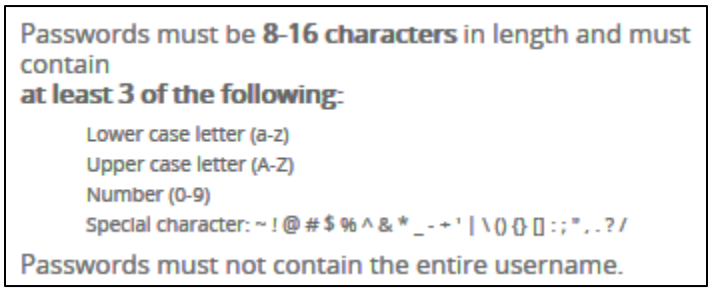
This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

If a Username is already in use, the following notice is displayed.



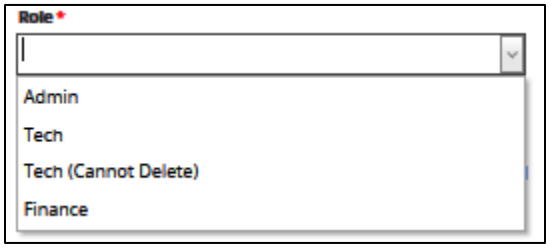
b. Type a password.

The following password requirements are displayed.



c. Type the Name and Email is the relevant fields.

d. Select a role from the Role drop-down list, as shown below.



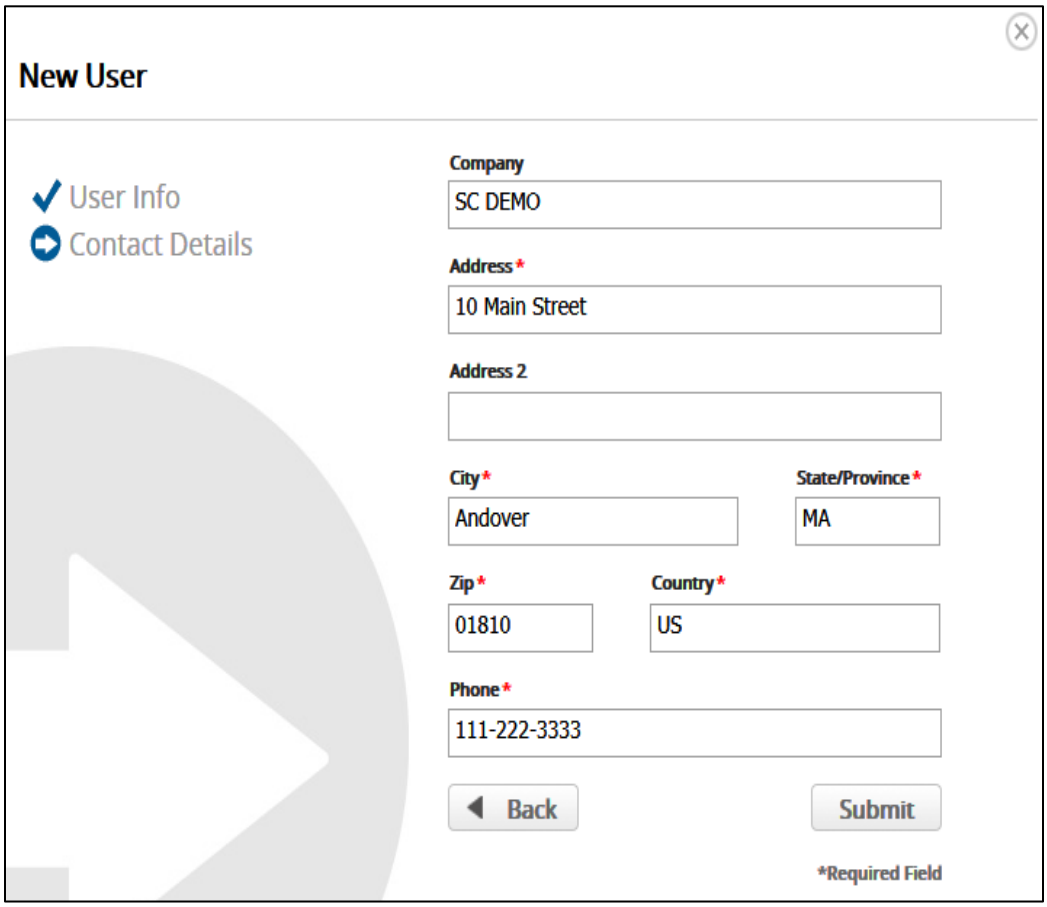
The roles are defined as:

- Admin – access to all features.
- Tech – access to management section and backup set related reporting.
- Tech (cannot delete)
- Finance – access to billing section and billing-related reporting.

4. When complete, click **Next**.

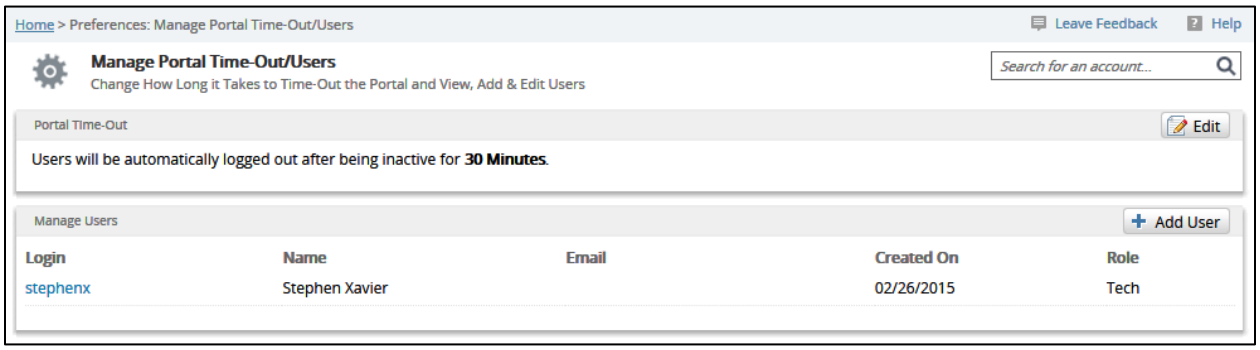
This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

The Contact Details page is displayed.
Notice that the fields are automatically populated.



5. Click **Submit**.

The new user is displayed, as shown below.

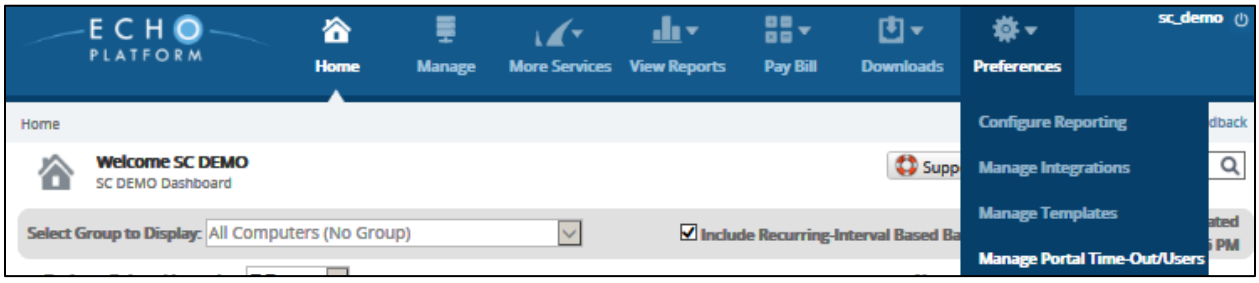


This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

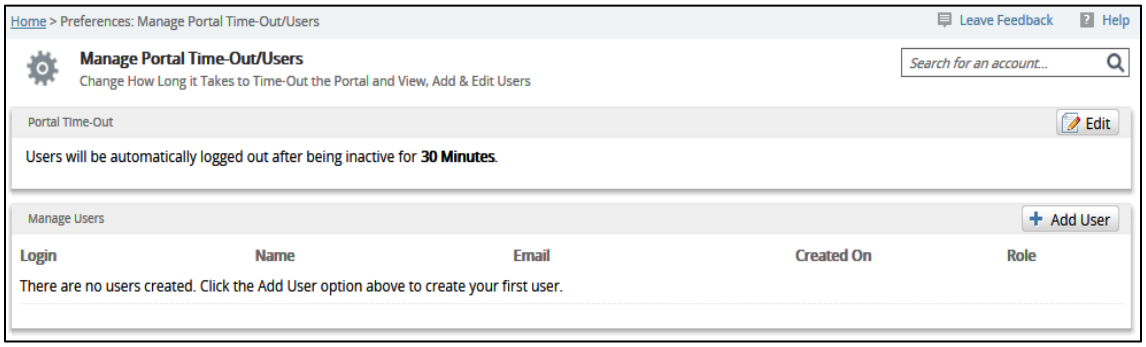
Managing Portal Time-Out for Employees

To manage portal time-out for your employees, perform the following steps.

1. At the ECHOplatform ribbon, click **Preferences, Manage Portal Time-Out/Users**.

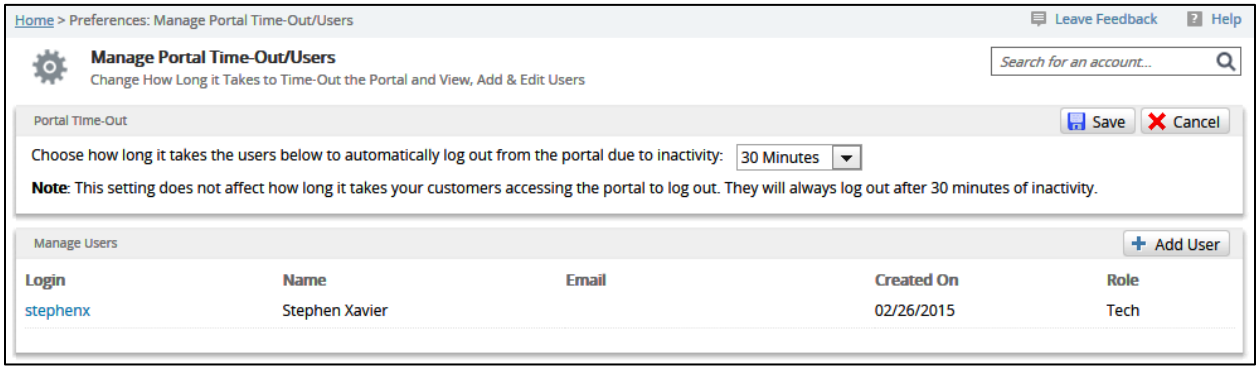


The Manage Portal Time-Out/Users page is displayed.



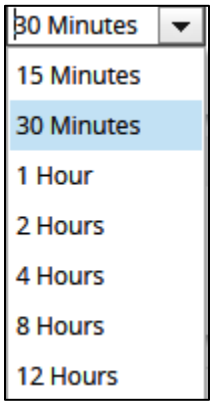
2. Click the **Edit** button.

The Portal Time-Out field is displayed.



This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

3. Select the drop-down arrow to display the following menu.



4. Select how long it takes the users that are displayed to log out automatically from the portal due to inactivity, and then click **Save**.

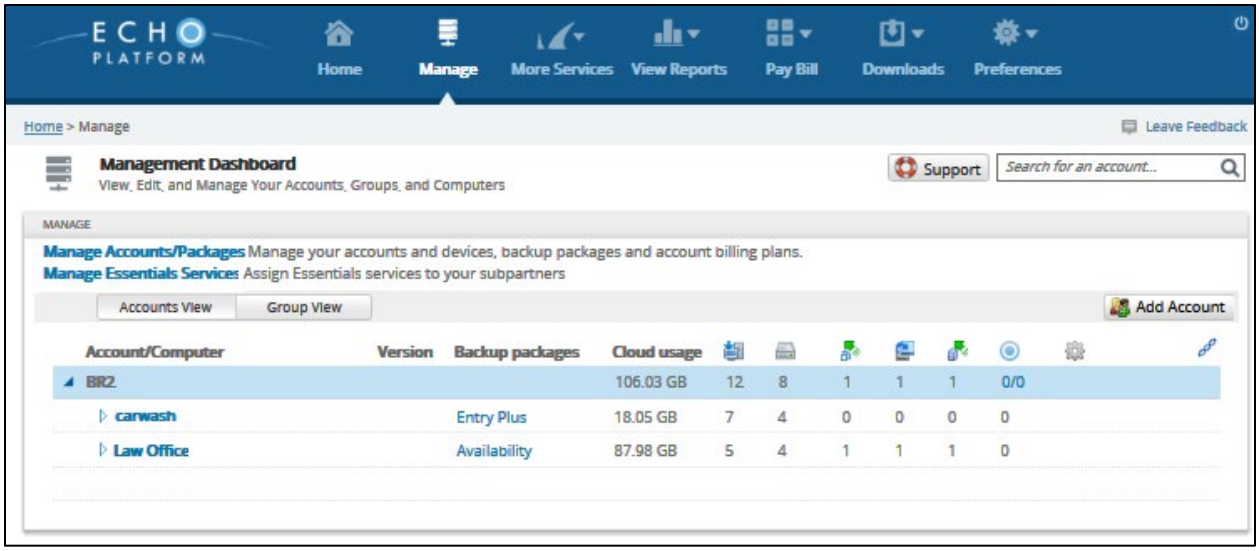
Note: This setting does not affect how long it takes your customers accessing the portal to log out. Customers are always logged out after 30 minutes of inactivity.

Creating Accounts for Customers

To create accounts for your customers, perform the following steps.

1. At the ECHOplatform ribbon, click **Manage**.

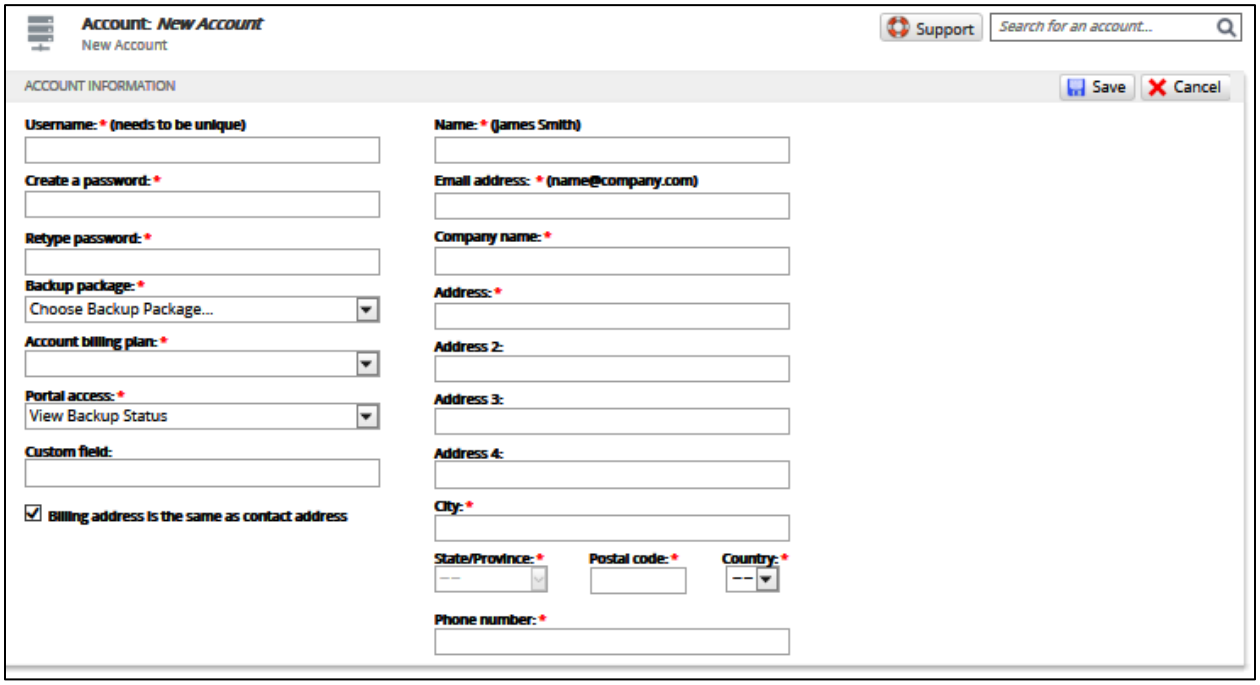
The Management Dashboard is displayed.



2. Click the **Add Account** button.

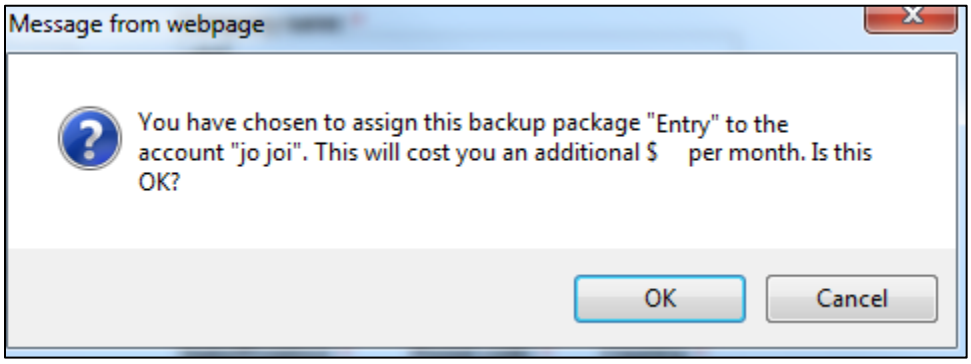
This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

The New Account form is displayed.



3. Complete the form, and then click **Save**.

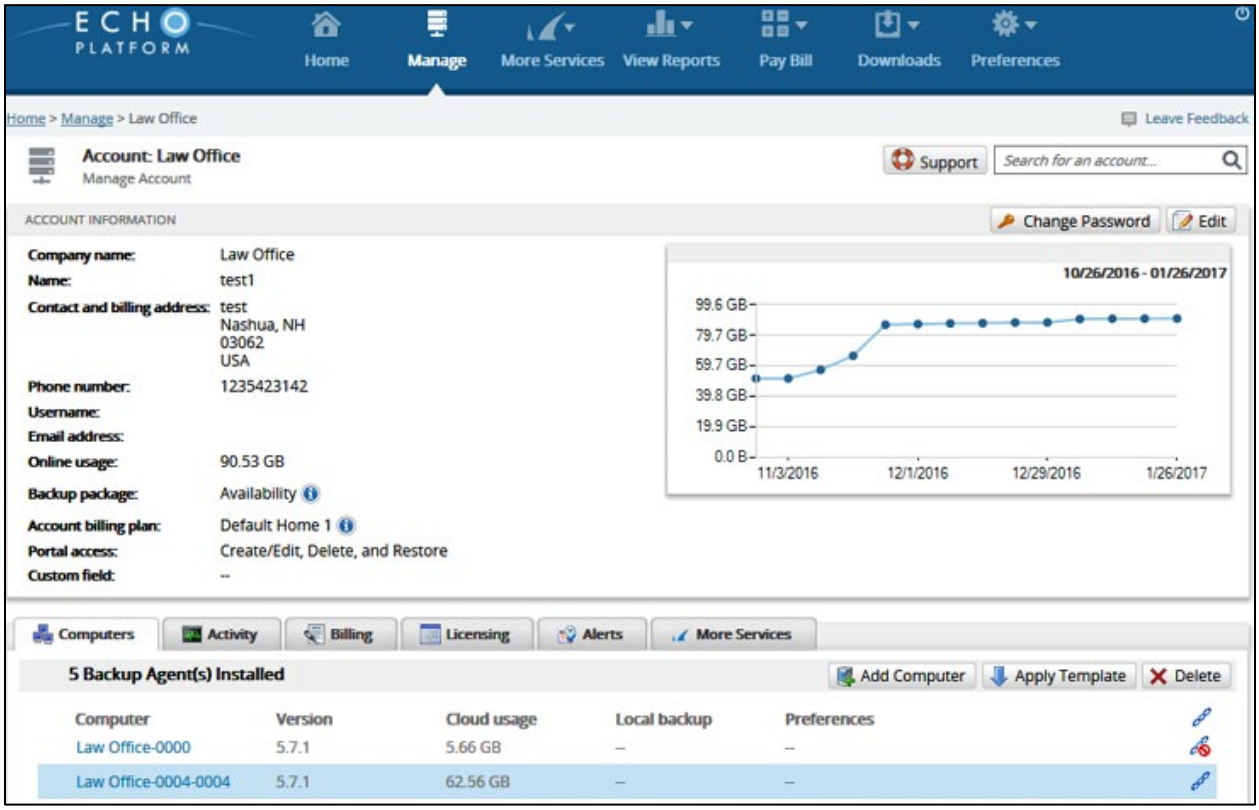
   Note: Asterisks indicate a mandatory field. Every new Account must have a package assigned.
   If you run over your pre-purchased amount, you are prompted to accept the new package, as shown below.



4. Click **OK**.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

The new Account page is displayed.



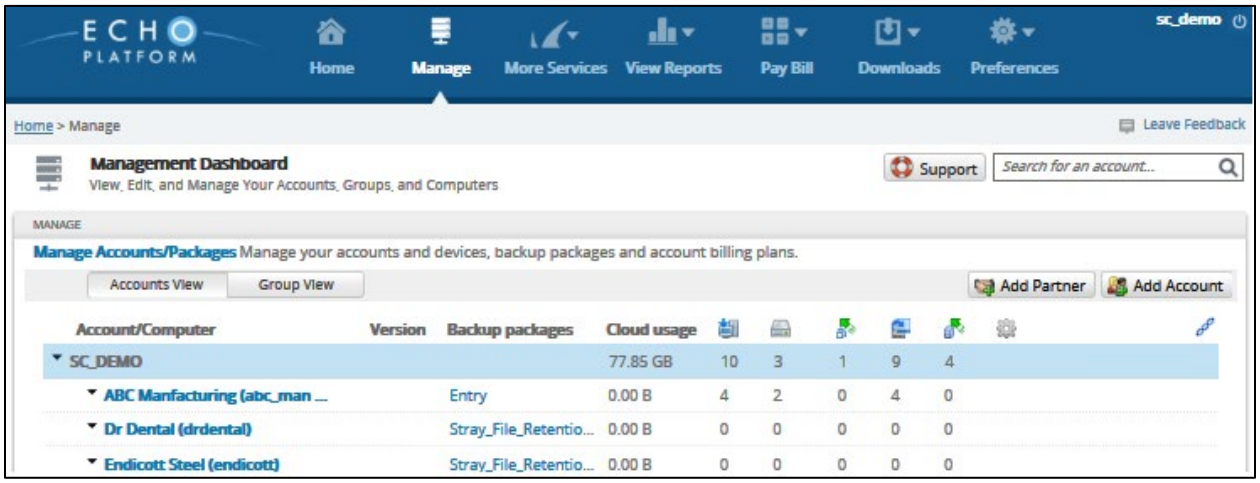
This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Adding Computers to Accounts

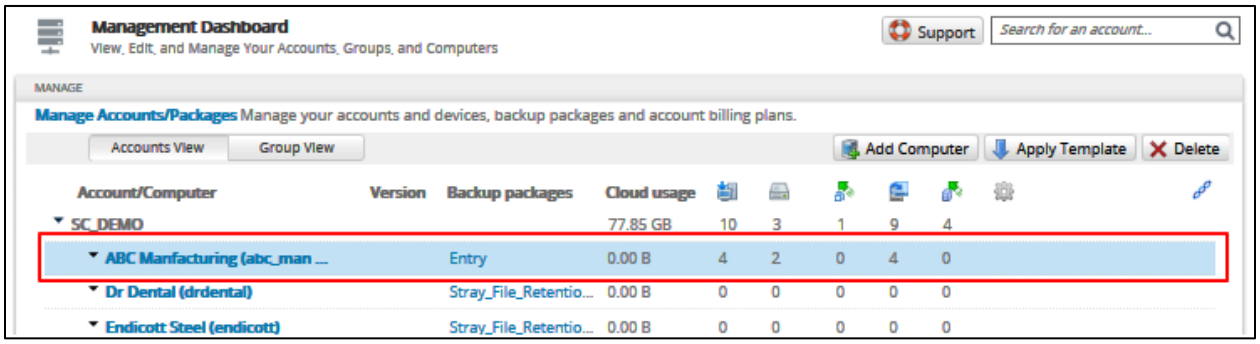
To add computers to accounts, perform the following steps.

1. At the ECHOplatform ribbon, click **Manage**.

   The Management Dashboard is displayed.

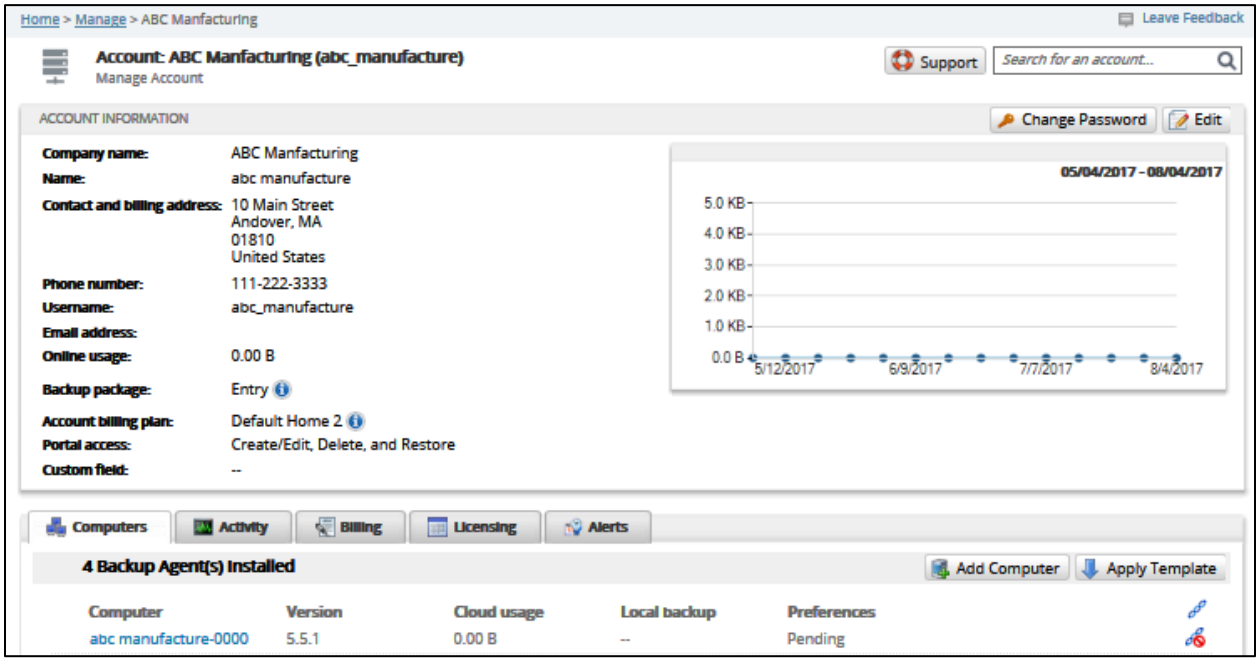


2. Select the account to which you want to add the computer, as shown below.



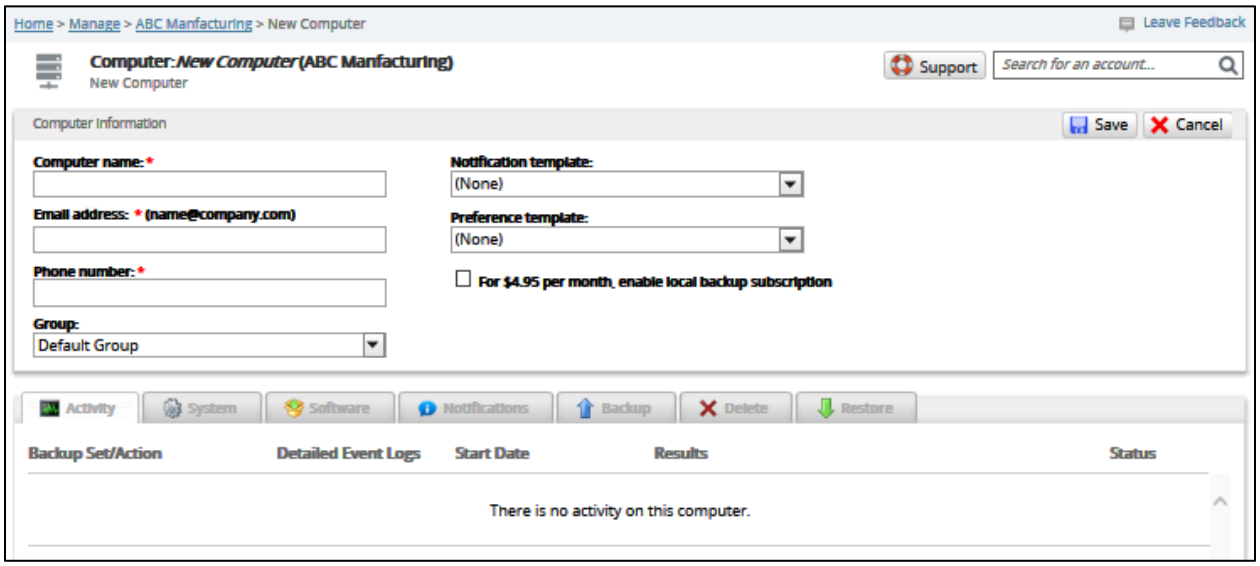
This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

The Manage Account page is displayed.



3. Click the **Add Computer** button.

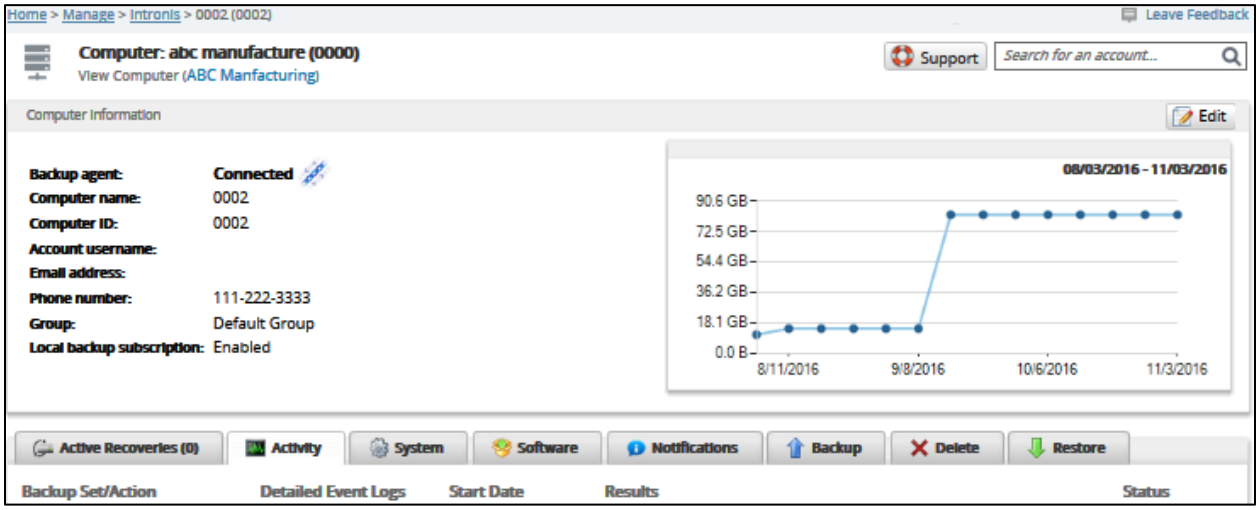
The New Computer form is displayed.



4. Complete the form for each computer to be added, and then click **Save**.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

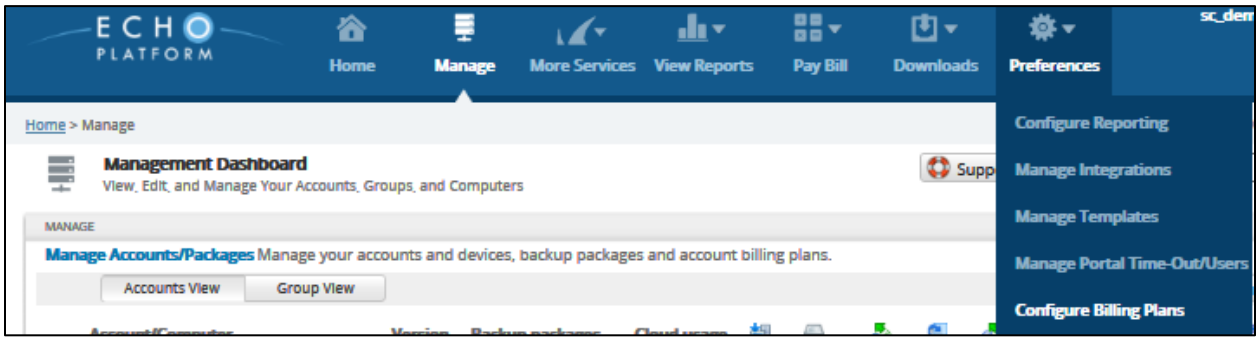
The new computer is displayed.



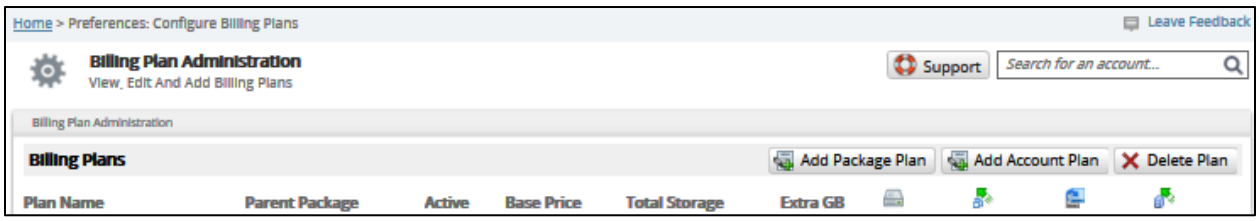
Creating an Account Billing Plan

To create an account-billing plan, perform the following steps.

1. At the ECHOplatform ribbon, click **Preferences**, **Configure Billing Plans**.



The Billing Plan Administration page is displayed.

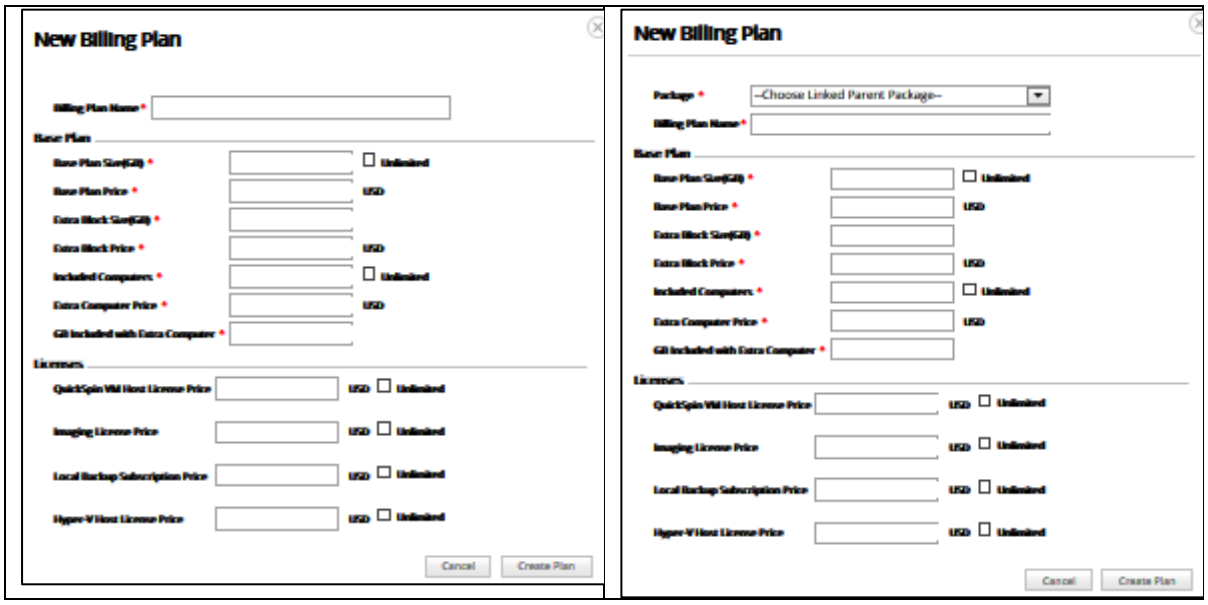


2. Click the **Add Account Plan** or the **Add Package Plan** button.

The **New Billing Plan** dialog is displayed.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Note: The Package Plan is displayed on the right.



This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

3. If you selected the Package Plan, then select the **Package** down arrow to display menu options.
4. Complete the fields, and then click the **Create Plan b**utton.

Note: The following table provides information about the **Unlimited** check box options.

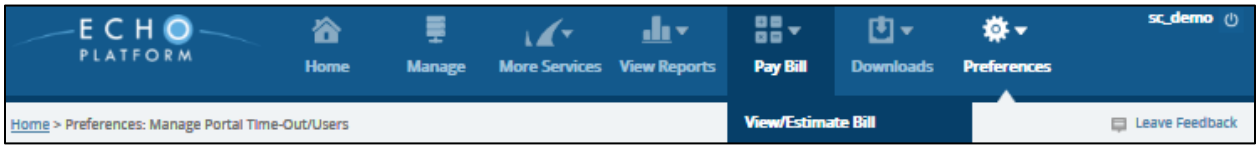
When you click the Unlimited check box beside the following field…	**Then,**
Base Plan Size	• the field becomes inactive and the word *Unlimited* displays indicating the Account Billing Plan does not impose a limitation on the amount of storage used by the accounts assigned to this billing plan. • the Extra GB Block Size field becomes inactive and *N.A.* (not applicable) displays. Accounts assigned to this Billing Plan have no limitations on extra blocks. • the Extra Block Price field becomes inactive and *N.A.* (not applicable) displays. Because there is no limitation on extra blocks, price is not tracked.
Included Computers	• the field becomes inactive and displays *Unlimited*. indicating that there is no limit on the number of computers an account can protect. • the Extra Computer Price field becomes inactive and displays *N.A.* (not applicable) indicating that because you can protect an unlimited number of computers, there is no need to specify an extra computer price. • the GB Included with Extra Computer field becomes inactive and displays *N.A.* (not applicable) indicating that because you can protect an unlimited number of computers, there is no need to specify an amount for allowed GBs.
QuickSpin VM Host License Price	the field becomes inactive and displays *N.A.* (not applicable) indicating that the account assigned to this billing plan can protect an unlimited amount of QuickSpin VM Hosts without incurring an extra charge.
Imaging License Price	the field becomes inactive and displays *N.A.* (not applicable) indicating that the account assigned to this billing plan can protect an unlimited amount of Imaging without incurring an extra charge.
Local Backup Subscription Price	the field becomes inactive and displays *N.A.* (not applicable) indicating that the account assigned to this billing plan can back up an unlimited number of computers locally without incurring an extra charge.
Hyper-V Host License Price	the field becomes inactive and displays *N.A.* (not applicable) indicating that the account assigned to this billing plan can protect an unlimited amount of Hyper-V Hosts without incurring an extra charge.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

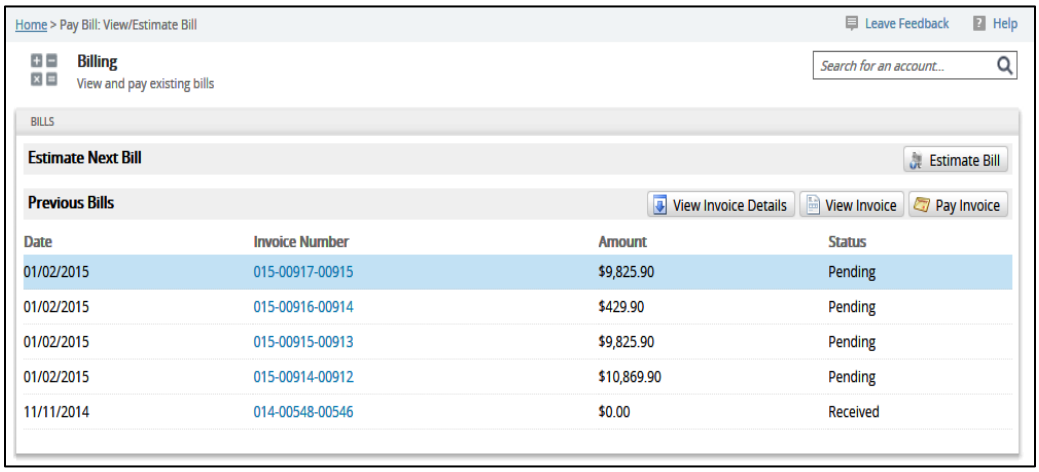
Managing Billing

To view your invoices, add credit cards or pay your bill, perform the following steps.

1. At the ECHOplatform ribbon, click **Pay Bill, View/Estimate Bill**.

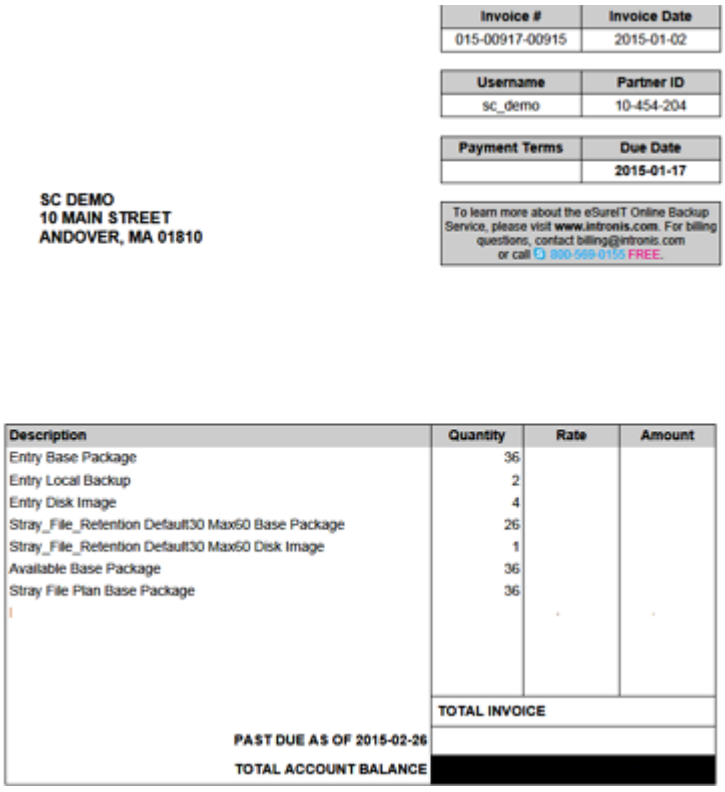
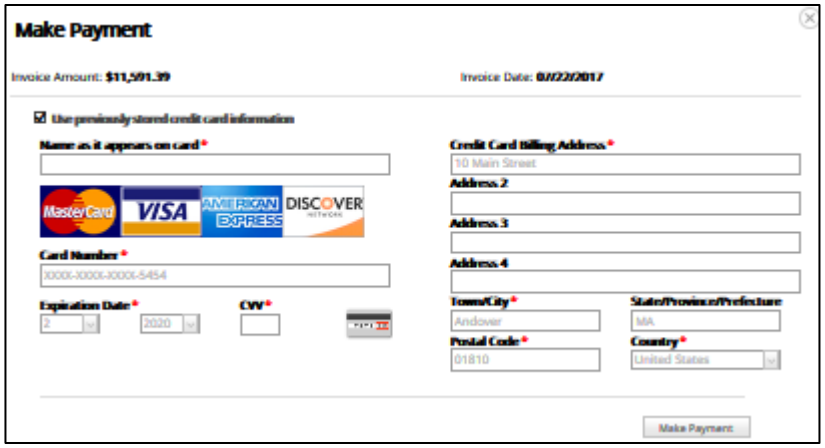


The Billing page is displayed.

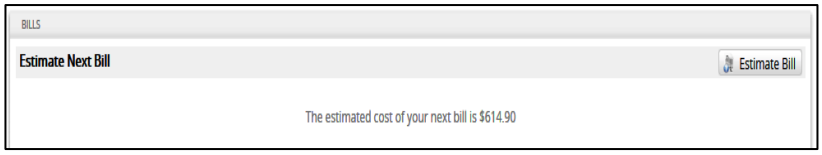


This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

2. You can perform any of the actions listed in the following table.

Action	Result
To view invoice details, select the **View Invoice Details** tab.	You are prompted to open or save a CSV report.
To view an invoice, click the Invoice Number or the **View Invoice** tab.	The invoice is displayed, as shown in the example below.  Invoice # 015-00917-00915 | Invoice Date 2015-01-02 Username sc_demo | Partner ID 10-454-204 Payment Terms | Due Date 2015-01-17 SC DEMO 10 MAIN STREET ANDOVER, MA 01810 To learn more about the eSureIT Online Backup Service, please visit www.intronis.com. For billing questions, contact billing@intronis.com or call 800-569-0155 FREE. Description | Quantity | Rate | Amount Entry Base Package 36 Entry Local Backup 2 Entry Disk Image 4 Stray_File_Retention Default30 Max60 Base Package 26 Stray_File_Retention Default30 Max60 Disk Image 1 Available Base Package 36 Stray File Plan Base Package 36 TOTAL INVOICE PAST DUE AS OF 2015-02-26 TOTAL ACCOUNT BALANCE
a. To make a payment, click the **Pay Invoice** tab. b. Type your information into the required fields, and then click **Make Payment**.	The Make Payment pop-up is displayed.  Make Payment Invoice Amount: $11,591.39 Invoice Date: 01/22/2017 Use previously stored credit card information Name as it appears on card * Credit Card billing Address * 10 Main Street Address 2 Address 3 Address 4 Card Number * Expiration Date * CVV * Town/City * Andover State/Province/Prefecture MA Postal Code * 01810 Country * United States Make Payment

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Action	Result
To view your bill estimate, click the **Estimate Bill** tab.	Your bill estimate is displayed. 

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Chapter 2. **Installing the Software**

This section includes the following topics:

- About software installation
- Downloading the backup agent software
- About the custom backup installer
- Creating a custom backup installer
- About the backup agent software
- Installing the backup agent software
- Deploying the backup agent software with an RMM tool

About Software Installation

Prerequisites: After you have created an account and added computers to the account, you can start downloading and installing the backup agent software by:

- Downloading the backup agent software, and then installing the backup agent software.
- Creating a custom backup agent installer, and then installing the backup agent software.

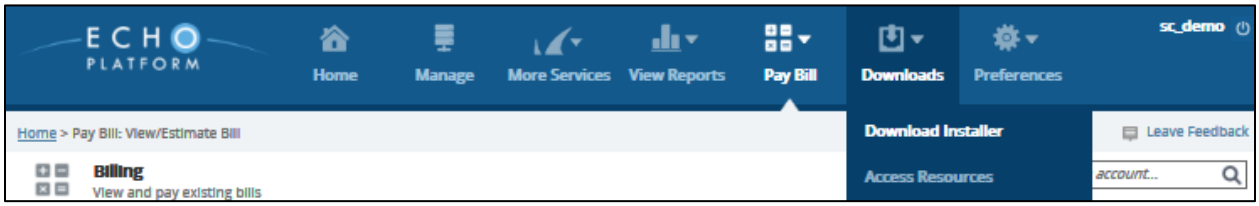
You can also deploy the backup agent software with a remote monitoring and management (RMM) tool.

Note: A custom backup agent installation allows you to configure the backup agent's settings from the Management Portal.

Downloading the Backup Agent Software

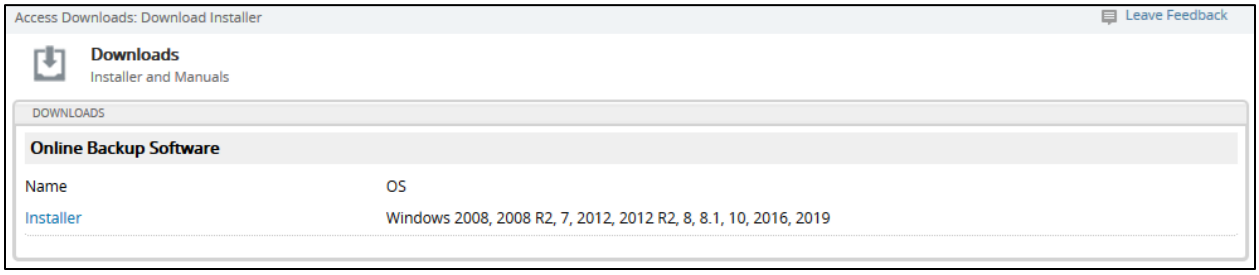
To download the backup agent software, perform the following steps.

1. At the ECHOplatform ribbon, click **Downloads, Download Installer**.



This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

The Downloads page is displayed.



2. Click the **Installer** link.
3. Run or save the software and install it on the computer.

The Setup Wizard is displayed.
See *Installing the Backup Agent Software* for procedure.

About the Custom Backup Installer

You can create a custom installer file that allows the software to self-install with the proper username, and Computer ID.

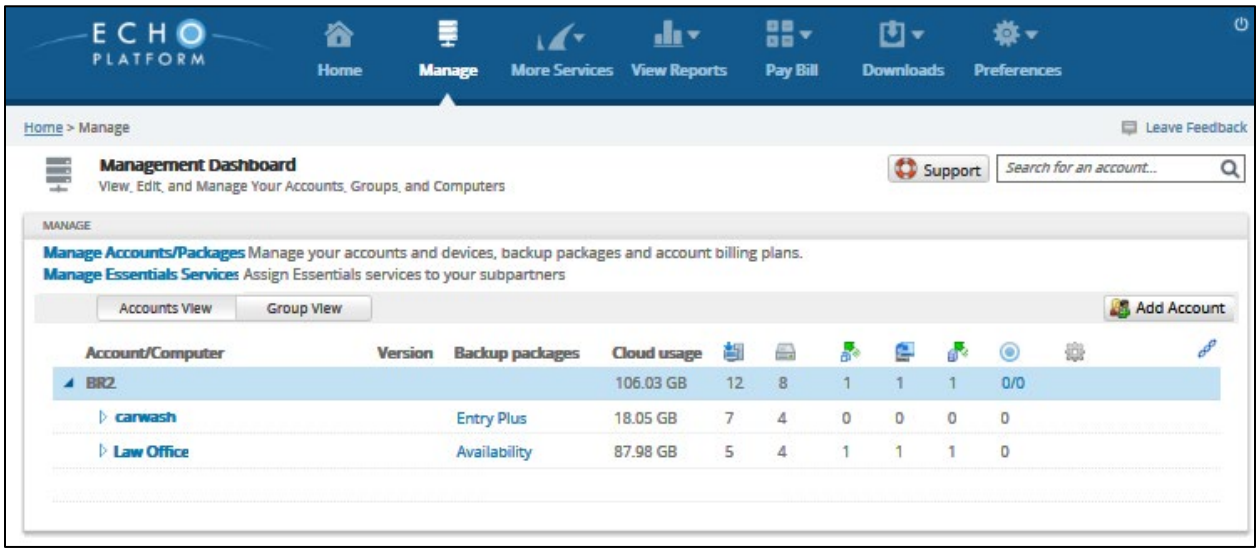
This option also allows you to configure the Backup Agent's settings from the Management Portal.

Creating a Custom Backup Installer

To create a custom backup installer, perform the following steps.

1. At the ECHOplatform ribbon, click **Manage**.

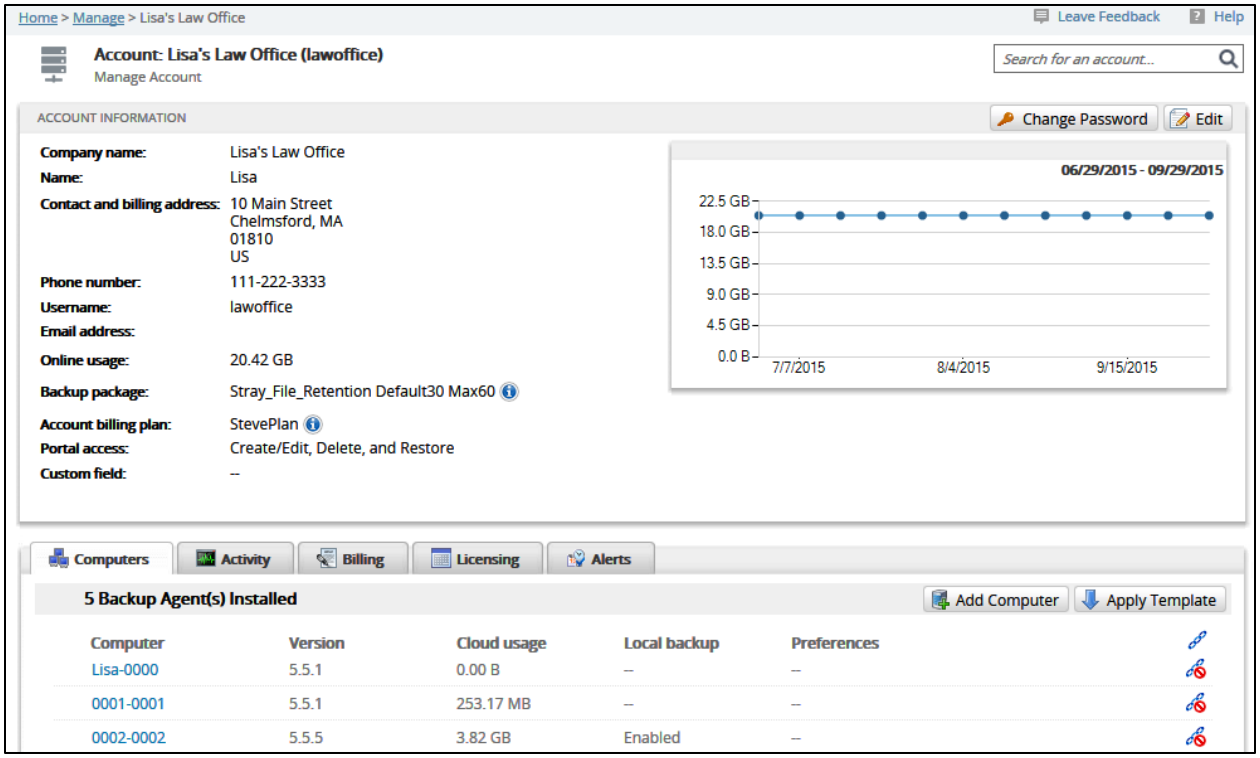
The Management Dashboard is displayed.



This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

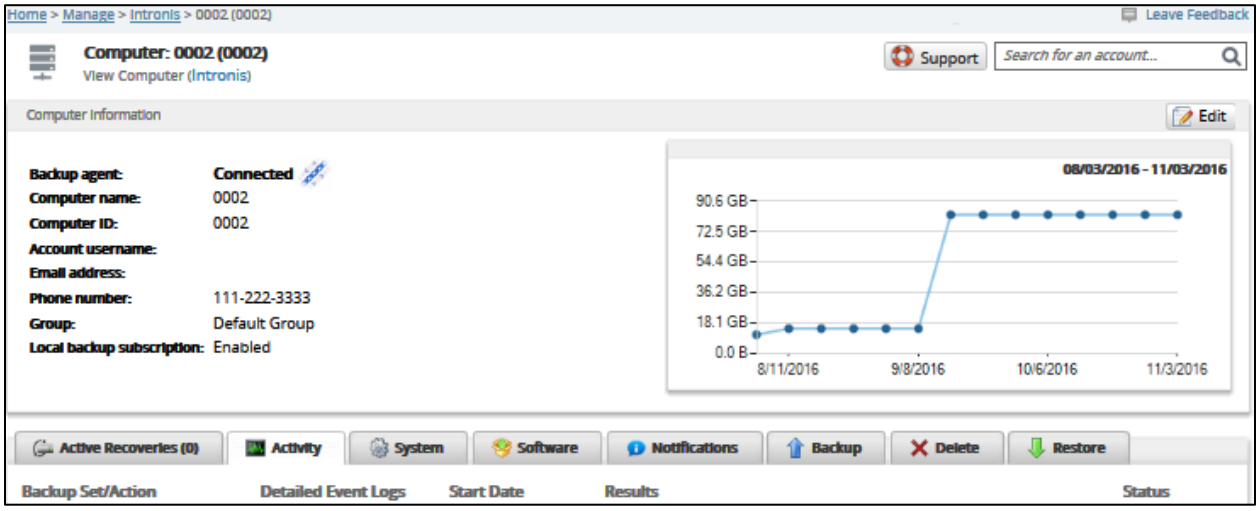
2. Select the account where the computer is located, for which you would like to create the installer.

The Manage Account page is displayed.



3. Select a computer from the Computer list.

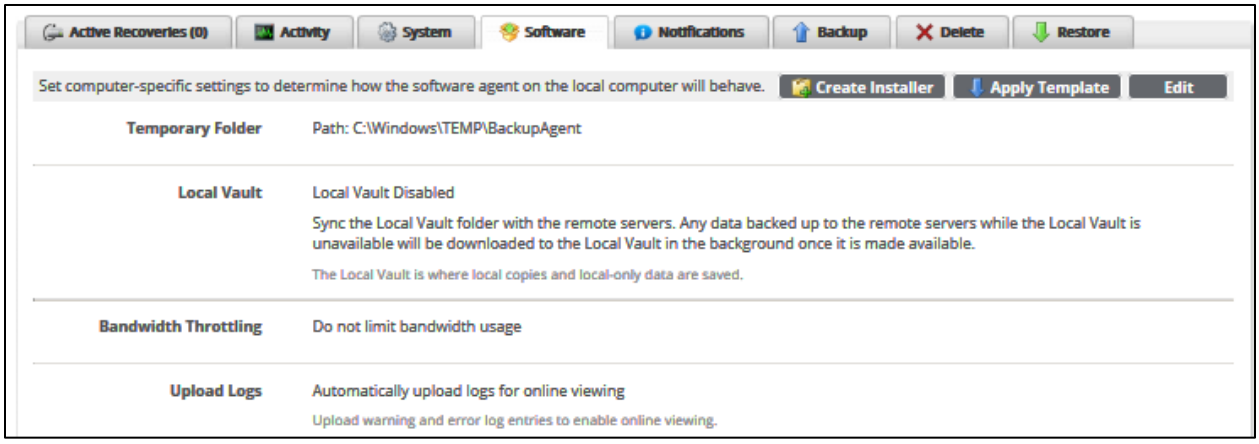
The Computer page is displayed.



This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

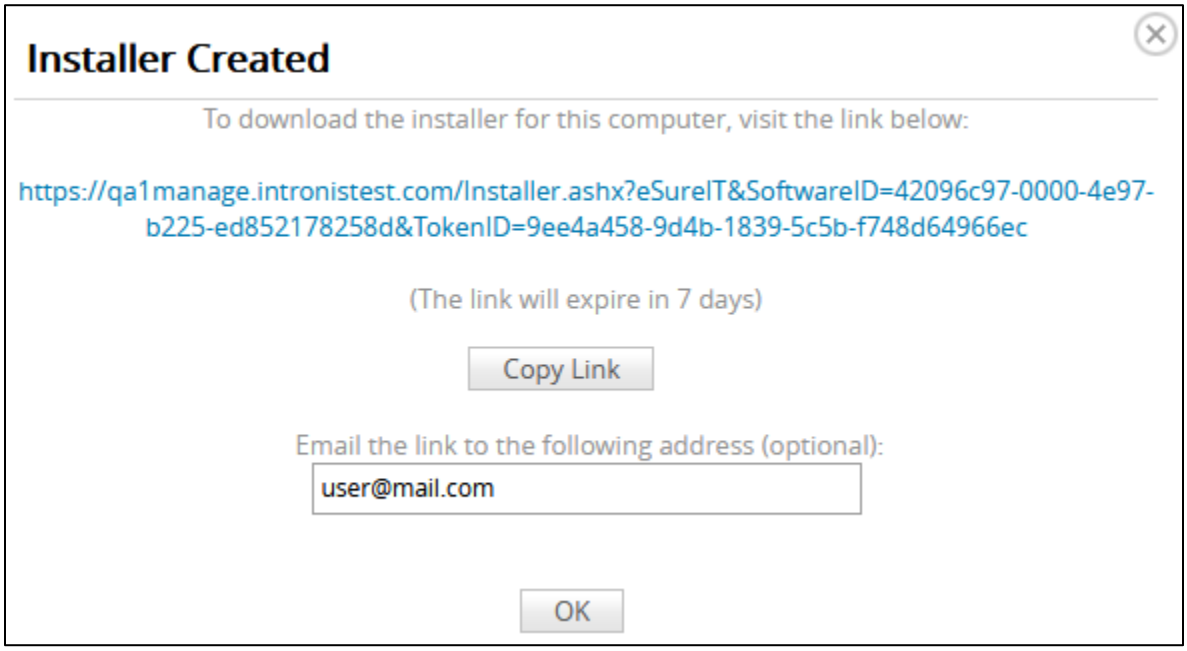
4. Click the **Software** tab.

   The software settings are displayed.



5. Click **Create Installer**.

   The Installer Created pop-up is displayed.



6. Copy and paste the link or email it to the contact for this computer, and then click **OK**.

   The Setup Wizard is displayed. See *Installing the Backup Agent Software* for procedure.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

About the Backup Agent Software

You have three options to choose from when installing the backup agent software:

- Recover Previous Installation
- Move Account to This Computer
- Recovery Mode

Recover Previous Installation

Recover Previous Installation is used when the agent has been removed or is unavailable and you want to reinstall.

Move Account to This Computer

Move Account to This Computer is used when the agent exists but you want to move it to this computer. Be aware that the other agent is invalidated.

Recovery Mode

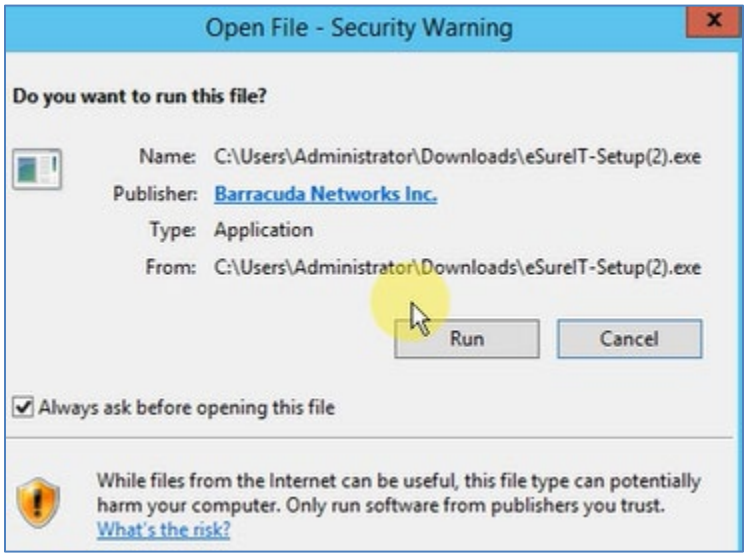
Recovery Mode is used when you want the other agent to continue to backup, but you want to install another agent for recovery purposes only.

Installing the Backup Agent Software

To install the backup agent software, perform the following steps.

1. Create a custom backup installer or download the backup agent software.
2. At your Download folder, click **eSureIT – Setup.exe**.

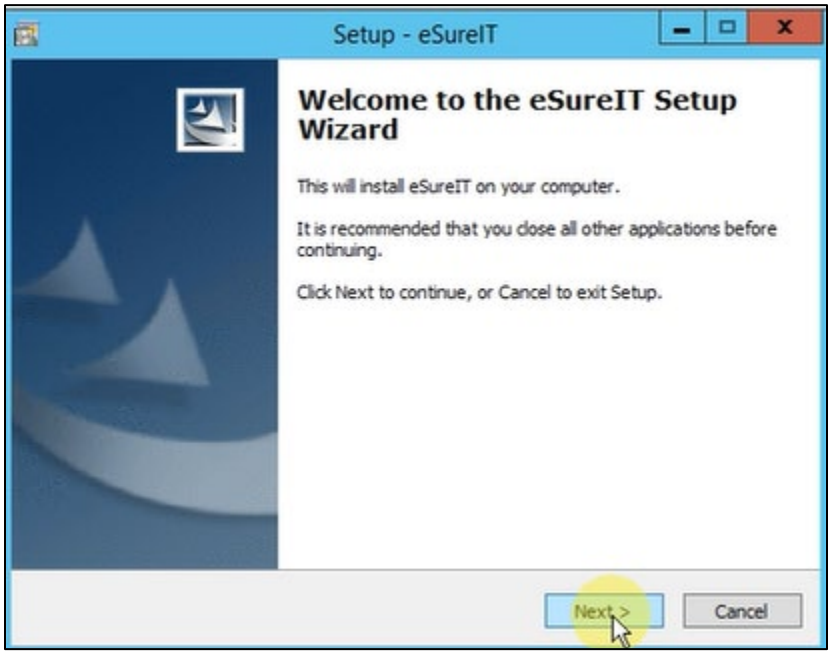
   The following pop-up is displayed.



3. Click **Run**.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

The Setup Wizard is displayed.



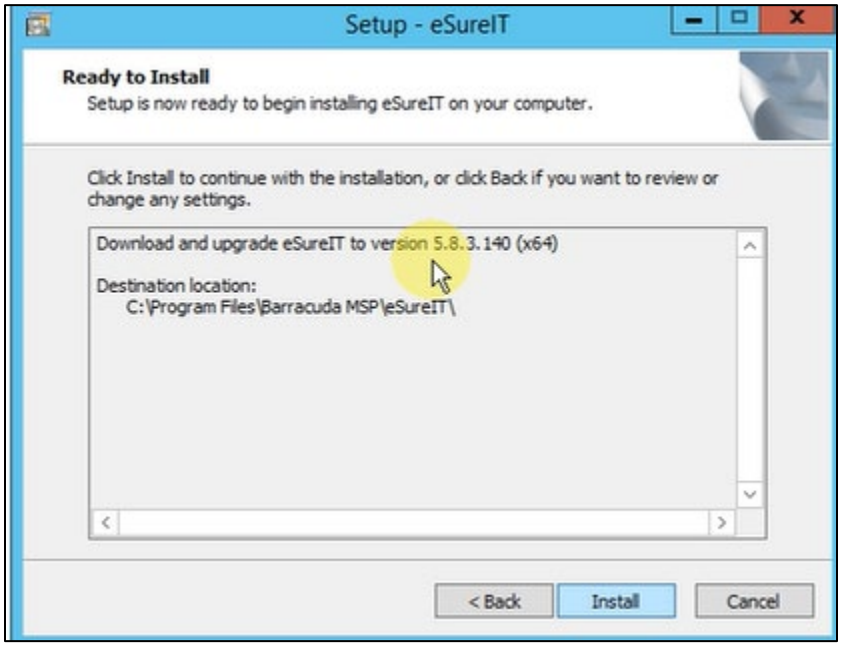
4. Close all open applications, and then click **Next**.

The License Agreement is displayed.

5. Read the agreement, click the **I accept the agreement** radio button, and then click **Next**.

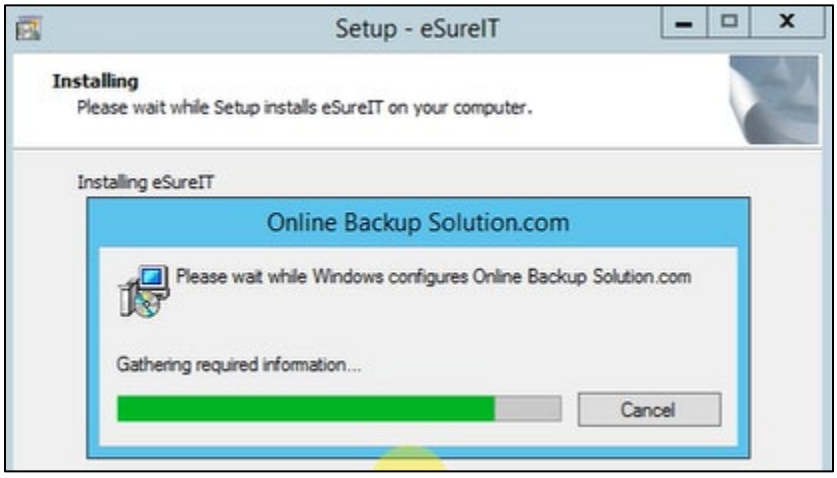
This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

The Ready to Install screen is displayed.



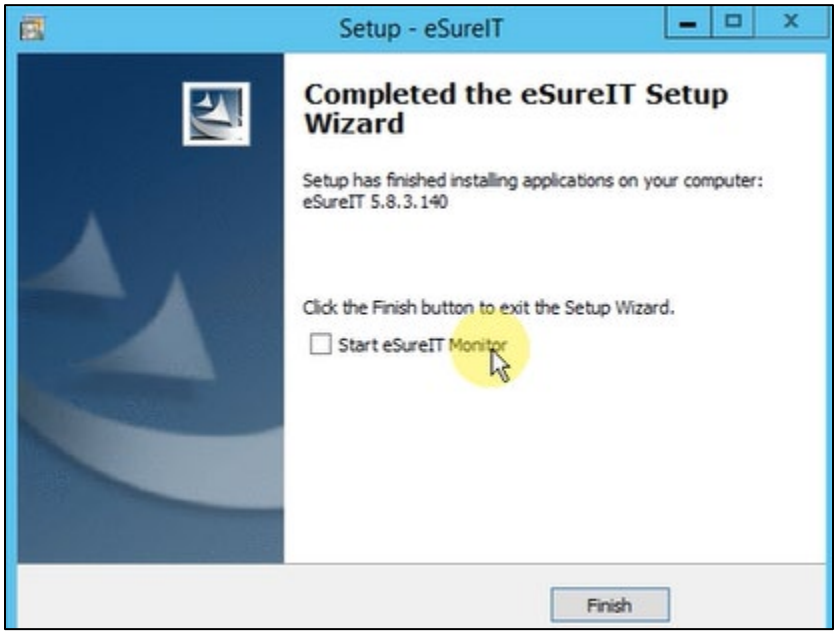
6. Click **Install**.

The installation status is displayed.



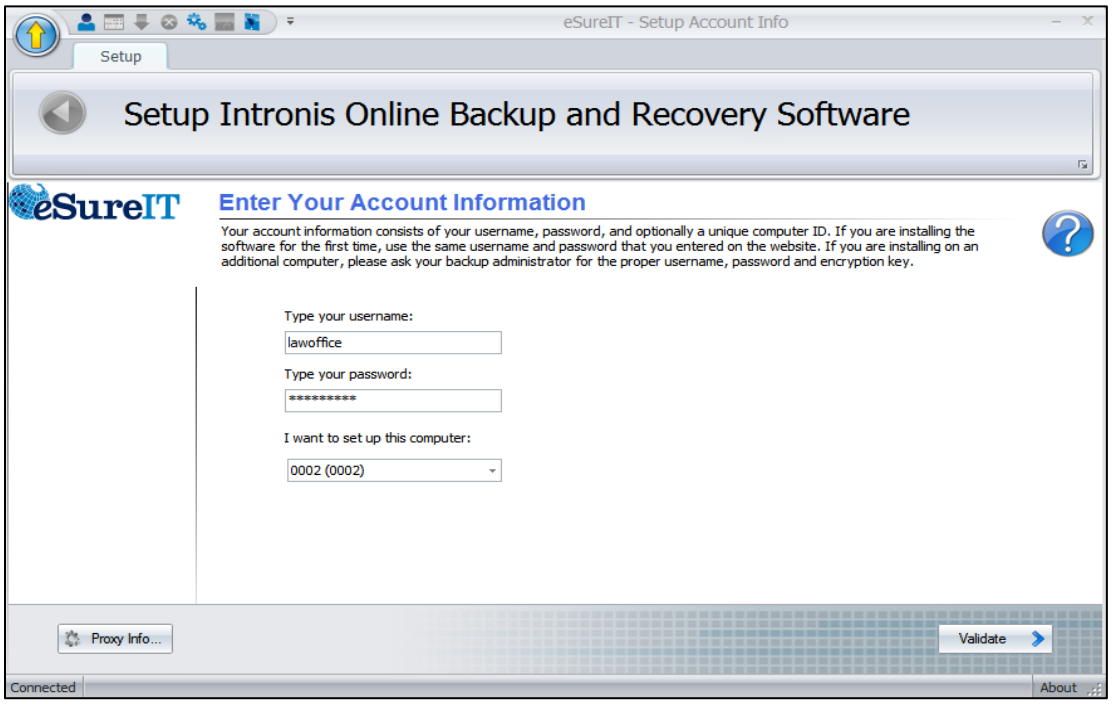
This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

After the setup is complete, the Finish screen is displayed.



7. Click the **Start eSureIT Monitor** check box, and then click **Finish** to complete installation.

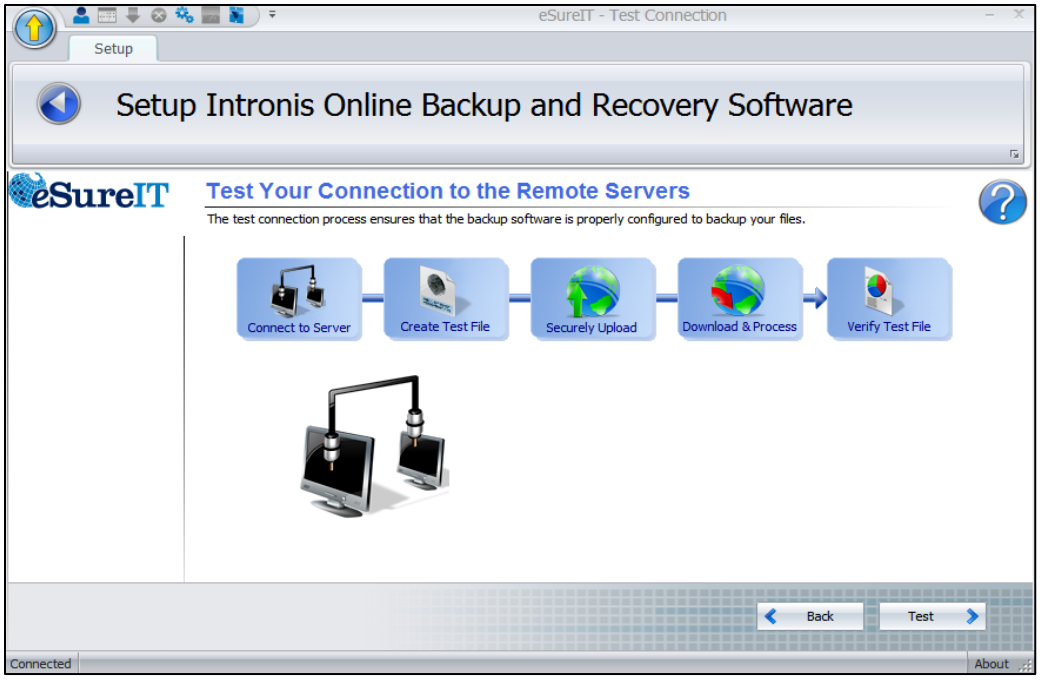
The Setup screen is displayed.



This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

8. Type username, password, and computer, and then click **Validate**.

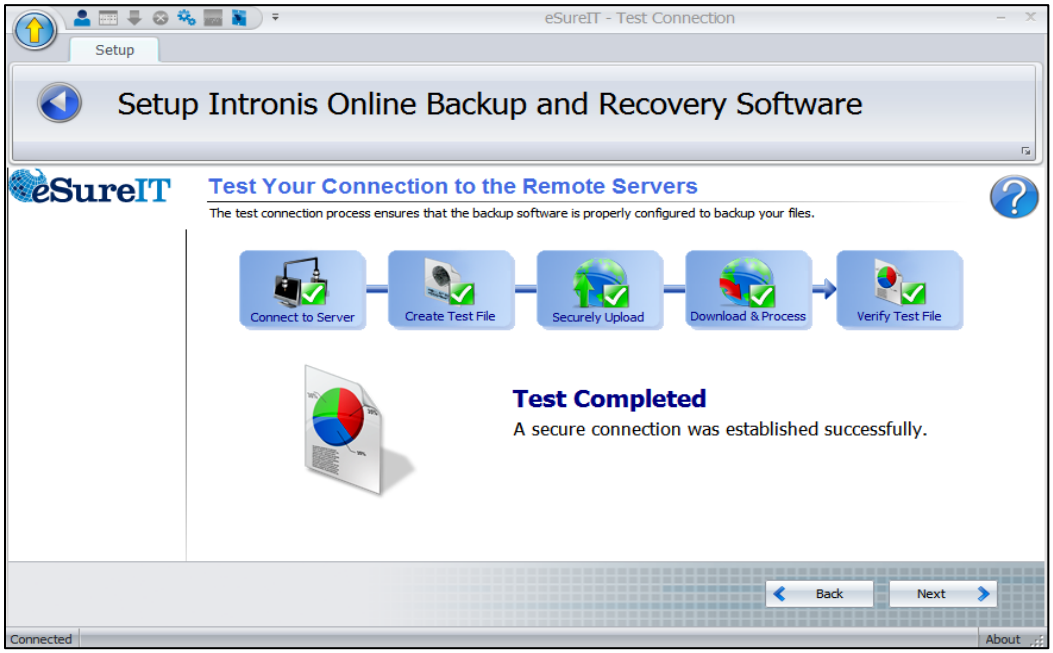
The Test screen is displayed.



9. Click the **Test** button.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

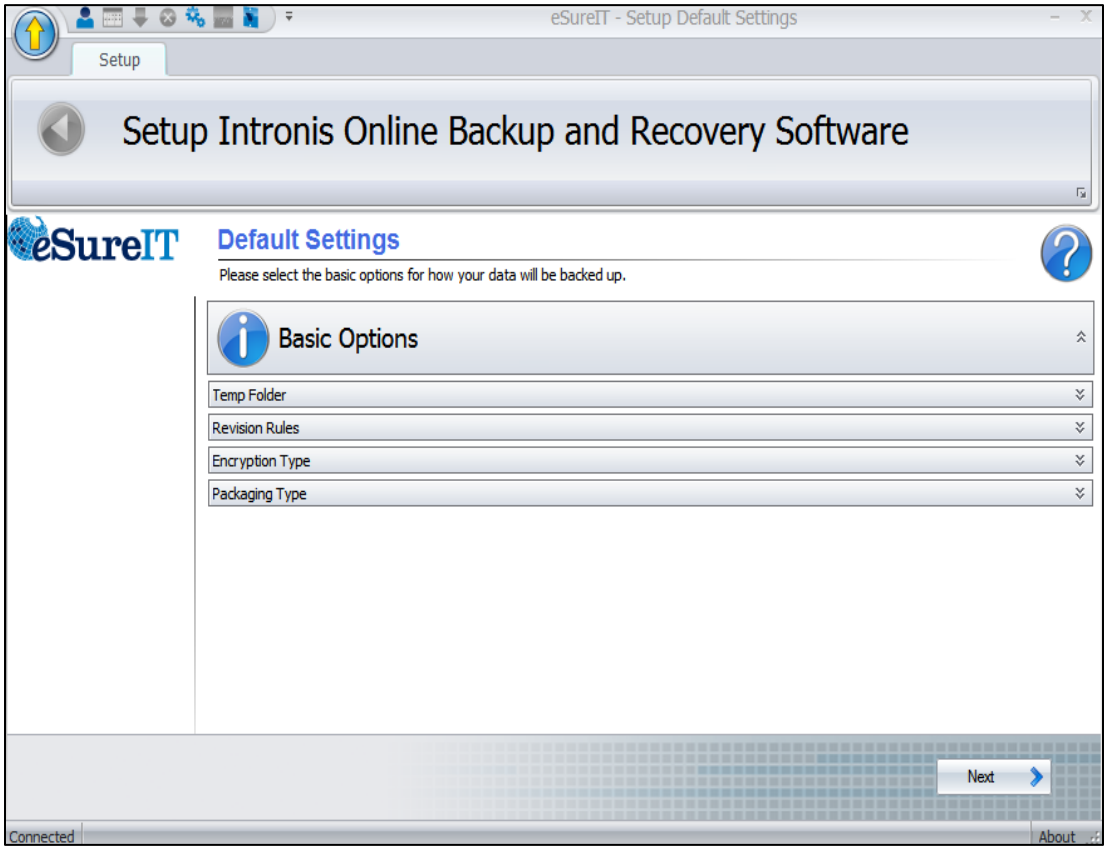
The tests are performed, and the Next button is displayed.



10. Click **Next**.

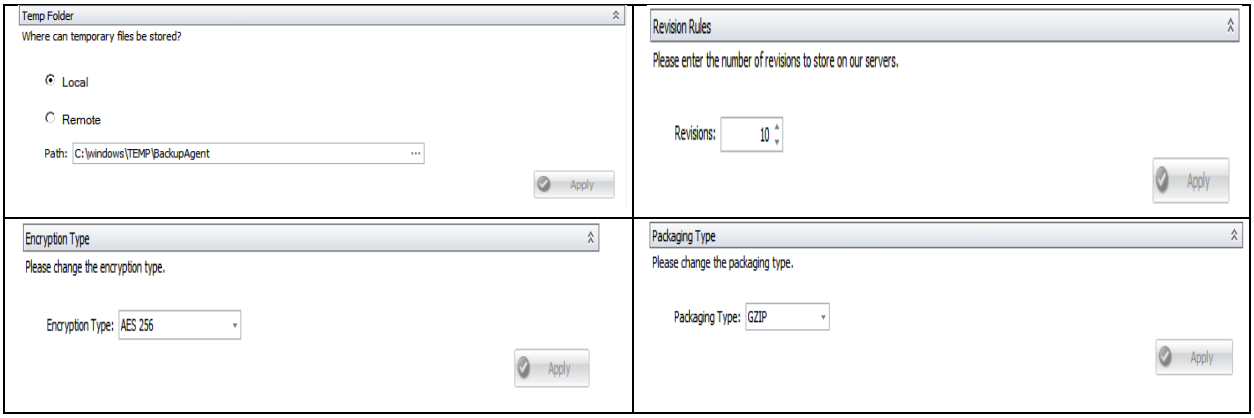
This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

The Default Settings screen is displayed.



11. Click each option bar to display default settings, and if desired make your changes.

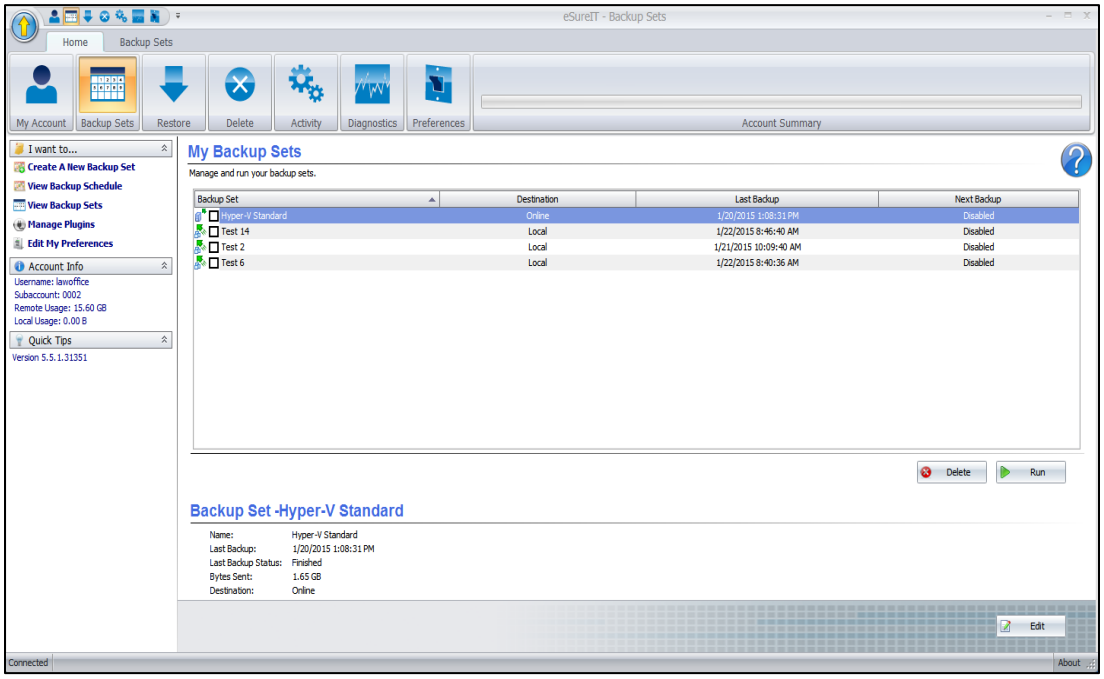
    The options are displayed below.



12. When complete, click **Next**.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

The Backup Monitor is displayed.



13. If moving an account or installing in recovery mode, run the restore.

- Select the files, folders, or backup sets from which you wish to restore.
- To restore the latest versions of the files, select them, and then select the **Restore** button.
- To restore different revisions that have been stored, select the **(+)** next to each individual file, select the desired revision, and then select the **Restore** button.

14. Proceed to restore data through the Restore wizard in the portal, making sure to choose the correct installation when prompted.

Note: An eSureIT Monitor shortcut is also displayed on your desktop, as shown in the following example.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Deploying the Backup Agent Software with RMM Tool

After you have downloaded the installer, you can deploy it with RMM tools such as:

- Kaseya
- Level Platforms
- N-able
- Avast

To deploy the backup agent software with RMM, use the command line switches in the following table.

Command Line Switch	Description
/Username=user_test	Specifies the username to be used during Monitor setup - only for new accounts.
/Password=1234567	Specifies the password to be used during Monitor setup - only for new accounts.
/ComputerID=0000	Specifies the Computer ID to be used during Monitor setup - only for new accounts.
/ManagedKey	If added, managed key will be used during Monitor setup - only for new accounts.
/Silent	Runs the installer in silent mod. User interaction is not required.
/SuppressMsgBoxes	Combined with /silent, suppresses setup message boxes.
/VerySilent	Does not display any software message boxes or screens unless errors are encountered.

Note: All parameters are case sensitive.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

[This page left intentionally blank.]

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Chapter 3. Initial Seed

This section includes the following topics:

- About initial seeds
- Initial seed requirements
- Initial seed recommendations
- Creating the initial seed

About Initial Seeds

An **initial seed** is your first full backup on a local hard drive. The initial seed is mailed to the Barracuda office for direct upload to Barracuda servers.

This option is recommended for uploading the initial full backup of backup sets greater than 100Gbs, especially where the customer's bandwidth is limited. After uploading this data to Barracuda servers, your backups continue running on schedule, backing up the block-level differential changes to the initial upload of the data.

The initial seed is a feature that *must* be enabled by request.

Initial Seed Requirements

Contact Partner Support to create a ticket for your initial seed. For contact information, see *Barracuda Partner Support*.

You can email or call with the specific username and subaccounts on which you would like to perform the initial seed. Barracuda emails you the **Local Drive Seed** form that should be returned with your drive.

Initial seed drives must be formatted as NTFS prior to seeding data to the drive.

This requirement ensures the integrity of the data being copied to the drive.

File systems such as FAT32 have restrictions on the number of files in a folder that can cause problems when backing up an initial seed.

Drives that are not formatted as NTFS or are flagged by Barracuda antivirus software are returned to the customer for proper initial seed drive processing.

Creating the Initial Seed

To create the Initial Seed, perform the following steps.

1. When preparing for local backup, create the following folder structure on your external drive: *X:\Intronis\username\subaccount id.*
2. When starting the initial backup, expand the **Local Backup** section in the Backup Request dialog, and then select **Perform a local backup**.
3. Select the path you have created in step 1, ending in the subaccount ID.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Special Considerations

The folder structure is case sensitive. Where *username* is the username on this account, and where *0000* is the subaccount ID on this subaccount. These items are reported in the left pane of the Backup Monitor.

The volume of data must be 100 Gb or larger. You can seed multiple accounts if necessary, to achieve this amount.

Running the initial seed from the Management Portal creates the file structure automatically.

If you run the initial seed from the Backup Monitor (for example, a customer's computer) you must name the folder structure as: *Intronis\username\subaccount id*.

Initial Seed Recommendations

The following table provides the initial seed backup recommendations.

Do…	**Do Not…**
Send Barracuda the initial seed sooner rather than later.	Put an Initial Seed and a Local Vault on the same drive.
Run backups while the initial seed is in transit. Intelliblox® technology sends only the changes made since the initial seed was created.	Put an Initial Seed and the Temporary Space on the same drive.
Fill out the Local Drive Seed Form after the local backup is complete and send the form, along with the hard drive, to: Barracuda ATTN: Client Services 100 Apollo Drive 2nd Floor Chelmsford, MA 01824	Include SQL or Exchange backups if you are doubtful of customer's connection.
Note any special circumstances that surround this initial seed.	Delete data without resetting the account. Restore data until the initial seed data has been uploaded by Barracuda.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Chapter 4. **Home Dashboard**

This section includes the following topics:

- About the Home Dashboard
- Group Selection Menu
- Include Recurring Interval-Based Backups Option
- Last Updated Summary
- Backups Finished
- Backup Status Icons
- Status Display Filters
- Expanded View
- Actual Time or Elapsed Time Display
- Backup Status Sorted by Accounts and Filters
- Backup Status Display
- Navigation Links
- Viewing Activity Logs from the Home Dashboard Expanded View
- Running Backup Sets from the Home Dashboard

About the Home Dashboard

The Home Dashboard is designed to provide you with a quick view of your backup status. From the dashboard, you can also perform the following actions:

- Sort by Account or Group
- Select status filters, computers, and logs
- Set time, date, and display parameters
- Run manual backups

Note: At least one agent must be connected for the dashboard to display.

The following sections describe the Home Dashboard from the top to the bottom.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Group Selection Menu

The Select Group to Display drop-down menu (see Figure 1) allows you to choose any group of computers that you have created and display only the results for computers in that group.

The default setting is **All Computers (No Group)**.

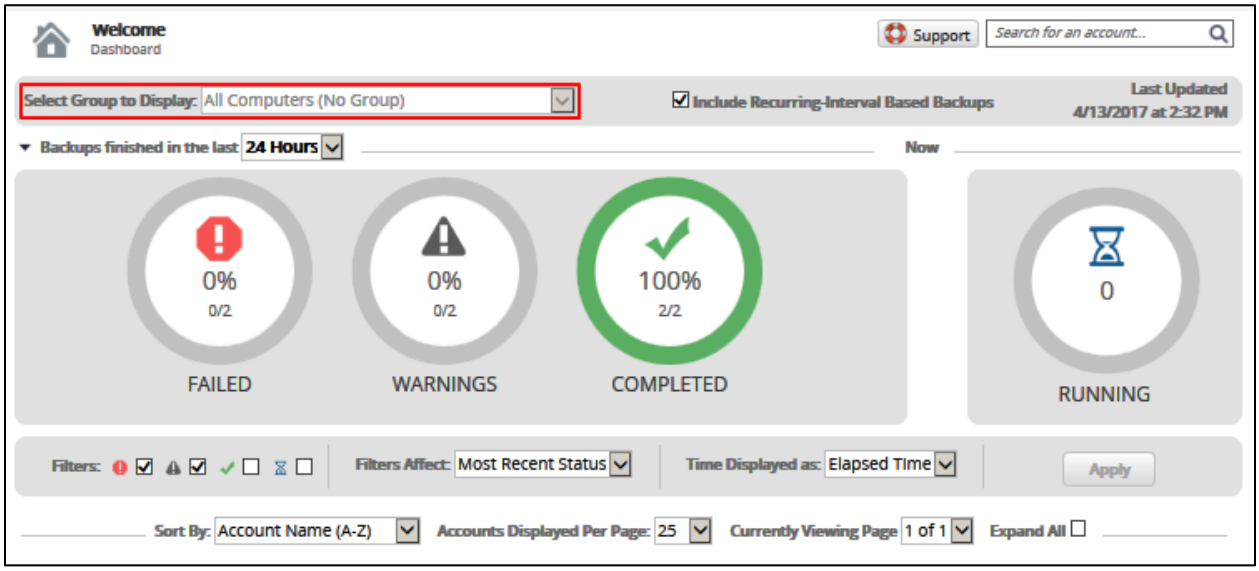


Figure 1. Group Selection Drop-down Menu.

Include Recurring Interval-Based Backups Option

The **Include Recurring Interval-Based Backups** check box allows you to include or exclude recurring interval-based backups. The default setting is to include recurring interval-based backups, as shown in Figure 2.

Figure 2. Include Recurring Interval-Based Backups Option.

Last Updated Summary

The Last Updated summary provides the date/time of the last update, and drop-down menus that allow you to select the number of accounts to display as well as the page that you want to view, as shown in Figure 3.

Figure 3. Last Updated Summary.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Backups Finished

The Backups Finished drop-down menu (see Figure 4) allows you to determine the period for which you want backup status reported. The incremental options are:

- 12 Hours
- 24 Hours
- 7 Days

Figure 4. Backup Time Periods.

Backup Status Icons

The following table provides a description of the Home dashboard icons.

Icon	Description
	Failed
	Warnings
	Completed
	Running

The ratio below each percentage (highlighted in Figure 5 below), represents the number of successful backups over the total number of backups that have completed. Therefore, if a backup is completed 3 times in the past 7 days, the count is reported as three.

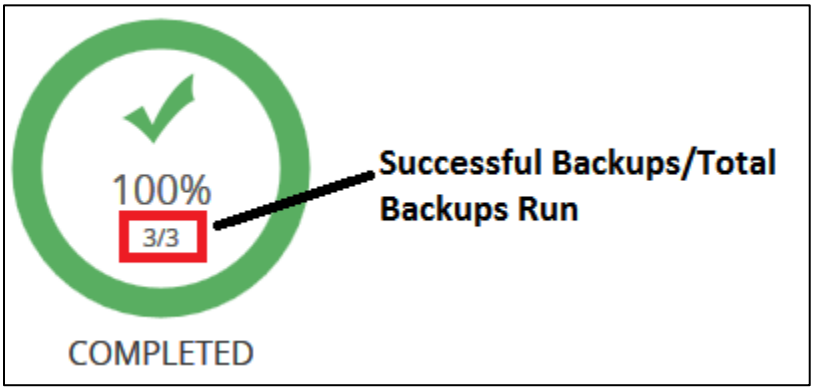


Figure 5. Ratio Example.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Status Display Filters

The Status Display Filters can be set by clicking the **Filters** checkbox and then selecting from the Filters Affect drop-down menu. You may select the most recent backup status or the status of all backups.

After selecting your option, you must click the **Apply** button.

The example shown in Figure 6 is set to display all backups that have failed.

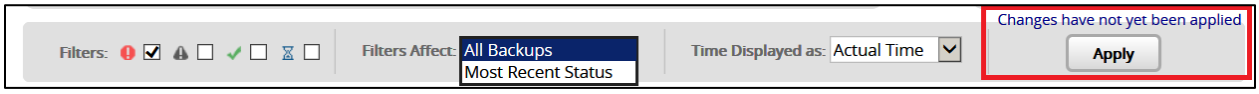


Figure 6. Filters Affect Drop-down Menu.

The Filters display the following status:

- Backups that have failed.
- Backups completed with warnings.
- Backups completed.
- Backups that are currently running.

Expanded View

Clicking the **Expand All** check box, as shown in Figure 7, provides a detailed view of backup status.

In the Expanded View, you may sort by Account Name and select the number of accounts displayed on the page. You do not need to click the **Apply** button to Expand All.

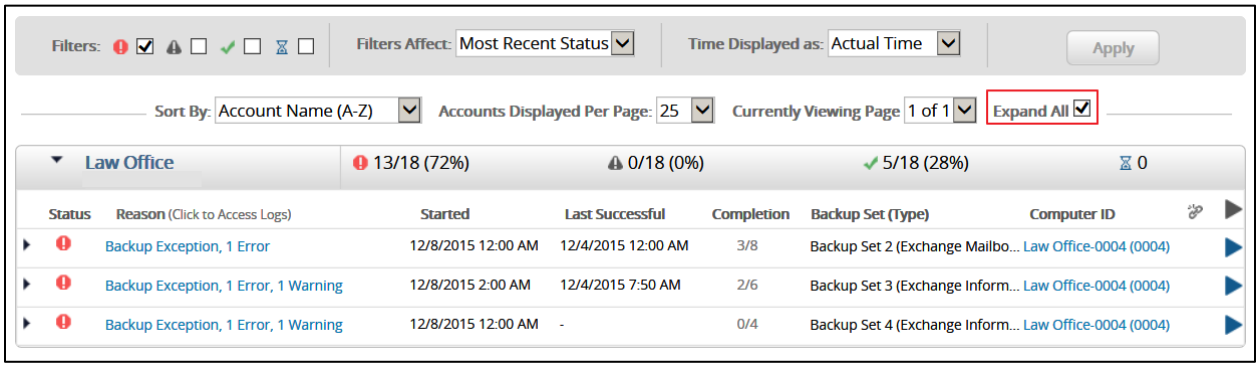


Figure 7. Expand All Option.

Also, by clicking the status icon within the donut chart (see Figure 8), you can change the display to only that selected status in the expanded view. You do not need to click the **Apply** button to filter status with this option.

For example, if all the **Filters:** check boxes are selected as shown in Figure 8, and you click the

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Completed status icon, then only the Completed check box remains selected and all other check boxes are cleared, as shown in Figure 9.

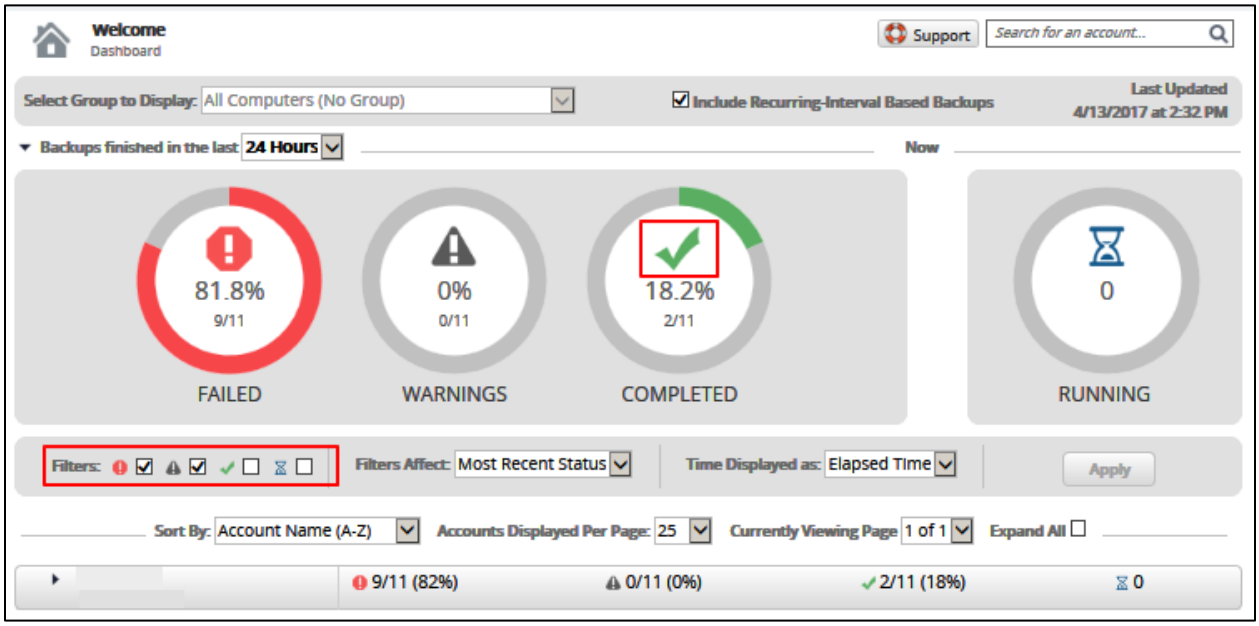


Figure 8. Before Status Filter Is Applied.

When adding or removing additional filters by selecting their check boxes, you must click the **Apply** button to effect the changes.

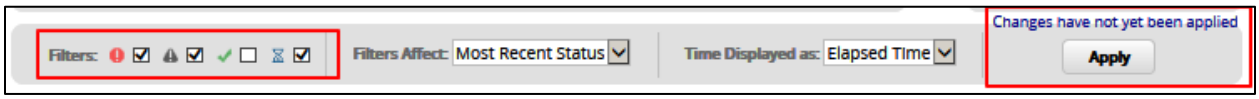


Figure 9. After Status Filter Is Applied.

Actual Time or Elapsed Time Display

You have the option to view accounts or backup sets by actual time or elapsed time. Both settings report when the backup was started and when the backup was last successful. The difference is in *how* that information is displayed:

Elapsed time, the default, displays that the backup started 7 hours ago.

Actual time displays that the backup started 8/13/2015 4:00 AM.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Figure 10 provides a display of the new feature.

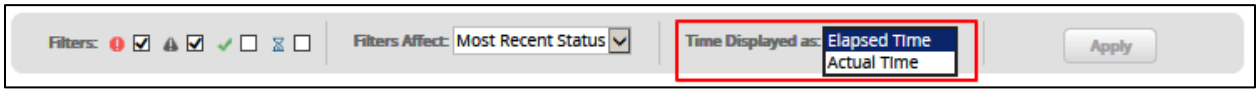


Figure 10. Actual Time and Elapsed Time Features.

To display backup times in the Start column and the Last Successful column (see Figure 11), select **Elapsed Time** or **Actual Time** from the **Time Displayed as** drop-down menu, and then click the **Apply** button.

Hovering over the time in the Started or Last Successful columns displays the alternate option. For example, if the *elapsed* time of **11 hours ago** is displayed, hovering over that time displays the *actual* time of **9/1/2015 10:25 A.M**.

Figure 11 provides an example of backup times displayed with the Elapsed Time option.

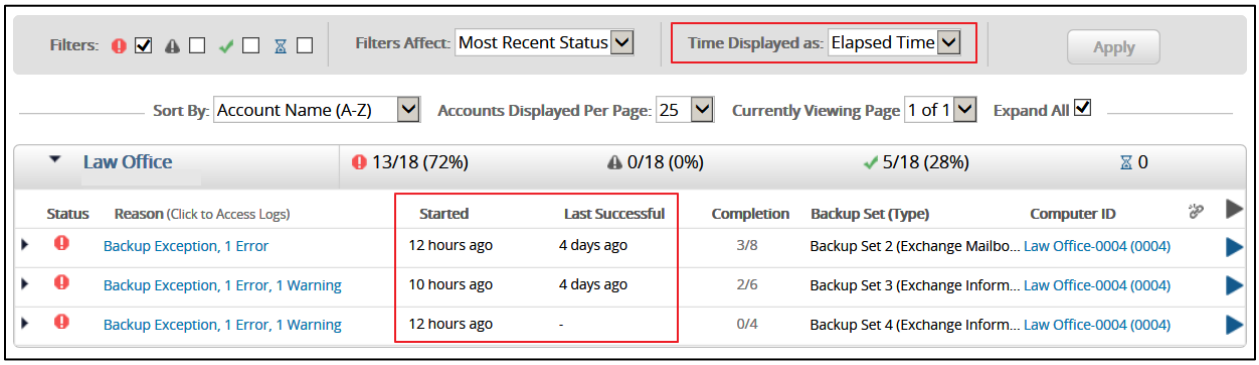


Figure 11. Elapsed Time Display.

Figure 12 provides an example of backup times displayed with the Actual Time option.

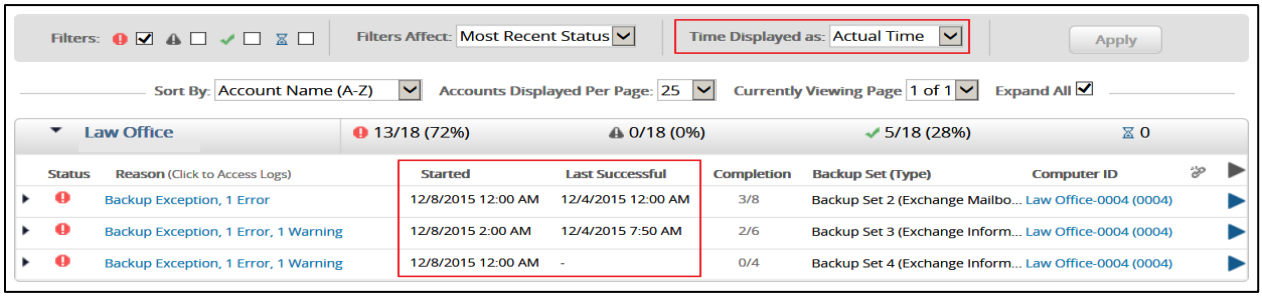


Figure 12. Actual Time Display.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Backup Status Sorted by Accounts and Filters

You can use the **Sort By** drop-down menu to manage the backup status that you would like displayed graphically, as shown in Figure 13.

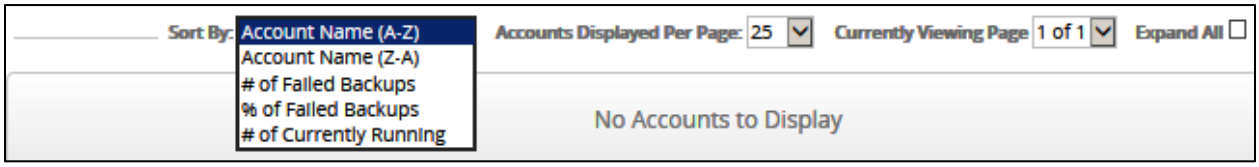
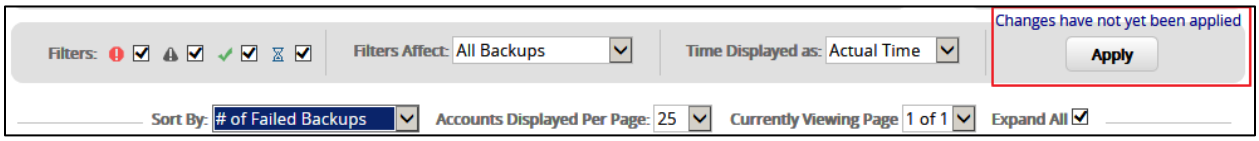


Figure 13. Graphic Status Sorted by Accounts and Filtered by Status.

You can *sort* the accounts that are to be displayed graphically by the following categories:

- Account name (A-Z)
- Account name (Z-A)
- # of failed backups
- % of failed backups
- # of currently running

After you make your selections, the **Changes have not yet been applied** message is displayed, as shown below.



Click the **Apply** button to apply the changes.

The Accounts Displayed Per Page and Viewing Page drop-down menus allow you to select the number of accounts to display as well as the page that you want to view.

Backup Status Display

The Backup Status is displayed on the Home page as shown in Figure 14. The Backup Status Display graphically shows all backup sets run under the accounts managed by a partner.

Failed, Warning, and Running backups are displayed by default.

Without logging into customers' computers to troubleshoot, you can view which user account, which computer, and even which activity needs to be examined from the Barracuda Management Portal.

Each backup set is listed along with the associated account and computer.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

The logs you can access list the errors and the warnings that occurred during an action, but they do not list informational details. See *Backup Status Report.*

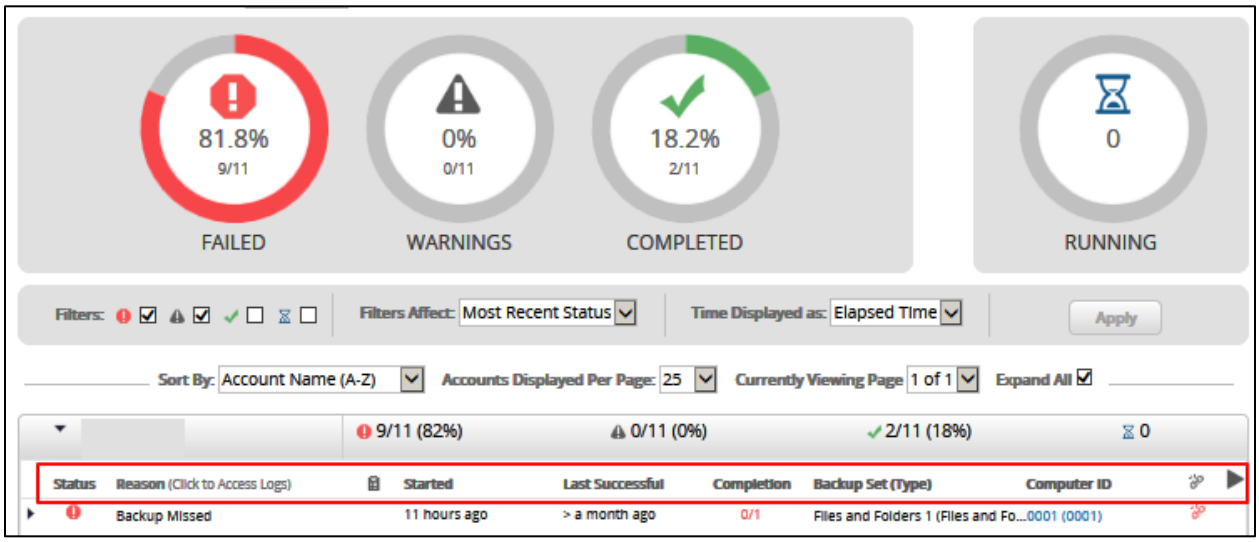


Figure 14. Backup Status.

Backup Status Details

The following table provides a description of the columns displayed in the Backup Status Display.

Column	Description
Status	The status of each backup is represented by an icon where: • Red = failed • yellow = warning • green = running • gray = completed
Reason	Includes all applicable reasons.
Started (Agent Local Time)	Displays start time date and time and represents the start time from the perspective of the agent running the backup.
Last Successful	Displays last successful backup date.
Completion	Displays number of completions.
Backup Set (Type)	Displays backup set name and type.
Computer (ID)	Displays computer name and ID. Links to the Computer Details page.
Connected Icon	Displays whether the agent is connected to the relay server or not.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Navigation Links

The following links are provided in the expanded status view:

- Account
- Status reason
- Computer ID
- Manually restart backup

Account Link

Clicking the Account link, highlighted in Figure 15, displays the Manage Account page.

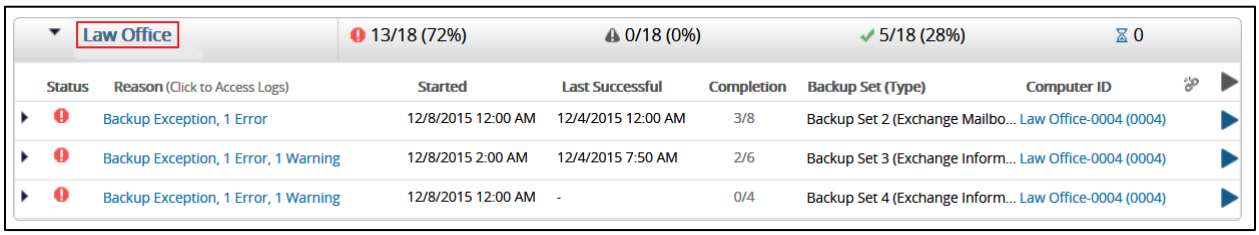


Figure 15. Account Link.

Status Reason Link

Clicking the Reason column link, highlighted in Figure 16, displays the Backup Set Status Log.

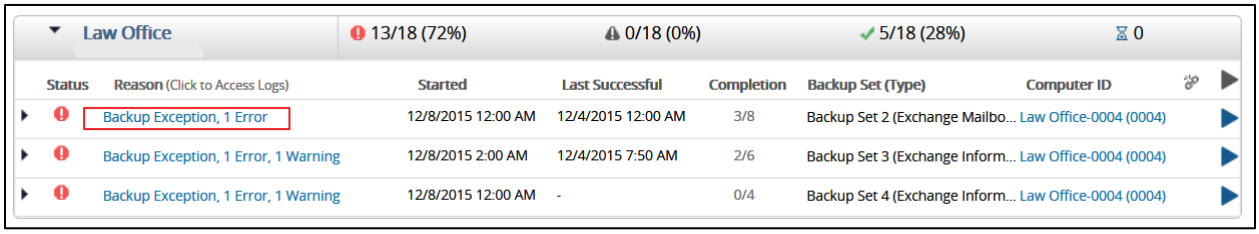


Figure 16. Status Reason Link.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Computer ID Link

Clicking the Computer ID link, highlighted in Figure 17, displays the Computer page.

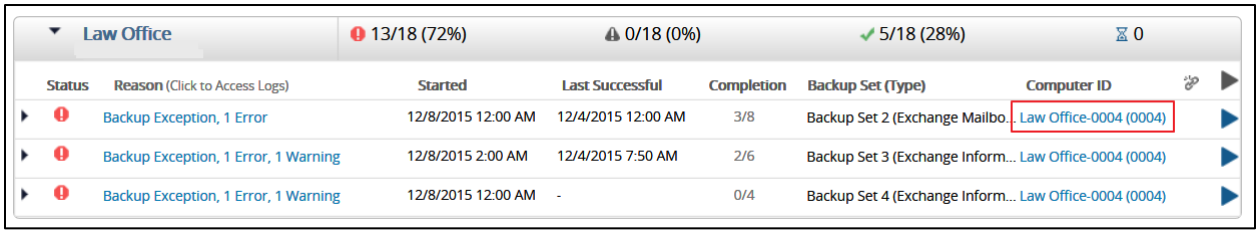


Figure 17. Computer ID Link.

Manually Restart Backup Link

Clicking the Manually Restart Backup link, highlighted in Figure 18, restarts the backup job.

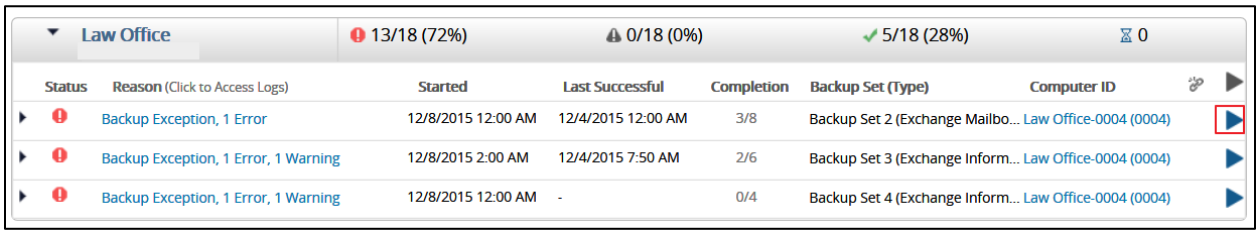


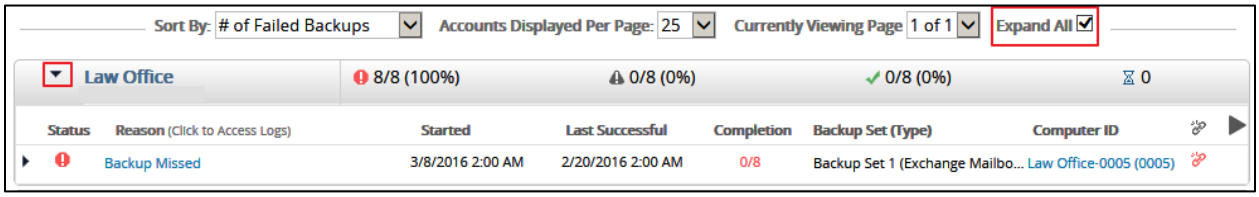
Figure 18. Manually Backup Restart Link.

Viewing Activity Logs from the Home Dashboard Expanded View

To view Activity logs from the Expanded View, perform the following steps.

1. Click the arrow by the account or selecting the **Expand All** check box, as highlighted below.

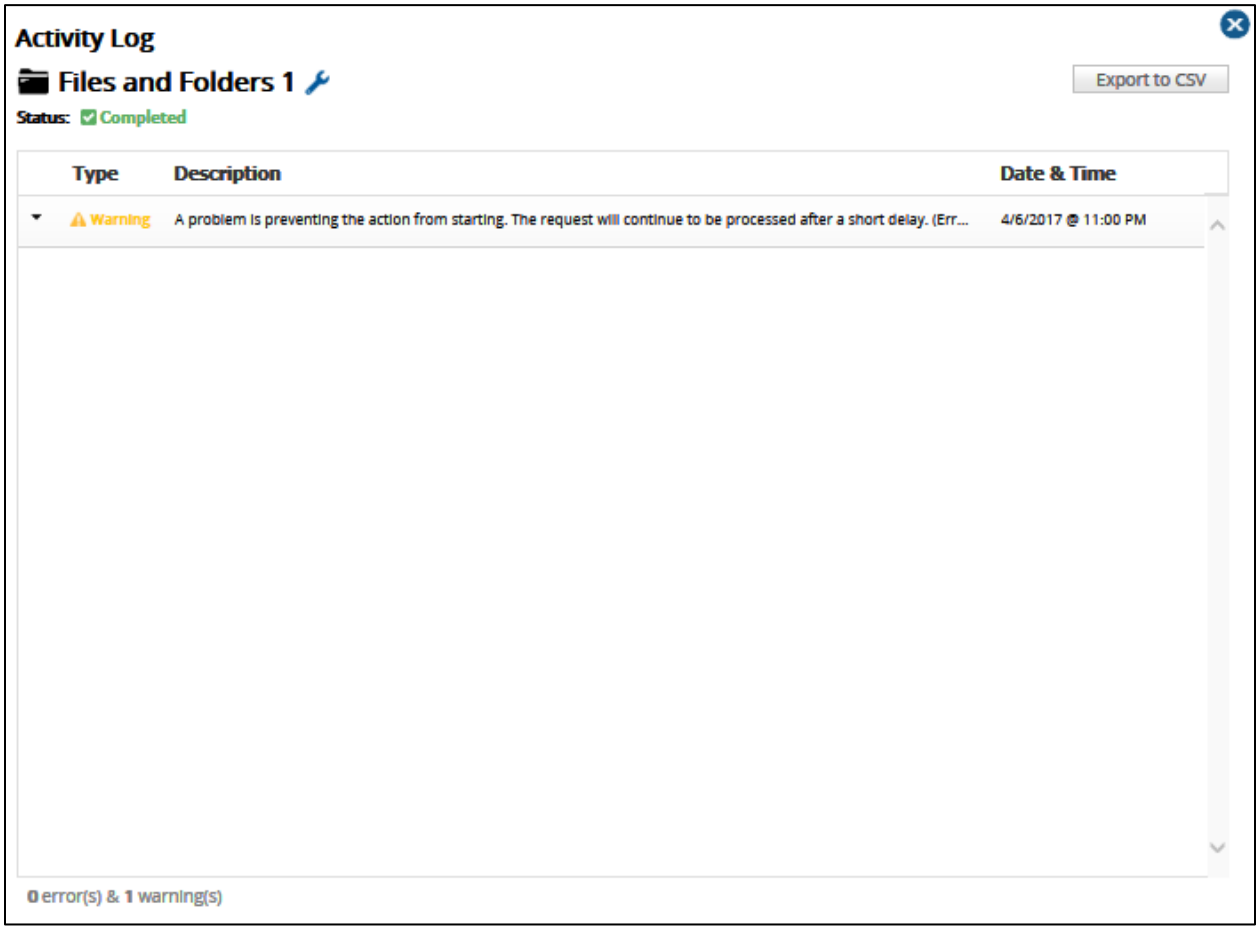
   The detailed list for each account with links to status logs and associated computers is displayed.



2. Click the link in the Reason column.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

The view log page is displayed.



3. In the log, you have the following options:

- View a summary of previous backups.
- Export to a CSV file by clicking the **Export to CSV** button at the lower right page.
- Edit the backup set by clicking the edit icon.

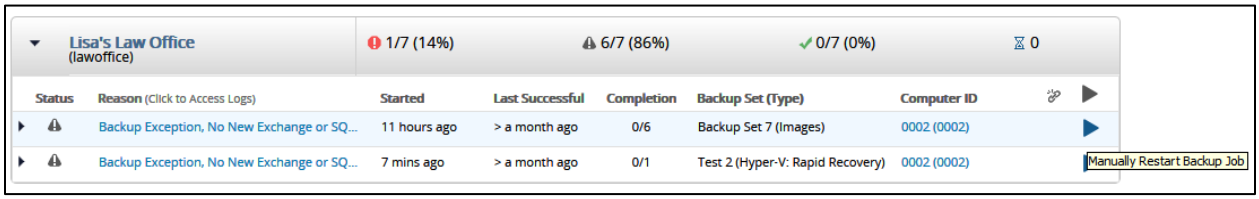
This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Running Backup Sets from the Home Dashboard

To run backup sets from the Home dashboard, perform the following steps.

1. Click the **Expand All** check box, and then click the **Apply** button.

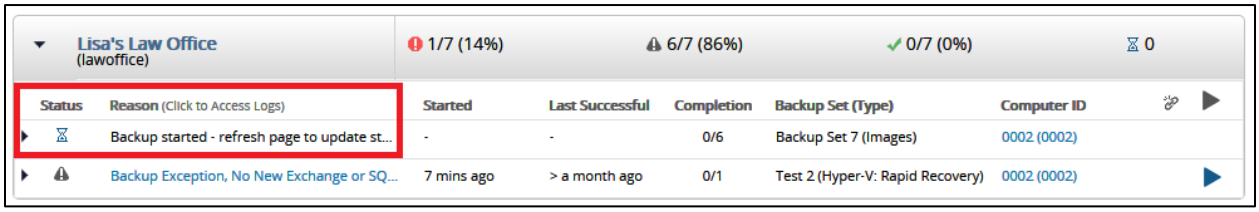
   The Backup Sets are displayed.



2. Select the run arrow to manually start a backup job.

   A new backup job is started.

   The Status and Reason columns display backup job information.



3. Refresh the page to display updated status.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Chapter 5. Backup Types, Templates, and Reports

This chapter provides an overview of the following software features:

- Backup Types
- Templates
- Reports

Backup Types

You can create the following types of backup sets:

- File and Folder
- Hyper-V Standard
- Hyper-V Rapid Recovery
- VMware Standard
- VMware QuickSpin
- Exchange Information Store
- Exchange Mailbox Level
- SQL Server
- System State
- Virtual Machine
- Physical Imaging Standard
- Physical Imaging Rapid Recovery

See the *ECHOplatform Backup and Restore Reference Guide* for details on how to create backups and restores for other backup types.

File and Folder Backup

This option lets you back up individual files and folders.

Hyper-V Standard & Hyper-V Rapid Recovery

Hyper-V VMs can be protected with Hyper-V Standard, which can be sent to the cloud, or Hyper-V Rapid Recovery, which can be recovered locally in minutes. Hyper-V Rapid Recovery supports performing object-level restores from protected VMs.

VMware Standard & VMware QuickSpin

You can back up VMware images using VMware Standard, which can be sent to the cloud, or QuickSpin, which lets you recover your VMware VMs locally in a matter of minutes.

Exchange Information Store

This option lets you back up an entire Exchange Information Store.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Exchange Mailbox Level

This option lets you back up individual Exchange mailboxes. This option is not recommended for full Exchange disaster recovery.

SQL Server

This option lets you back up SQL databases.

System State

This option lets you back up the computer's system state data.

Physical Imaging Standard & Physical Imaging Rapid Recovery

This option lets you back up physical machines as volume-level images.

Additionally, you can use Rapid Recovery to restore a failed system in minutes or object-level restore to recover individual files and folders from an image.

Imaging also supports Bare-Metal Recovery. See the *ECHOplatform Backup and Restore Reference Guide* for more information.

Templates

The Backup Software provides you with access to the following templates:

- System preferences template
- Software preferences template
- Email Notification template
- Overage Alert template

For detailed information on templates, refer to the *Backup and Restore Reference Guide.*

Reports

The Backup Software provides you with access to the following reports:

- Executive Summary Report
- User Access Report
- Backup Status Report
- Activity Log
- Plan Percentage Report
- Accounts History Report
- Account Snapshot Report
- No Recent Backup Report
- Storage Usage Over Time Report

For detailed information on reports, refer to the *Backup and Restore Reference Guide.*

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Chapter 6. **Barracuda Essentials**

Barracuda Essentials provides the following features:

- Protects against email-borne attacks
- Archives emails with policy-based retention and search capabilities
- Automates backup and recovery for emails, attachments, and files

Email-Borne Threat Protection

The Barracuda Email Security Service includes Advanced Threat Protection to help keep email-borne attacks outside your customers' networks and provides email continuity and data leakage protection.

Archiving for Compliance

Barracuda Cloud Email Archiving Service integrates with your email to create cloud-based, indexed archive that enables the following features:

Granular retention policies

Extensive search, auditing/permissions

Legal hold, and export to facilitate eDiscovery and retention

Litigation holds preserve email from tampering. Native and mobile apps provide intuitive interfaces that simplify search to ensure messages are found easily, even when email services are unavailable.

Real-Time Analysis

The Barracuda Essentials for Email Security platform provides real-time detection for dynamic threat analysis with 24x7 updates and protection.

Backed by Barracuda Central, your reports include over 170,000 active sites with threat intelligence across all potential vectors.

For more information about Barracuda Essentials refer to the *Barracuda Backup Services User Guide* or contact support@barracudamsp.com.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

[This page left intentionally blank.]

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Chapter 7. **Barracuda Appliances**

Barracuda appliances offer the following features:

- Fast and easy installation
- High Performance
- Other Deployment Options

Fast and Easy Installation

Most Barracuda appliances can be installed in minutes. Just plug the appliance into your network and set up your security policies or use the default appliance settings.

High Performance

Barracuda appliances are purpose-built for their intended function. This offers much faster and more consistent performance and better protection than all-in-one UTM servers. To further boost performance, all appliances are connected to the Barracuda Cloud. Resource-intensive tasks are automatically offloaded to the cloud to keep your network running fast and avoiding bottlenecks during peak workloads.

Other Deployment Options

Most appliances are also available as Virtual Machines. You can also host our appliances in the public cloud in Amazon Web Services and Microsoft Azure.

For more information about Barracuda appliances refer to the *Barracuda Backup Services User Guide* or contact support@barracudamsp.com.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

[This page left intentionally blank.]

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Chapter 8. Barracuda Content Shield

Barracuda Content Shield provides the following features:

- Robust DNS Filtering
- Real-time Threat Intelligence
- Centralized Management & Comprehensive Reporting
- Policy Enforcement

Robust DNS Filtering

By blocking endpoint communication to websites that host malicious content, DNS filtering provides protection from online threats such as:

- Viruses
- Malware
- Ransomware
- Phishing attacks
- Botnets

Barracuda Content Shield provides agentless DNS protection for all devices that sit behind your customers' router or firewall — which is critical as IoT devices become more common in today's workplaces. By enforcing policy at the DNS level, you can block access to the sites before that connection is made, preventing dangerous communication between endpoint and website.

Real-time Threat Intelligence

Content Shield leverages Barracuda's powerful threat intelligence network, which combines data collected from multiple sources with advanced analysis and research to provide comprehensive, timely, up-to-date protection.

Barracuda collects emails, domains, URLs, binaries and other threat data from tens of thousands of honeypots located in more than100 countries and an extensive web crawler network. This collection is supplemented by data contributions from more than 180,000 collection points across several types of organizations. This combination allows Barracuda to leverage threat data across multiple vectors and rapidly respond to modern, aggressive web-based attacks. For example, Content Shield benefits from malicious domain data that is gathered through email submissions from Barracuda Email Security customers.

Centralized Management & Comprehensive Reporting

Administrators are kept informed of the status of each of their customers and can implement centrally defined protection and content filtering rules for every location. The integrated reporting functionality issues instant alerts of malicious threats and provides customizable reports with comprehensive views of issues in your customers' environments.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Policy Enforcement

Content Shield provides visibility into customer web activity while enforcing access policies across all users and devices. With more than 90 URL categories, Content Shield does more than protect your customers from malicious websites; it also ensures that you're protecting their employees from accessing sites that would violate company policy, norms, and standards.

For more information about Barracuda Essentials refer to the *Barracuda Backup Services User Guide* or contact support@barracudamsp.com.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Chapter 9. Accessing Resources and Marketing Materials

Within the Management Portal, there are several types of resources and white label marketing materials available to you. You can access everything you need to help you start and manage your cloud backup and recovery solution.

These documents are in editable Microsoft Word and PowerPoint format, so you may update them with your own logo, company name, and product information. This packet is updated regularly with new pieces of collateral and fresh content, so remember to download a new copy every so often.

Check the Management Portal periodically to download the latest materials.

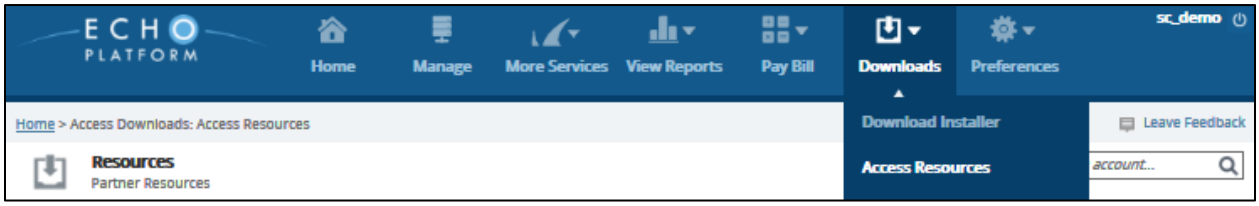
The following table lists the types of resources and white label marketing materials available to you within the Management Portal.

Material	Description
Release Notes	Guide to important product information.
Re-brandable Marketing Material in the Partner Toolkit (requires Registration/Login)	Contains several pieces of end-user-facing marketing collateral including white papers, brochures, email templates, a cold call script, and a PowerPoint presentation.
ECHOplatform Quick Start Partner Guide	Guide to getting started with our cloud backup and recovery solution.
Barracuda MSP Best Practices Partner Guide	Comprehensive guide to ECHOplatform best practices, including DR planning.
ECHOplatform Portal REST API Reference	Reference guide for use of the ECHOplatform portal REST API.
RMM Deployment Kit	Guide to deploy and monitor the backup solution using RMM tools.
Technology Whitepaper	Information on our solution and how it can help protect your clients' data.
ECHOplatform - Autotask Integration Guide	Details on how to get the most out of our Autotask Integration.
ECHOplatform - ConnectWise Integration Guide	Details on how to get the most out of our ConnectWise Integration.
BMR Media Creator	Download the BMR media creator for the pre-installation media required to perform a bare metal recovery.

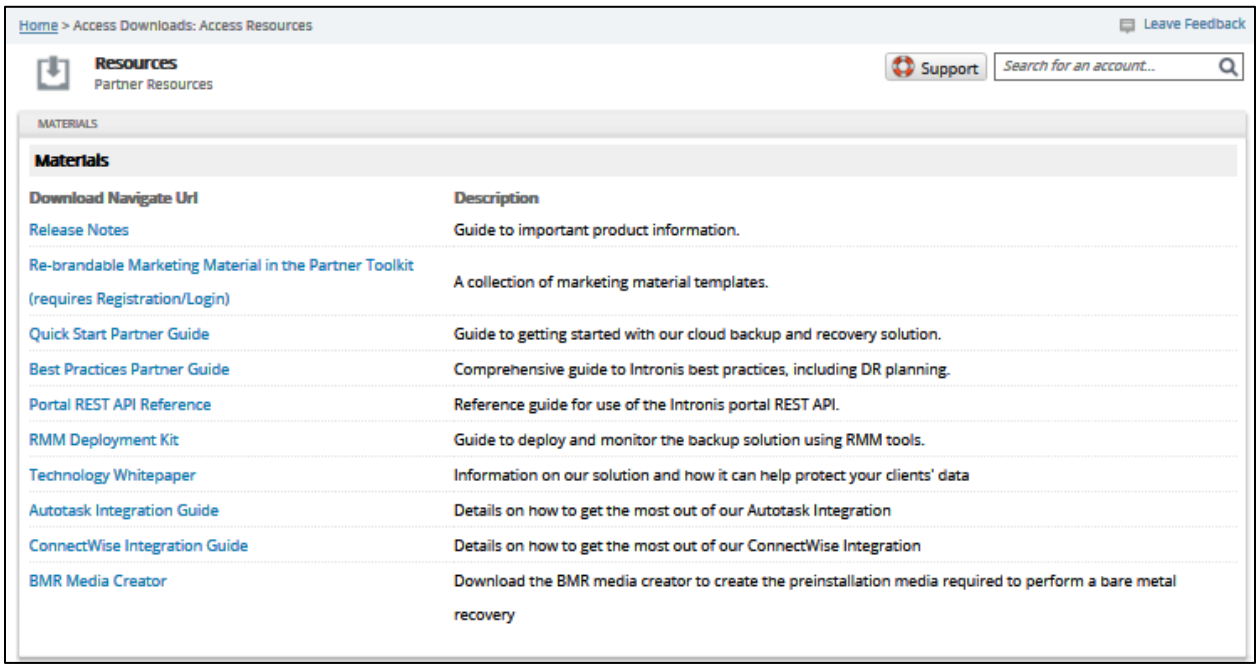
This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Accessing Marketing Materials

To access Barracuda marketing materials, at the ECHOplatform ribbon, click the **Downloads** tab, and then select **Access Resources**, as shown below.



The Resources page is displayed.



This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Chapter 10. Contacting Partner Support

This section includes the following topics:

- How and when to contact partner support
- Common things you can check
- Preparing for support

How and When to Contact Partner Support

Our current Partner Support hours are Monday – Friday 8 am – 9 pm EST.

Contact Partner Support as follows:

- Phone at 1-800-569-0155 option 1.
- Live chat from the website or management portal.
- Emailing support@barracudamsp.com.

During the weekends and holidays, coverage during our normal business hours is provided via email only. Before contacting our Partner Support Team, attempt level-one troubleshooting of the issue.

Common Things You Can Check

Here are some common things you can check.

- Access the logs through the management portal or on the local software.
- When a failed Backup notice is received, try to reproduce the issue or manually run a backup.
- Check the network and environmental variables that could cause a backup to fail.
    - Check Event Viewer for corresponding errors
    - VSS writers
    - Permissions
    - Connection/Firewall/Anti-Virus
- Check our Knowledge Base for relevant articles.

Preparing for Support

When you contact our Partner Support Team, be ready to provide the following:

- The user name of the client with the issue and the computer.
- Any warnings, exceptions, or error messages.

If an existing case, Barracuda can access that open case to find all relevant information.

Depending on the backup solution, a remote connection to the machine may be necessary.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

[This page left intentionally blank.]

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Glossary

The following table provides definitions for some of the terms used in this guide for cloud computing restore and backup functions.

Term	Definition
4k Sector	A 4k sector size rather than the traditional 512-byte sector used on legacy disk drives is larger and allows for higher capacity storage as well as the potential for improved performance.
Archive Rules	Used to control the number of revisions that are stored, by removing unneeded revisions indicated in the rule. When the backup set is run, each rule is applied in the order listed within the set's revision rule list. The Standard Rules Types are: • Disk Usage • Number of Revisions • Disk Usage • Date Range
Asynchronous	An attribute of a before and after action. If designated for a before action, the action starts at the start of a backup set but may not completely finish before the backup set begins. If designated for an after action, the backup set may not completely finish before the action is run.
Backup Set	A selected set of data and folders that are backed up when either run, manually, or automatically based on an associated schedule. Backup sets can include files and folders, VMware and Hyper-V virtual machines (VMs), an image of one or more physical drives, or SQL and Exchange data.
Checkpoint	A snapshot of a Hyper-V virtual machine. Differs from a VSS Snapshot.
Cloud Archive	Data that no longer needs to be accessed on a regular basis is maintained and backed up remotely by a cloud storage service provider.
Cloud Application	A software application that is never installed on a local machine and is always accessed over the Internet.
Cloud Provider	A company that provides cloud-based platform, infrastructure, application, or storage services to other organizations and/or individuals.
Computer ID	A unique four-digit code used to keep track of multiple subaccounts that are associated with a single main account. The first computer you install Online Backup Solution.com on has the computer ID 0000. Subsequent subaccounts have the next sequential computer ID of 0001, 0002, and so on.
Cluster	A group of hosts that are linked providing high availability.
Differencing Disk	A virtual hard disk (VHD) that stores changes made to another VHD or to the guest operating system. The purpose of differencing disks is to maintain information about any changes made so changes can be reversed.
Differential Backup	A type of backup associated with SQL Server, for File and Folder, VMware Standard, and Hyper-V Standard backup sets. After the initial full backup is completed, a differential backup backups only data that has changed since the prior full backup.
FAT	File allocation table. A file system developed mostly for hard drives.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Term	Definition
File Catalog	A list of all of data, and revisions that are contained within backup set. The catalog is transmitted to the backup servers with every backup.
GPT	Globally unique identifier (GUID) partition table. A standard for the layout of the partition table on a physical hard disk using globally unique identifiers.
Hypervisor	A platform that allows multiple operating systems to run on a host computer at the same time.
Hyper-V	A Microsoft virtualization solution. Formerly known as Windows Server Virtualization, it can create virtual machines on x86-64 systems.
Hyper-V Manager	The primary GUI for Microsoft's Hyper-V through which virtual machines are managed.
Image-level (volume-level) Backup	A process that backs up an entire storage volume.
Incremental Backup	Backs up only the data changed since the last backup.
IntelliBlox	A proprietary technology that uploads only the changed blocks of a file. At your next backup, the data is scanned and any changes at the block level are detected; only these changes are uploaded.
Local Backup	Any backup where the storage medium is kept nearby.
Local Storage	The on-site destination for Image and Hyper-V Rapid Recovery backups. This location should be directly attached or network storage. The data stored for these backups in local storage is unencrypted and stored in reverse-incremental format.
Local Vault	Keeps a mirror copy of backup data stored on Barracuda and local servers.
MBR	Master boot record. The first sector on a hard drive occupied by code necessary to start the operating system startup process.
MSP	Managed Service Provider. Provides delivery and management of a variety of services that include but are not limited to network-based services (online backup), applications, and equipment.
NTFS	New technologies file system. The standard file system of all supported Microsoft operating systems.
Object-level Recovery	A method of recovery that allows recovery of individual files and folders from an image backup. This option is available for Imaging and Hyper-V Rapid Recovery backups.
Quiescing	A process of bringing the data on a disk of a physical or virtual computer into a state suitable for backups.
Rapid Recovery	A recovery option for Hyper-V Rapid Recovery and Imaging that allows a VM to be created and/or run directly from the backup data in local storage. Because this option does not require a network copy, it is very fast to complete, especially for the most recent revision of a protected machine.
Restore	The process of retrieving backed up data. You can restore your data to their original locations, or to a different folder.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.

Term	Definition
Reverse Incremental Backup	A methodology used in Imaging, Hyper-V Rapid Recovery, and VMware QuickSpin backups. Allows only the changes to be backed up while the most recent state of the protected system is saved as the base revision. Allows for a more stable revision chain and the fastest recoveries of the most recent state.
Revision	The state of data at a particular point of time.
Revision Rules	See *Archive Rules*.
Snapshot	A reproduction of the virtual machine as it was when you took the snapshot, including the state of the data on all the virtual machine's disks and the virtual machine's power state (on, off, or suspended).
Synchronous	An attribute of a Before and After action. If designated for a Before action, the action completely finishes before the backup set begins. If designated for an After action, the backup set completely finishes, before the action is run.
UNC	Uniform Naming Convention. Specifies a well-formed syntax to describe the location of a network resource, such as a shared file, directory, or printer.
vCenter Server	The management tool used to administer the various available servers in the enterprise. These servers can be ESX or ESXi, each tied to a physical server and able to host a number of virtual machines.
vCenter Server Database	A persistent storage area for maintaining the status of each virtual machine and user that is managed in the vCenter Server environment. Located on the same machine as vCenter Server.
vMotion	The live migration of VMs across hosts in a cluster without having to power them down.
Volume Shadow Copy	A copy of a volume (a VHD/VHDX file) created by a VSS writer that enables files to be backed up even if they reopened by another process.
VMware ESX/ESXi	VMware hypervisors that are installed on bare metal and run on the host computer.
VMware vSphere	The name of the VMware virtualization system.
VMware Virtual Machine Console	An interface that provides access to one or more virtual machines on the local host or on a remote host running vCenter Server.
VSS	Volume Shadow Copy Service. A Windows service for capturing and creating snapshots called shadow copies.
VSS Snapshot	See Volume Shadow Copy.

This document constitutes proprietary and confidential information of Barracuda Networks, Inc. This document may not be disclosed, used or duplicated, in whole or in part without the prior written consent of Barracuda Networks, Inc.