

# Connected Backup

Software Version 9.0.3

## Administering Mac Agents



Document Release Date: October 2020  
Software Release Date: October 2020

## Legal notices

### Copyright notice

© Copyright 2016-2020 Micro Focus or one of its affiliates.

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

## Documentation updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

You can check for more recent versions of a document through the [MySupport portal](#). Many areas of the portal, including the one for documentation, require you to sign in with a Software Passport. If you need a Passport, you can create one when prompted to sign in.

Additionally, if you subscribe to the appropriate product support service, you will receive new or updated editions of documentation. Contact your Micro Focus sales representative for details.

## Support

Visit the [MySupport portal](#) to access contact information and details about the products, services, and support that Micro Focus offers.

This portal also provides customer self-solve capabilities. It gives you a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the MySupport portal to:

- Search for knowledge documents of interest
- Access product documentation
- View software vulnerability alerts
- Enter into discussions with other software customers
- Download software patches
- Manage software licenses, downloads, and support contracts
- Submit and track service requests
- Contact customer support
- View information about all services that Support offers

Many areas of the portal require you to sign in with a Software Passport. If you need a Passport, you can create one when prompted to sign in. To learn about the different access levels the portal uses, see the [Access Levels descriptions](#).

# Contents

<b>Chapter 1: Agent overview</b> .....	<b>9</b>
The role of the Agent .....	9
Support Center .....	9
Support Center interface .....	10
Nodes .....	10
Communities and subcommunities .....	11
Technicians .....	11
Communities .....	12
Agent configurations .....	12
Rules .....	12
Reports .....	12
Inheritance of Support Center objects .....	12
Duplicate object names .....	13
Open Support Center .....	13
Internet Explorer preparation for FDCC environments .....	13
SCBrowserUtils.dll Signed ActiveX Control .....	14
Adobe SVG Viewer NPSVG3.dll ActiveX Control .....	14
Agent accounts .....	15
Agent connections to Data Centers .....	15
Agent connection properties .....	15
Proxy servers .....	16
Connect through a SOCKS proxy server .....	16
Connect through a Non-SOCKS proxy server .....	16
Connect Through firewalls .....	16
Network interruptions .....	17
Agent deployment tasks .....	17
Create communities and subcommunities .....	17
Specify properties and settings .....	17
Distribute the Agent software .....	18
Register and install the Agent .....	19
 <b>Chapter 2: Set up communities and accounts</b> .....	 <b>20</b>
Communities .....	20
Communities in Support Center .....	20
The Default community .....	20
New communities .....	21
Subcommunities .....	21
Create subcommunities .....	22

- Agent accounts in subcommunities ..... 22
- Disable registration in communities ..... 22
- Manage accounts ..... 23
  - View an account number ..... 23
  - View Account Information ..... 24
  - Change account status ..... 24
- Managing general account functions ..... 26
  - Reserve accounts ..... 26
  - Change the primary server for an account ..... 26
  - Change an agent configuration ..... 27
  - Send informational messages to Agents ..... 27
  - Display backup messages ..... 28
  - Use the Agent Dock icon ..... 29
- Agent Security ..... 29
- Technician accounts ..... 30
- Licenses for Agent accounts ..... 31
  - How licenses affect the Support Center display ..... 31
  - License inheritance and allocation ..... 31
  - Used and unused licenses ..... 32
  - Licensed features for communities ..... 32
    - Feature state inheritance ..... 32
  - Expired licenses ..... 33
  - Effect of licenses on accounts and communities ..... 33
- Manage licenses and licensed features ..... 34
  - License allocation examples ..... 34
    - Inherited licences ..... 34
    - Allocated licenses ..... 35
    - Licenses allocated to subcommunities ..... 36
  - Allocate licenses ..... 37
  - Enable or disable licensed features ..... 38
- Apply bandwidth throttling during Agent backups ..... 38
- Chapter 3: Create Agent configurations ..... 40**
  - About Agent configurations ..... 40
  - Configuration components ..... 40
    - Profile and Website settings ..... 41
    - Agent versions ..... 41
    - Agent settings ..... 41
    - Agent rule sets ..... 41
    - Default Agent configuration ..... 42
  - Create an Agent configuration ..... 42
    - Allocate licenses ..... 43

Create an Agent version .....	43
Create Agent settings .....	44
Create Profile and Website settings .....	44
Create an Agent rule set .....	44
Create the Agent configuration .....	45
<b>Chapter 4: Create Agent rule sets .....</b>	<b>46</b>
Rule types .....	46
The rule matching process .....	46
Rule logic .....	47
Rule precedence .....	48
Rule categories .....	49
Create rules .....	50
Best practices for creating rules .....	50
Use rule sets .....	50
Rules page .....	51
Use the Agent Rules wizard .....	52
<b>Chapter 5: Agent security features .....</b>	<b>54</b>
Encryption .....	54
Access Control List management .....	54
Unauthorized access prevention .....	54
Security certificates .....	55
Password protection for retrieval .....	55
Prevent access to files on a lost or stolen computer .....	55
<b>Chapter 6: Brand product components .....</b>	<b>57</b>
Branding overview .....	57
Agent branding options .....	57
Support Center branding options .....	58
Account Management Website branding options .....	59
Branding options for Agents .....	59
Branding options in the Installer window .....	60
Branding options in the Agent User interface window .....	60
Brand the About window .....	61
Branding options for Support Center .....	62
Inherited branding .....	62
Brand the Support Center sign in page .....	62
Brand the Change Password Dialog Box .....	62
Brand the Support Center Interface .....	63
Branding Options for the Account Management Website .....	63

Brand product components .....	64
Requirements for Agent graphics .....	64
Requirements for Support Center graphics .....	64
Requirements for Account Management Website Graphics .....	64
Technician account requirements .....	65
Start the branding process .....	65
Gain access to branding communities .....	66
<b>Chapter 7: Deploy Account Management Website .....</b>	<b>67</b>
Overview of Account Management Website .....	67
Deploy Account Management Website .....	68
Ensure security .....	68
Edit the Terms of Use and Privacy pages .....	68
Set the Default URL for Registration and Sign In .....	69
Set up user access .....	69
Set up technician access .....	69
Account credentials .....	70
Account credential management .....	70
Account Management Website Interface .....	70
Welcome page .....	71
Registration page .....	71
Sign In page .....	72
Summary page .....	73
MyRoam .....	74
License and permission requirements .....	75
MyRoam installation .....	75
Enable MyRoam .....	75
Enable MyRoam for individual accounts .....	76
<b>Chapter 8: Agent interfaces .....</b>	<b>77</b>
Overview of the Agent interfaces .....	77
Agent Startup wizard .....	78
Startup Wizard main pages .....	78
Startup Wizard – Create Account option .....	79
Startup Wizard – Recover Account Option .....	80
Agent User Interface .....	80
Agent Main window .....	81
Agent user interface components .....	81
Use the Agent user interface .....	82
Agent command-line interface .....	83
Use the UpdateProfile Command .....	83

<b>Chapter 9: File backup</b> .....	<b>85</b>
The backup process .....	85
Disk scan .....	85
File analysis .....	86
Modified file identification .....	87
File preparation .....	87
Connection to the Data Center .....	87
Transmission of files .....	87
Record of backup results .....	88
Outlook for Mac support .....	88
Back up encrypted files, metadata, and attributes .....	89
Backup settings .....	90
Use the Agent user interface to back up files .....	92
Backup Set tab .....	92
Summary tab .....	92
You can use the Summary tab to start a backup and view History details about the last backup that the Agent performed. ....	92
Backup monitoring .....	92
Back up files using the Backup command .....	93
Backup command syntax .....	93
Backup command options .....	94
Backup command example .....	94
<b>Chapter 10: File retrieval</b> .....	<b>95</b>
The Retrieval Process .....	95
File repackaging .....	95
E-mail notification .....	95
Support for encrypted files, metadata, and attributes .....	96
Retrieval of sparse files .....	96
Retrieval of resource forks .....	96
Retrieval of open files .....	96
Retrieve files using the Agent user interface .....	96
Retrieve tab .....	96
Retrieve permissions .....	97
File selection .....	97
Destination options .....	98
File name conflict options .....	98
Retrieve files using the Retrieve command .....	98
Retrieve command syntax .....	99
Retrieve command options .....	99
Examples of how to use the Retrieve command .....	102
Retrieve a single file .....	102

- Retrieve a single file and specify date and time ..... 102
- Specify a retrieve location ..... 102
- Retrieve files only in a top-level folder ..... 102
- Retrieve all files in a backup set ..... 103
- Retrieve data using MyRoam ..... 103
  - The MyRoam retrieval process ..... 103
  - Files that you cannot retrieve ..... 104
  - Select files for retrieval ..... 104
  - Retrieve files ..... 106
- Chapter 11: Agent history and reports ..... 108**
  - Agent history ..... 108
    - View Agent history in the Agent interface ..... 108
    - Viewing Agent History in Support Center ..... 110
  - Support Center reports ..... 111
    - Default reports ..... 112
    - Report components ..... 113
    - Create report templates ..... 114
    - Generate and view reports ..... 114
    - View charts ..... 114
    - Save report results in XML ..... 115
    - Create account groups ..... 115
  - Use the Agent Protocol Session log ..... 115
    - Enable the Agent Protocol Session log ..... 115
- Chapter 12: Troubleshooting ..... 118**
  - Scenario: Mac backups might complete with errors on macOS Mojave or later version(s) .... 118
    - Authorizing Connected Backup Mac Agent on single macOS Mojave or later version(s) .. 118
    - Authorizing Connected Backup Mac agent in enterprise environments ..... 119
- Index ..... 120**
- Send documentation feedback ..... 125**

# Chapter 1: Agent overview

This chapter explains the role of the Agent, the components that comprise the Agent, and how to deploy the Agent.

- [The role of the Agent, below](#)
- [Support Center, below](#)
- [Agent accounts, on page 15](#)
- [Agent connections to Data Centers, on page 15](#)
- [Agent deployment tasks, on page 17](#)

## The role of the Agent

The Agent is a software that you install and configure on client computers that require signed binaries. You use the Agent to back up files on the client computers and to retrieve files that you previously backed up.

Every Agent has an account in the Data Center. The account contains information about the Agent configuration.

The Agent sends files to the Data Center for backup. To perform a backup, the Agent scans the hard drives of the computer on which it resides for files that require backup. Next, the Agent contacts the Data Center to initiate a backup session. The Agent prepares the files for backup and notifies the Data Center if users have deleted previously backed-up files since the last backup session.

To retrieve or restore files, the Agent requests the files from the Data Center, then downloads or restores the files to the client computer.

The Agent initiates communication with the Data Center. The Data Center cannot contact an Agent independently.

### **IMPORTANT:**

The Agent does not support multi-user environments. Although you can install the Agent on a computer that hosts more than one user account, you can only associate one user account with the Agent. Additionally, more than one user account on a computer that hosts the Agent can cause problems during file retrieval and backups.

## Support Center

Support Center is a Web-based management application that technicians use to manage Agent configurations and accounts. You can use Support Center from any computer with a supported browser and a network or Internet connection. For the list of supported browsers, refer to the *Micro Focus Connected Backup Requirements Matrix*.

Use Support Center to manage the following information:

- Technician accounts
- Communities and Agent accounts
- Agent settings
- Agent profile and Web site settings
- Agent versions
- Agent rules
- Reports

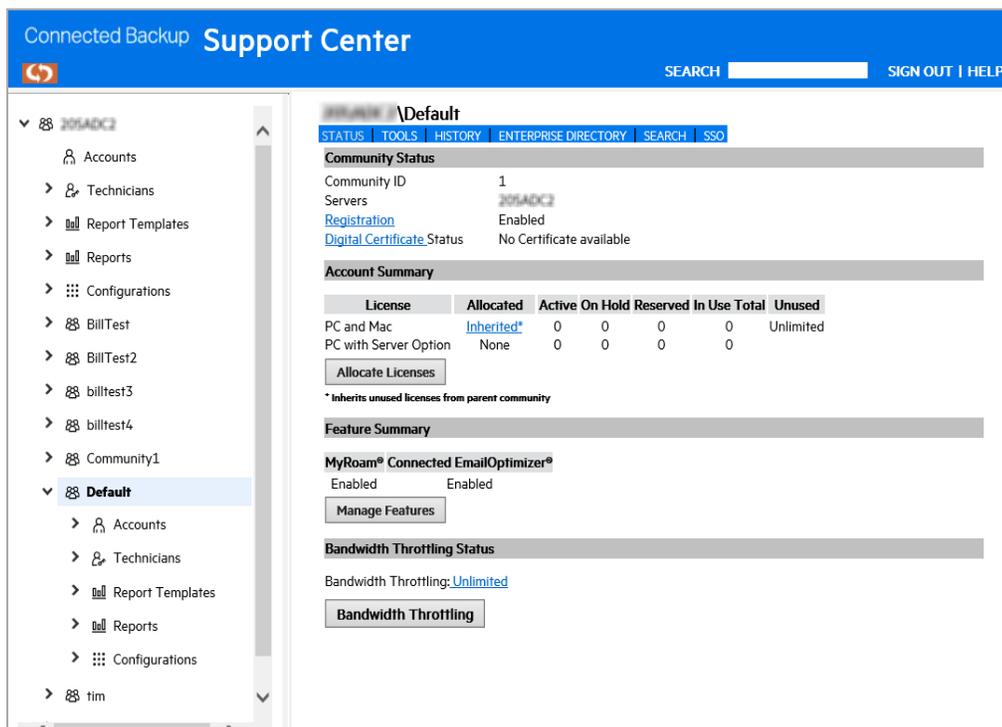
## Support Center interface

The Support Center interface consists of two panes.

The left pane displays a hierarchical tree that represents the organization of Agent accounts on your Data Center (if you host your Data Center) and your communities.

The right pane displays information relevant to the node that you select in the left pane.

The following figure shows the Support Center interface.



## Nodes

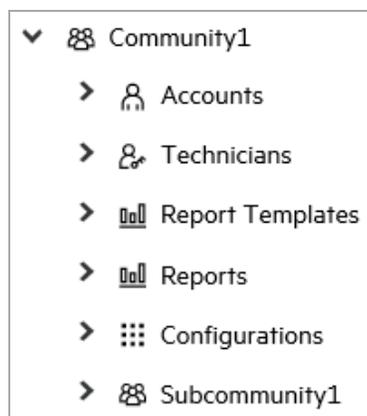
The following table describes the major nodes and subnodes in the Support Center interface:

Item	Description
Top-level node	Expand the top-level node to view the nodes and subnodes in the tree. The top-level node uses the Data Center server name and is the top-level community.
Accounts	Find and display information about the user accounts in your Data Center.
Technicians	Create and modify logon accounts for technicians who use Support Center.
Report Templates	Create templates to generate reports that track account use and other statistics.
Reports	Display report results after you use the Report Templates node to generate a report.
Legacy PC Configurations	Use the Configuration Summary page to create, edit, and view version 7.x or earlier PC Agent configurations.
Configurations	Create, edit, and view Profile and Website settings, Mac Agent configurations and version 8.0 or later PC Agent configurations.

## Communities and subcommunities

You can create communities and subcommunities to organize accounts. A community appears as a node below the top-level node. A subcommunity appears as a subnode below a community node.

The following figure shows **Subcommunity 1** under **Community 1**.



Each community and subcommunity has its own **Accounts**, **Technicians**, **Configurations**, **Report Templates**, and **Reports** nodes.

## Technicians

Technicians include Data Center administrators, Information Technology individuals, Technical Support individuals, and others who support your user community. To use Support Center to perform administrative tasks, a technician must create a technician account. A technician can give the account as many permissions as necessary, and can delegate different tasks to supporting personnel.

For more information, see [Set up communities and accounts, on page 20](#).

## Communities

A community is a group of accounts with a common element. You can create communities based on department, office location, Agent configuration, or any category that helps you manage your accounts efficiently.

For more information, see [Set up communities and accounts, on page 20](#).

## Agent configurations

An Agent configuration is a set of settings and features that you want to apply to one or more Agents. You can create configurations to meet enterprise needs such as a backup schedule, security, and features. After you create an Agent configuration, users can go to the Account Management Website to download an Agent Setup file that uses the configuration. The Agent Setup applies the configuration settings when users employ it to install an Agent, recover an Agent account, or upgrade an Agent. Alternatively, you can install the Agent Setup file on client computers.

For more information, see [Create Agent configurations, on page 40](#).

## Rules

The Agent uses rules to determine which files to back up. When you build an Agent configuration, you must assign a rule set.

For more information, see [Create Agent rule sets, on page 46](#).

## Reports

You can use Support Center to create and run reports about the use and status of accounts. You can run reports once or regularly. You can configure reports to include charts. You can save reports in XML format.

For more information, see [Agent history and reports, on page 108](#).

## Inheritance of Support Center objects

A Support Center object can be an Agent configuration, a report template, or a technician account. The inheritance feature lets you use top-level objects in all subcommunities. In other words, when you create objects in a community, the objects apply to the community and its subcommunities.

Support Center displays inherited objects in the left pane in regular text. It displays objects that you create in the community in bold text. You cannot edit the inherited objects. However, you can edit the objects you create.

## Duplicate object names

Because communities contain inherited objects and objects that you create, a community can contain multiple objects that have the same name.

For example, if a parent community has a configuration named Finance, its subcommunity inherits that configuration. You also can create a new configuration in the subcommunity named Finance. Support Center displays the inherited community in regular text and the configuration you create in **bold** text.

As a best practice, use unique names or unique descriptions for all objects you create.

## Open Support Center

You can open Support Center from any computer with Internet Explorer 6.0 or later and a network or Internet connection.

Open Support Center in the following ways:

- **Subscription users.** Open a Web browser, and then enter the URL that the enterprise that hosts the Data Center provides.
- **Licensed users.** Open a Web browser, and then enter a URL in one of the formats described in the following table:

SSL Status	Using DNS or WINS to store server names	Not using DNS or WINS to store server names
SSL is enabled	<code>https://server_name/supportcenter/</code> where <code>server_name</code> is the name of the server that hosts Support Center	<code>https://ip_address/supportcenter/</code> where <code>ip_address</code> is the IP address of the Support Center server
SSL is not enabled	<code>http://server_name/supportcenter/</code> where <code>server_name</code> is the name of the server that hosts Support Center	<code>http://ip_address/supportcenter/</code> where <code>ip_address</code> is the IP address of the Support Center server

## Internet Explorer preparation for FDCC environments

You must install the following applications in a Federal Desktop Core Configuration (FDCC) environment to allow Internet Explorer access to Support Center in order to manage your Connected Backup accounts:

- `SCBrowserUtils.dll` signed ActiveX control
- Adobe SVG viewer `NPSVG3.dll` ActiveX control

These applications require administrative rights to install.

## SCBrowserUtils.dll Signed ActiveX Control

Support Center uses the `SCBrowserUtils.dll` ActiveX control for the following functions:

- Downloading Agent Setup files
- Uploading Agent File Sets
- Uploading Branding-related files
- Uploading MSI certificates
- Downloading report XML file results
- Running the ACE utility to update Legacy Agent configurations

### To install the application

1. Use Internet Explorer to log in to the Support Center as a technician.
2. Navigate to an Agent configuration page to download an Agent Setup file.
3. During the page display, Internet Explorer prompts the user to install the `SCBrowserUtils.dll` ActiveX control.
4. Click **Install**.

Internet Explorer installs the control. Once the **Download** button is selectable, the control is installed.

#### **NOTE:**

##### **In Internet Explorer 8, to enable the ActiveX control**

- a. In Internet Explorer, select **Tools > Manage Add-ons**.
- b. In the Manage Add-ons window, right-click **BrowserUtility Class**, and then click **More Information**.
- c. In the More Information window, click **Allow on all sites**, and then click **Close**.
- d. Close the Manage Add-ons window and return to Internet Explorer.

## Adobe SVG Viewer NPSVG3.dll ActiveX Control

Support Center uses the Adobe SVG viewer ActiveX control to display graphical report results.

### To install the application

1. Download the installation file for the control from <http://www.adobe.com/devnet/svg/adobe-svg-viewer-download-area.html>.
2. Install the control by running the setup file and following the on-screen instructions.

## Agent accounts

Each deployed Agent has an account in the Data Center. Each account has a unique 10-digit number that identifies it. The Data Center uses this account number to label and organize all data that it backs up from the client. To view the account number, search for an account in Support Center. Record this number in case you need to reinstall the account.

As a technician, you can use Support Center to complete the following tasks:

- Change the account status.
- Manage account features.
- Manage security settings.
- Create and change Agent configurations.

As a user with native Connected Backup account credentials, you can use the Account Management Website (AMWS) to perform the following tasks:

- Change your password.
- Update your profile (e-mail address, address, and telephone number).

However, if your account is mapped to an enterprise directory or a single sign-on account, you cannot use AMWS to change your profile.

For more information about how to manage accounts, see [Manage accounts, on page 23](#).

## Agent connections to Data Centers

To connect to the Data Center, the Agent can use any Transmission Control Protocol/Internet Protocol (TCP/IP) connection, including local area networks (LANs) and wide area networks (WANs).

The amount of network traffic that Agents generate depends on the following conditions:

- Number of Agents that you deploy
- File backup rules
- Agent backup schedules relative to your network peak and off-peak hours of use for your network

## Agent connection properties

To connect to the Data Center, the Agent uses the DNS name or IP address of the Data Center server. In a mirrored configuration, you can designate which of two Data Center servers the Agent contacts as the primary server.

The Data Center replicates data from one server to the other. If the primary server is busy, the Agent connects to the secondary server to back up files and retrieve files.

When you run the Data Center setup, you can configure which Data Center server acts as the primary server. You can designate different servers as the primary server for different communities. For example, if you manage a mirrored configuration and have six distinct communities, you can designate

Server 1 as the primary server for Communities A, B, and C. You then can designate Server 2 as the primary server for communities D, E, and F. When you designate different servers for different communities, each server shares the volume of Agent transactions.

## Proxy servers

If the client computer and the Data Center reside on different sides of a proxy server, configure the Agent to connect to the Data Center through the proxy server.

The Agent can connect through the following proxy servers:

- SOCKS proxy server
- Non-SOCKS proxy server
- Software firewall

You configure the proxy server settings in Support Center. For more information, refer to Support Center Help.

### Connect through a SOCKS proxy server

When you use a SOCKS proxy server, all connections to the Data Center first require a connection to the SOCKS server. The server then uses the IP/Port information in the Agent configuration to connect to the Data Center.

To configure an Agent to connect to the Data Center through a SOCKS proxy server, use Support Center to edit the proxy server settings. Specify the IP address and port number for the proxy server. The Agent uses the SOCKS protocol to tell the proxy server the IP address and port number (16384) of the Data Center.

If you use SOCKS, do not reconfigure your proxy server. For more information about how to configure Agent proxy server settings, refer to Support Center Help.

### Connect through a Non-SOCKS proxy server

If your enterprise uses a non-SOCKS-compliant proxy server, configure the Agent and your proxy server to communicate with the Data Center. You configure the Agent proxy server information to map the Data Center IP address to the IP address of the proxy server, and you specify the port on which to connect to the proxy server. You can use domain names instead of IP addresses when you specify the Data Center and proxy server mapping. If you use a mirrored pair, designate this mapping for both the primary and secondary servers.

The Agent uses the mapping to connect to the IP address of the appropriate proxy server (using the appropriate port) instead of connecting directly to the Data Center server. The firewall then routes the connection to the Data Center that resides behind the proxy server.

### Connect Through firewalls

The Mac Agent supports only the OS X built-in firewall.

## Network interruptions

If the initial attempt to connect to a stand-alone Data Center server fails, the Agent records the failure in the Agent History. In a mirrored environment, if an Agent cannot establish a network connection to its primary server, the Agent attempts to connect to the secondary server. If the Agent connects to its secondary server, it proceeds as normal and completes its task. If the Agent cannot connect to its secondary server, it records the failed attempt in the Agent History.

If an interruption in the network connection occurs or the connection fails during a backup or retrieval, the Agent attempts to reconnect and finish the operation after it waits for a predefined period of time. After the wait period, the Agent attempts to reconnect to the Data Center server. The Agent does not attempt to connect to a different Data Center server to continue an aborted backup or retrieval. When the Agent reconnects, it starts at the beginning of the last file it worked on before the connection failed.

## Agent deployment tasks

You begin a first-time Agent deployment by logically grouping your user accounts into communities. You then define Agent configurations that have appropriate permissions and features for each community. You can have several different Agent configurations that you can assign to accounts and communities individually.

After you create or modify an Agent, you can download the Agent Setup program to users' computers for registration and installation.

## Create communities and subcommunities

You can configure multiple Agent configurations, each with different properties, to suit the needs of different groups in your enterprise. Before you create new Agent configurations, consider the different groups in your enterprise and determine which Agent features benefit each group.

Use Support Center to create subcommunities based on factors such as department, geographical location, or job function. After you create a subcommunity, you can move an Agent configuration to that subcommunity, or create a new Agent configuration with properties that meet the requirements of the subcommunity.

For more information, see [Set up communities and accounts, on page 20](#).

## Specify properties and settings

The **Configurations** node in Support Center contains the following types of Agent configurations:

- **PC Configurations.** PC Agent configurations.
- **Mac Configurations.** Mac Agent configurations.

Support Center can contain the following Legacy Agent configuration:

- **Legacy PC Configurations.** Version 7.x PC Agent configurations

To define an Agent configuration, you must define the following components:

- **Agent Versions.** Determines the software version of the Agent and the language.
- **Agent Settings.** Determines the settings and features available to users.
- **Agent Rule Sets.** Determines the files included and excluded for backup.
- **Profile and Website Settings.** Determines the features that users can gain access to through the Account Management Website. The Account Management Website lets users register accounts, download Agent software, and manage their accounts.

For more information about Agent settings, versions, and rules, see [Create Agent configurations](#), on page 40.

## Distribute the Agent software

After you define the Agent features during configuration, Support Center creates an Agent Setup program (`AgentSetup.pkg`) that installs the Agent software on a client computer. The Agent Setup program is in the `AgentSetup.zip` file.

To distribute the file, use the following methods:

- **Account Management Website.** Users log on to this Web site to register accounts and download the Agent Setup program. You can use the Account Management Website to distribute only files customized for one user. If you use this method to distribute the files to other users, the backup process does not work correctly. All users must download their own file from the Account Management Website. For more information, refer to *Installing Mac Agents*.
- **Support Center download.** You can download the Agent Setup program from Support Center and distribute a generic Agent Setup file to users so that they can install the Agent themselves. For more information, refer to *Installing Mac Agents*.

**NOTE:** From 9.0.2 onwards, the packaging structure has changed as follows:

1. The following are the Agent Setup files when downloaded using Support Center:
  - a. `AgentSetup.pkg`
  - b. `AgentSetup.mpkg`
  - c. Resources
  - d. Install
2. The following are the Agent Setup files when downloaded using Account Management Website:
  - a. `AgentSetup.pkg`
  - b. Resources
  - c. Install

**Do not delete or replace any setup files. Make sure to run `AgentSetup.pkg` instead of earlier preferred `AgentSetup.mpkg` when you want to install Mac Agent.**

**NOTE:** From 9.0.2 onwards, the `install.exe` will be outside the `AgentSetup.pkg` or `AgentSetup.mpkg`.

- **Disk image distribution.** You can install an Agent on a computer and then create a disk image to clone to other computers. For more information, refer to *Installing Mac Agents*.
- **Hands-free installation.** You can download the Agent Setup file from Support Center and use the installation command-line interface to install the Agent on multiple computers simultaneously without user participation. For more information, refer to *Installing Mac Agents*.

## Register and install the Agent

When you register an Agent, the Data Center establishes an account for the Agent. The account identifies the Agent client computer to the Data Center server. An account number in the Data Center represents the client computer and the files on that computer.

Installation and registration occur in one of the following ways:

- After a user logs on to Account Management Website (AMWS) and enters profile information, AMWS communicates with the Data Center to register a new account. Each user must register on the Account Management Website individually to get an Agent Setup program file that is particular to the user's account. After the user registers the Agent, the user downloads the Agent Setup program and installs the Agent. The Agent Setup program (`AgentSetup.pkg`) is contained in the `AgentSetup.zip` file.
- After you download the Agent Setup program from Support Center, you install and register the Agent in one of the following ways:
  - **Use the Agent Startup Wizard.** To use the Wizard, a technician must use Support Center to enable it for the Agent configuration. For more information, refer to *Installing Mac Agents*.
  - **Use the Agent installation command-line interface.** You can use an XML file to specify registration information. For more information, refer to *Installing Mac Agents*.

If you do not provide registration information, the Agent registers anonymously. That means that the Data Center identifies the Agent by only a computer name, and not by a user name.

During registration, the Data Center assigns a 10-digit account number to the Agent. The Data Center uses the account number to label and organize the data it receives in a backup. The Agent account is unique to the computer. You cannot use the same account number to install more than one Agent. Also, you cannot have multiple Agents or accounts on the same computer.

The Data Center tracks each Agent that you register and the total number of registrations against the total number of users permitted by your organization's license agreement, and the number of licenses allocated to a community where the Agent registers. When you use up the licenses, the Data Center does not accept new registrations from Agents until you buy more licenses, allocate additional licenses to the community, or cancel unused accounts.

# Chapter 2: Set up communities and accounts

This chapter explains how to set up communities and subcommunities, manage accounts, work with technician accounts, allocate and manage licenses, and apply bandwidth throttling to Agent backups.

- [Communities, below](#)
- [Subcommunities , on the next page](#)
- [Manage accounts, on page 23](#)
- [Managing general account functions, on page 26](#)
- [Agent Security, on page 29](#)
- [Technician accounts, on page 30](#)
- [Licenses for Agent accounts, on page 31](#)
- [Manage licenses and licensed features, on page 34](#)
- [Apply bandwidth throttling during Agent backups, on page 38](#)

## Communities

A community is a group of Agent accounts that share common characteristics, such as configuration settings, the geographical location of the clients, or similar bandwidth throttling requirements. You can use communities to run reports, edit settings, upgrade Agent configurations, and manage accounts.

## Communities in Support Center

Each community that you create in Support Center appears as a node in the left pane of the Support Center interface. The node contains subnodes that represent the accounts, technicians, reports, configurations, and subcommunities in the community.

Each community or subcommunity inherits objects from the top-level community Data Center (root level) node. For example, technicians whose permissions you define in the root level of your community can gain access to all subcommunities. You can use the Agent configurations, reports, and other objects that are defined at the root level of your community in any subcommunity.

## The Default community

If you host your Data Center, depending on the permissions that are assigned to your technician account, you might have access to a community labeled **Default**. When you install a self-hosted

Support Center, the installation procedure creates this default community.

The Default community includes the Default Agent configuration, which contains default settings and rules. You can use this community to organize your Agents, or as a model to construct your communities. You must set the correct permissions for the technician account that you use to log on to Support Center so that the account allows you access to the Default community.

If you do not host your own Data Center, you have access to specific subcommunities in the Default community. However, you might not have permissions to gain access to the top-level Default community.

## New communities

You can create as many communities and subcommunities as necessary to organize your accounts. All subcommunities that you create inherit the default Agent configuration in the root community. However, any new Agent configurations that you create in a new subcommunity are available only to that subcommunity and any of its subcommunities.

For more information, refer to Support Center Help.

### To create a new community

1. Log on to Support Center.
2. Click **Tools > Add Community**.  
The Add Community page opens.
3. In the **Community Name** field, enter a community name.
4. Click **Save**.

The name of the community appears in the left pane of the Support Center. The community node contains subnodes representing the accounts, technicians, reports, and configurations for the community.

#### **IMPORTANT:**

You can rename and move communities. However, you cannot delete communities.

## Subcommunities

You can create subcommunities in any community that you can access. You can use subcommunities to divide your Agent accounts into smaller categories, based on geographic location, departments, bandwidth throttling, or other criteria. You can reassociate a subcommunity with a different parent community, which is useful if you want your communities to reflect the changes in your organization. For more information, refer to Support Center Help.

#### **NOTE:**

To manage Agents more easily, create separate subcommunities for each type of Agent that you plan to deploy. Also keep Agent configurations for different operating systems in separate

subcommunities.

For more information about Agent configurations, see [Create Agent configurations, on page 40](#).

## Create subcommunities

### To create a subcommunity

1. Log on to Support Center.
2. Click the community for which you want to create the subcommunity.
3. From the **Tools** menu, select **Add Subcommunity**.

The Create Subcommunity page opens.

4. In the **Community Name** field, enter a name for the subcommunity.
5. Click **Save**.

The name of the subcommunity appears in the left pane of the Support Center. The subcommunity node contains subnodes representing the accounts, technicians, reports, and configurations for the community.

For more information, see the Support Center Help.

## Agent accounts in subcommunities

Agent accounts in a subcommunity share characteristics with the parent community, but they have distinct characteristics that set them apart from the parent community. For example, you might create one community to represent the Agents in your branch office. In this parent community, you can create subcommunities to represent the departments in the branch office, such as Finance, Accounting, and Marketing.

The Agents in each subcommunity inherit versions, settings, and rule sets from the parent community. They also can contain configurations unique to each subcommunity. For example, you define common rules at the community level for your entire organization. Then, for each group in your organization, you have subcommunities for which you can define unique settings. You then use the common rules and the Agent settings that you define for each group to create Agent configurations for each subcommunity.

## Disable registration in communities

After you deploy Agents throughout your enterprise, you can use Support Center to disable registration for communities and subcommunities. When you disable registration, no one can use a copy of Agent Setup to register an account that you did not intend to create. If you must add new accounts to the community or recover an account, you can enable registration.

## Manage accounts

Use Support Center to perform the following account management tasks:

- View an account number.
- View account information.
- Change account status.
- Manage general functions.
- Manage Agent security.
- Gain access to the Account Management Website to manage an account.

### View an account number

Each deployed Agent has an account in the Data Center. Each account has a 10-digit number that uniquely identifies it. The following is an example of an account number:

10203-61718

The sixth digit in the account number (the digit following the dash) is a check digit. Some of the Data Center database tables drop the check digit and use a nine-digit format instead (for example, 102031718.)

The Data Center uses this account number to label and organize all data backed up from the client.

You can view an account number in the following ways:

- From the Agent interface
- From Support Center

#### To view your account number from the Agent interface

1. Open the Agent interface.
2. Click **Connected Backup > About Connected Backup**.

The About Connected Backup window opens. Your account number is at the bottom of the window.

You can use the Agent interface to view the number of only your own account.

#### To view an account number from the Support Center

1. Use your technician ID and password to log on to Support Center.  
The organization that hosts your Data Center provides the URL you need to log on.
2. In the left pane of Support Center, click **Accounts**.  
The Account Search page opens in the right pane.

3. On the Account Search page, enter one of the following kinds of information:
  - Account name
  - Organization name
  - Department

4. Click **Search**.

The Accounts page lists the account number for every account that matches the search criteria.

## View Account Information

### To view information about an account

1. Log on to Support Center.
2. In the left pane of Support Center, click **Accounts**.

The Account Search page opens in the right pane.

3. On the Account Search page, enter one of the following kinds of information:
  - Account name
  - Organization name
  - Department
  - Account number

**TIP:**

The fastest way to find an account in Support Center is to search for the account number. If you do not know the account number, you can use the account name, organization name, department, or other identifying criteria to search for the account. For more information, refer to Support Center Help.

4. Click **Search**.

The Accounts page opens and lists the account number for every account that matches the search criteria.

5. Click the number of the account.

The Account Summary page opens and lists information about the account.

## Change account status

The status of an account determines whether the account can connect to the Data Center. If you change the account status, you can temporarily or permanently disable backup and retrieval for an Agent.

For example, change the account status to block access to the Data Center from client computers that were stolen or are no longer used. When an employee leaves your organization, you can cancel the

account for that employee so that unauthorized users cannot gain access to the files that the former employee previously backed up.

The account status includes the following options:

Status option	Description
<b>Active</b>	An account can connect to the Data Center and perform backup and retrieve operations.
<b>On Hold</b>	An account temporarily cannot connect to the Data Center and perform backup and retrieve operations.  For example, you can place an account on hold if a employee associated with the account takes a long-term leave from your organization. When the user returns, you can change the status of the account back to Active.
<b>Canceled</b>	An account cannot connect to the Data Center and perform backup and retrieve operations. The Compactor labels the information that the Agent backed up as expired and, after a defined expiration period, removes the information from the Data Center server.  For example, you can cancel a user account if the employee associated with the account permanently leaves your organization.
<b>Canceled and Data Deleted</b>	The compaction process ran on a canceled account, and the files, archives and encryption key associated with the account no longer exist on the Data Center.

**TIP:**

To cancel or place on hold multiple SSO-enabled accounts at the same time, use the `CancelHoldAccounts` command-line utility. For more information about this utility, which is part of the DC toolkit, refer to *Administering the Data Center*.

**To change the status of an account**

1. Open Support Center and search for the Agent account.
2. When Support Center displays the search results, click the Agent account number.  
The Account Summary page opens.
3. On the Account Summary page, click **Account Status**.  
The Change Account Status page opens.
4. Select a status option.  
For more information, refer to Support Center Help.
5. To save your changes, click **Change Status Now**.

## Managing general account functions

Use Support Center to manage the following general account functions:

- Reserve accounts.
- Change the primary server for an account.
- Change an Agent configuration.
- Send messages to Agents.
- Display backup messages.

### Reserve accounts

As an alternative to the standard account registration, you can reserve accounts in specific communities. To reserve accounts, you can use Support Center to generate account codes. Users can enter the code or ticket to register under the Agent community.

When users register new accounts, the Data Center verifies the code or ticket that they specify. If the code or ticket is valid, the Data Center registers the account in the community where the technician created the reservation.

**NOTE:**

Reserved accounts use client licenses on the Data Center in the same way as Active accounts.

For more information about how to reserve accounts, see Support Center Help.

### Change the primary server for an account

In mirrored or clustered environments, Agents use one Data Center server as their primary server during backup or retrieval. The Agent always attempts to contact its designated primary first. If the primary is offline, the Agent connects to the mirror of the primary server to complete the operation.

You can use Support Center to change the primary server to the secondary server.

#### To designate a primary server for an Agent

1. Open Support Center and search for the Agent account.
2. When Support Center displays the search results, click the Agent account number.

The Account Summary page opens in the right pane.

3. On the Account Summary page, click **Primary Server**.

If the Agent does not belong to a clustered or mirrored environment, **Primary Server** is not a link.

The Change Primary Server page opens.

4. Select a primary server.
5. To change the primary server to the one that you selected, click **Save**.

For more information, see Support Center Help.

## Change an agent configuration

The Agent configuration determines the following:

- Agent rules
- Security settings
- Interface controls
- Profile and Website settings

If you use multiple configurations within one community, you can change the configuration of an Agent in that community. The next time that the Agent connects to the Data Center, the Agent downloads the new configuration.

### To change an Agent configuration

1. Open Support Center and search for the Agent account.
2. When Support Center displays the search results, click the Agent account number.  
The Account Summary page opens.
3. Click the **Assigned Configuration** link.  
The Change Agent Configuration page opens.
4. Select the appropriate configuration from the displayed list.
5. To change the configuration to the one that you selected, click **Save and Deploy**.

For more information, see [Create Agent configurations, on page 40](#) and see Support Center Help.

## Send informational messages to Agents

You can send informational messages to Agents. For example, you want to provide instructions to users for an upcoming Agent configuration upgrade. This feature is different from the message notification that you can enable when you change the status of an account. For more information about how to change the status of an account, see [Change account status, on page 24](#) and refer to Support Center Help.

When you create informational messages, the Agent receives the messages the next time it connects to the Data Center. If configured to do so, the Agent displays a message notification window that it received one or more messages from the Data Center. Users must open the Agent User interface to view the messages in the Message panel of the Summary tab.

### To send a message to one or more Agents

1. Log on to Support Center.
2. Search for an account or create an account group.
3. Perform one of the following actions:
  - To send a message to a single account, from the Account Summary page, select **Tools > Send Message to Agent**.
  - To send a message to a group of accounts, from the Group Accounts page, select **Group > Send Message to Agents**.
4. In the Send Message to Agent page, enter the message that you want to send.
5. Click **Send Message**.

For more information, see Support Center Help.

## Display backup messages

Depending on your Agent configuration, the Agent can display a message notification window in the following situations:

- When a backup completes and the Agent User interface is closed
- When a backup does not successfully complete after four days.

### To enable backup messages

1. Log on to Support Center.
2. Select a community and expand the **Configurations** node, then expand the **Mac** subnode.  
The Mac Agent Configuration summary page opens.
3. Expand the **Agent Settings** node, and select a setting configuration.  
The Edit Agent Settings - General page opens.
4. On the Edit Agent Settings - General page, click **Display**.  
The Edit Agent Settings - Display page opens.
5. In the **Messages** section of the Edit Agent Settings - Display page, select the message setting that you want to enable.
6. Click **Finish**.

For more information, refer to Support Center Help.

## Use the Agent Dock icon

The Agent icon always appears on the Dock unless you remove it. Use the Agent icon to open the Agent window and view the status of the Agent during backup and retrieval, and to open the Agent Dock menu.

The appearance of the Agent Dock icon indicates whether a backup or retrieval is in progress, or the outcome of the last backup. The following table describes each variation of the Agent Dock icon:

Agent Status Icon Appearance	Indicates
	No backup has been performed since this Agent was installed, and no backup is in progress.
	A backup is in progress.
	A file retrieval is in progress.

When the Agent is open, you can gain access to the Dock menu options from the Agent Dock icon. To open the Dock menu, right-click the Agent Dock icon.

The following table describes the Dock menu options:

Menu item	Task
<b>Back Up Now</b>	Start a manual backup.
<b>Cancel Backup</b>	Cancel a backup.
<b>About</b>	View Agent version information.
<b>Manage Account Online</b>	Manage your account using the Account Management Website, if it is enabled for your account.

**NOTE:**

The Connected Backup Agent does not display the Dock menu options on Mac OS 10.6 (Snow Leopard).

For more information, see Support Center Help.

## Agent Security

Every account has an encryption key that the Agent creates during installation and registration. The Agent and Data Center uses the encryption key to encrypt and decrypt each file that the Agent backs up.

For additional security, you can configure the Data Center to notify users by e-mail when anyone retrieves a file from an account. Technicians can take appropriate action if an unauthorized person retrieves files from a specific account.

You can enable e-mail notification at the community or subcommunity level. You cannot configure e-mail notification for specific Agent configurations.

**NOTE:**

Ensure that the DCAlert service is running and configured with a valid e-mail server. For more information about how to configure the DCAlert service, refer to Data Center Management Console Help.

**To enable e-mail notification**

1. Log on to Support Center.
2. Select a community or subcommunity.
3. Click **Tools > Email Notification**.

The Change Email Notification Status page opens.

4. Select the appropriate option and click **Save**.

For more information, see Support Center Help.

## Technician accounts

Technician accounts let you control who has access to Support Center, and who has access to the Agent retrieve feature.

An administrator assigns the Support Center Administrator technician ID during the Data Center installation. The technician ID provides access to Support Center controls. Use this technician ID to create your subcommunities and other technician accounts.

If you want multiple staff members to use Support Center, create a technician account for each staff member. You can set permissions to control the level of access a technician has to Support Center features. For example, you might limit a technicians' access to specific communities.

**To create a technician account**

1. Log on to Support Center.
2. Select a community.
3. Select the **Technicians** node.
4. In the Add Technician page, enter the required information and select the permissions you want to assign to the account.
5. Click **Add Technician**.

For more information, see Support Center Help.

## Licenses for Agent accounts

The Data Center licenses control the number of accounts that you can connect to a Data Center. They also enable licensed features such as MyRoam.

If you host your Data Center, you receive a license file to use when you install the Data Center. For more information, refer to *Installing the Data Center*.

If you back up your files to a Data Center that another company manages, one of the following can occur:

- Your top-level community inherits unused licenses from a parent community.
- The technician that manages the parent community allocates a specific number of licenses for your top-level community.

## How licenses affect the Support Center display

Based on the types of licenses that you buy, Support Center displays the following configuration nodes in the left pane of the user interface:

Software Licenses	Version	Support Center display
PC and Mac Agents	8.3 and later	Configurations node, PC subnode, and Mac subnode
PC Agents	8.0 through 8.2.2	Configurations node, PC subnode
Legacy PC Agents	7.x and earlier	Legacy PC Configurations node

If you log on to Support Center and you or another technician changes the licenses, Support Center does not display the change in the left pane until you refresh the view or log into a new session.

For example, if you log on to Support Center and another technician removes licenses for PC and Mac Agents, you continue to see the **PC** and **Mac** subnodes under the **Configurations** node until you start a new session.

## License inheritance and allocation

When you register an Agent in a community or subcommunity on the Data Center, the registration completes only if a license is available. Additionally, without an available license, the Agent cannot connect to the Data Center.

A technician can allocate licenses to subcommunities, or subcommunities can inherit licenses from a parent community. By default, lower-level communities inherit licenses from parent communities. For example, if your top-level node in Support Center has access to 1,000 licenses and you create two communities below the top-level node, each subcommunity has access to the 1,000 unused licenses in the parent community.

You can use license allocation to control the number of licenses to each community or subcommunity can access. For example, you have a total of 1,000 licenses available, and you have two communities: Operations and Engineering. If you expect the Engineering community to require more registered

accounts than the Operations community, you can allocate 700 licenses to the Engineering community and 300 licenses to the Operations community. You can adjust the allocation of licenses at any time.

PC Agents and Mac Agents share the same license pool. For more information about license inheritance and allocation, see [License allocation examples, on page 34](#).

## Used and unused licenses

The Data Center considers a license in use when any of the following conditions exist:

- Accounts register in a community.  
For example, a community has access to 500 licenses and 100 accounts register in the community. The number of licenses in use for the community is 100 and the number of unused licenses is 400.
- You allocate a specific number of licenses to a subcommunity.  
For example, your top-level community has 1,000 licenses available for use, and you allocate 600 of the licenses to a subcommunity. The number of licenses in use in the top-level community is 600 and the number of unused licenses is 400.
- Accounts register in a community and you allocate some of the licenses to a subcommunity.  
For example, your top level-community has 1,000 licenses. A hundred accounts register in the top-level community, and you allocate 600 licenses to a subcommunity. The number of in use licenses is 700 and the number of unused licenses is 300.

## Licensed features for communities

You can enable or disable the MyRoam feature for a selected community.

### Feature state inheritance

Each feature in a community inherits its default state from the parent community. However, you can enable a feature in a parent community and disable the feature in its subcommunities. You also can disable MyRoam at the configuration level. For more information, refer to Support Center Help.

If you change the state of licensed features in a parent community, you affect its subcommunities in the following ways:

- If you disable licensed features in a parent community, you disable the features in its subcommunities. For example, you enable MyRoam in a subcommunity and disable MyRoam in the parent community. As a result, you also disable MyRoam in the subcommunity.
- Licensed features in subcommunities return to their previously set states if you re-enable licensed features in the parent community. For example, you disable a licensed feature in a subcommunity and in the parent community. You then re-enable the licensed feature in the parent community. As a result, you also re-enable the feature in the subcommunity.

For more information, see Support Center Help.

## Expired licenses

When licenses expire, the following behavior occurs:

- If licenses in the Data Center License File expire, the Data Center server no longer accepts connections from Agents.
- If the licenses for a product type (PC or Mac) expire, the Data Center no longer accepts connections from those Agents.
- If licenses expire, new Agents cannot register in the Data Center.
- If a registered PC Agent attempts to back up files or retrieve files, and the licenses expire, the process fails. The History tab in the Agent User interface displays a failed event.
- If a user attempts to register an account with an expired license, the Account Management Website informs the user that the license is not valid.

To get more licenses, contact your Sales Representative.

## Effect of licenses on accounts and communities

The availability of unused and unexpired licenses affect the following tasks:

- **Agent registration**

If no licenses are available in a community, or if the licenses expire, new Agents cannot register in the Data Center and the Account Management Website displays an error message. If the Agent cannot register an account, it cannot back up or retrieve files. To let new Agents register, buy or allocate additional licenses to the affected community.

- **Changing account status**

- If no unused licenses exist for the community in which an account is registered, you cannot change its status to Active or On Hold.
- If you change the status of an account to Canceled, the license that the account used becomes available. A new account can register and use this license.
- If you change the status for multiple accounts simultaneously, and you do not have an available license for every accounts in the group, the Data Center changes the status for only a subset of the selected accounts.
- The Data Center does not change the status for all accounts. The Results page in Support Center lists the changes that did not occur. For example, a community had five available licenses, and you tried to change the status of seven accounts. The status of two of the accounts remains the same.

- **Moving communities**

When you move communities from one location to another, the destination community must have a sufficient number of unused licenses for the communities that you move.

For example, you have a community named Accounting that has 500 licenses allocated for its use, and you want to move it to a new parent community named GlobalOperations. The GlobalOperations

community must have at least 500 or more unused licenses to accommodate the Accounting community.

After you move a community, the licenses that it used become available to the original parent community and the moved community uses licenses that it obtains from its new parent community.

- **Moving accounts**

If you move an account from one community to a different community, the new community must have an unused license of the appropriate product type that the account can use. After you move the account, the license it used in the original community becomes available. The moved account uses a license from its new community.

If you move a group of accounts from one community to a different community, and the new community does not have enough licenses of the appropriate product type for all of the accounts, Support Center moves some accounts and displays a message that indicates that some accounts did not move. To move the remaining accounts, buy or allocate additional licenses to the community.

## Manage licenses and licensed features

This section contains an example of license allocation. It also describes how to perform the following tasks:

- Allocate licenses.
- Enable or disable licensed features.

## License allocation examples

Assume that you host your Data Center. Your Data Center License File provides you with 5,000 account licenses.

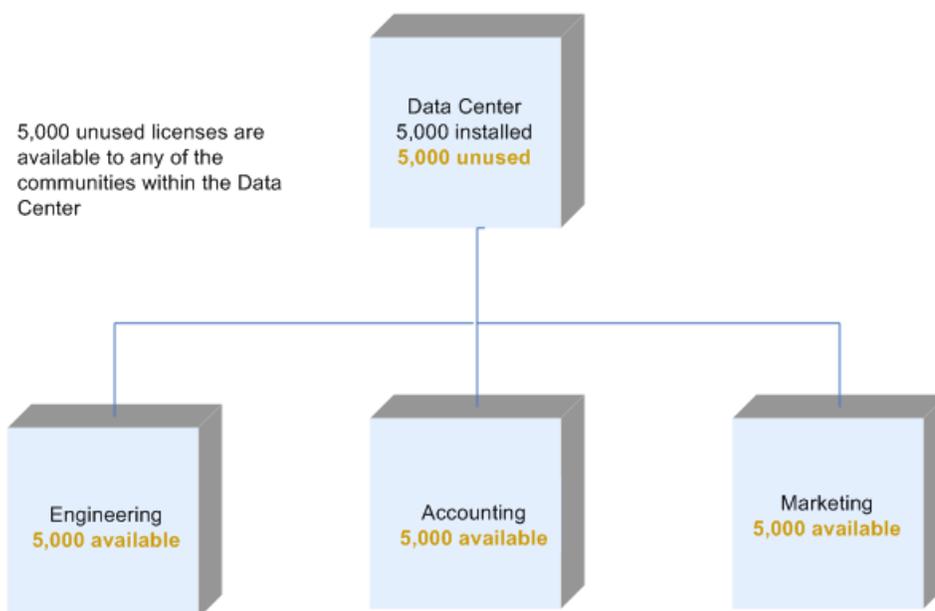
After you install your Data Center, you create the following communities:

- Engineering
- Accounting
- Marketing

## Inherited licences

Initially, all communities inherit the licenses. Because you have not yet explicitly allocated the licenses, each community has access to the 5,000 licenses. The following figure shows the initial license allocation.

### Initial License Allocation



As users register accounts in the individual communities or as you allocate licenses to other communities, the number of licenses in use increases and each community that inherits its licenses has access to fewer licenses.

For example, 100 accounts register in the Engineering community, and you do not explicitly allocate any licenses to other communities. You have 4,900 unused licenses to which all communities have access.

## Allocated licenses

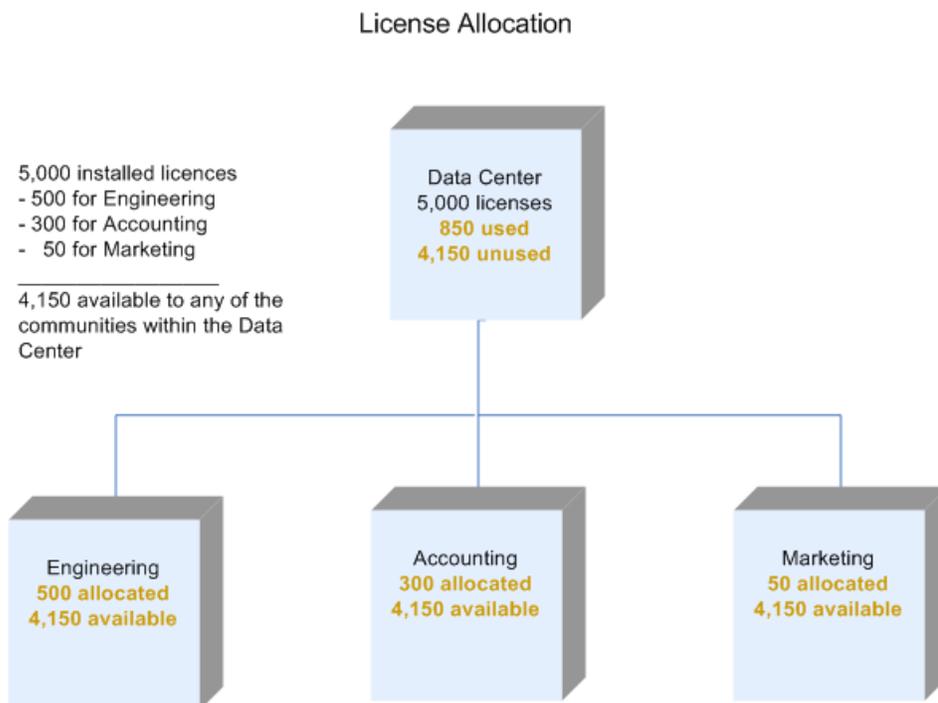
To control the use of licenses, and to avoid a situation where one community runs out of needed licenses, you allocate some of the licenses. In addition, your enterprise charges other enterprises for backup services, so you must control the number of licenses to which other enterprises have access.

You know the following information:

- The Engineering division has 500 client systems that must back up their data.
- The Accounting division has 300 client systems that must back up their data.
- The Marketing division has 50 client systems that must back up their data.

After you allocate required licenses to each division, you have 4,150 unused licenses and 850 licenses in use. In this example, a license is in use after you allocate it to another community. If you create another community and let it inherit licenses, it would have access to the 4,150 unused licenses.

The following figure shows the license allocation for this example.



## Licenses allocated to subcommunities

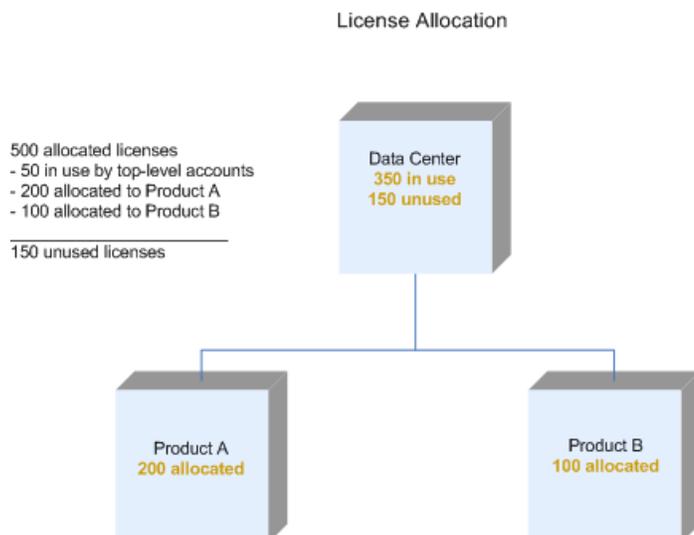
The Engineering division can create subcommunities and allocate licenses to these subcommunities. After you inform the Engineering division that their community is available, the administrator in the Engineering division divides the community into the following subcommunities:

- Product A
- Product B

Initially, the Engineering community and each subcommunity has access to the 500 allocated licenses, with the following use of licenses:

- Fifty accounts register in the top-level community. Each subcommunity now has access to 450.
- You allocate the remaining unused licenses as follows:
  - Product A receives 100 licenses.
  - Product B receives 200 licenses.

You have 150 remaining licenses. Up to 150 new accounts can register in the top-level community, or you can allocate any of these licenses to existing subcommunities or to a new subcommunity, or both, as shown in the following figure:



## Allocate licenses

To make it easier to manage licenses, create different communities for different types of licenses. For example, create a community for Mac licenses, and a different community for PC licenses.

### To allocate licenses

1. Log on to Support Center. Use a technician ID that has permissions to allocate licenses in sub-communities.
2. In the left pane of the Support Center interface, select a community or subcommunity.
3. On the Community Status page, click **Allocate Licenses**.

The Allocate License page opens.

4. Select the appropriate allocation options.  
For more information, see Support Center Help.

5. To save your selections, click **Save**.

Support Center displays the following message:

The license allocation changes have been saved.

If you do not have permission to allocate licenses for a selected community, Support Center displays the View License Summary page instead of the Allocate Licenses page. You can use this page to view the current license allocation.

For more information, see Support Center Help.

## Enable or disable licensed features

### To manage licensed features

1. Log on to Support Center. Use a technician ID that has permissions to allocate licenses in sub-communities.
2. In the left pane of the Support Center interface, select a community or subcommunity.
3. On the Community Status page, click **Manage Features**.  
The Manage Features page opens.
4. In the Manage Features dialog box, select the feature that you want to enable or disable, and then click **Save**.

Support Center displays the following message:

The Manage Feature changes have been saved.

For more information, see [Licensed features for communities, on page 32](#).

## Apply bandwidth throttling during Agent backups

You can use the bandwidth throttling feature to limit the amount of network bandwidth that Agents use during backups. If you throttle bandwidth during Agent backups, you can allocate more bandwidth to other network activities and to user's Internet applications. When you use bandwidth throttling for Agent backups, backups are less intrusive, but take longer to complete.

### NOTE:

- Bandwidth throttling applies to only Agent backups. It does not apply to Retrieve operations.
- Set bandwidth throttling limits that are appropriate for your network. The Data Center does not check the available bandwidth of your network against the bandwidth throttling limits that you set in Support Center. If you set maximum bandwidth limits that exceed actual data transfer speed of your network, the bandwidth throttling does not reduce Agent intrusiveness during backups.

You can set the following bandwidth limits:

- Minimum bandwidth required for an Agent to perform a backup
- Maximum bandwidth to allocate to an Agent performing a backup
- Maximum bandwidth to allocate to all Agents performing backups

You also can establish a schedule to identify the peak, medium peak, and off peak network traffic times, and vary the bandwidth allocations accordingly.

You can configure bandwidth throttling at the Data Center level and the community level. At the Data Center level, you can choose whether to throttle bandwidth for all accounts that the Data Center manages. At the community level, you can choose whether to throttle bandwidth for the accounts in the community, or you can choose to inherit the bandwidth throttling configuration (throttled or not throttled)

from the parent community. When a subcommunity inherits bandwidth throttling from its parent community, and you specify a maximum shared bandwidth, the maximum shared bandwidth is shared among all Agents in the parent communities and any subcommunities that inherit bandwidth throttling.

### **To configure bandwidth throttling**

1. Log on to Support Center.
2. In the left pane of the Support Center interface, select a community or subcommunity.
3. On the Community Status page, click **Bandwidth Throttling**.

The Bandwidth Throttling - Options page opens.

4. Select a bandwidth throttling option.

For more information, click **Help**.

5. Click **Save**.

Support Center displays the following message:

Your bandwidth throttling options have been saved.

For more information, see Support Center Help.

# Chapter 3: Create Agent configurations

This chapter explains the components that make up an Agent configuration. It also explains how to create Agent configurations.

- [About Agent configurations, below](#)
- [Configuration components, below](#)
- [Create an Agent configuration, on page 42](#)

## About Agent configurations

You create Agent configurations in Support Center to specify the features that are in the Agents that you deploy. Agent configurations also contain the settings and rules that control the behavior of an Agent after you install it on a client computer.

Support Center supports the following types of Agents:

- 7.x Legacy PC Agents
- 8.x or later PC Agents
- 8.3 or later Mac Agents

## Configuration components

An Agent configuration contains the following components:

- Profile and Website settings
- Agent versions
- Agent settings
- Agent rule sets

Support Center compiles Agent configurations from a set of components that each specify some of the Agent features. You can gain access to the configuration information for each community.

### To gain access to the configuration information for a community

1. Open Support Center.
2. In the left pane of the Support Center interface, under the name of the community in which the Agent resides, expand **Configurations**, and then expand **Mac**.

The following sections describe the configuration components in detail.

## Profile and Website settings

The Profile and Website settings determine the information and features that are available to users in the Account Management Website. They also determine the information that is in users' profiles, and the fields that are in the Agent Startup Wizard. In Support Center, the Profile and Website settings for each community appear in the **Configurations** node.

For more information about the Account Management Website, see [Deploy Account Management Website, on page 67](#).

For more information about Profile and Website settings, see Support Center Help.

## Agent versions

Agent versions point to an Agent file set of a specific version and language. For example, you have an Agent version named Marketing PC. When a new version of the Agent software becomes available, you can download the new version and apply it to your deployed Agents.

For best practice, consider the following recommendations:

- When you create new Agent version in Support Center, do not include the version number in the name. For example, do not use Marketing versionX. Instead, use Marketing. If you include the version number in the name, the name becomes obsolete when you update the Agent version.
- Based on the needs of your organization, you might need to create one or more Agent versions. For example, you have computers in different departments with different backup requirements. You can create an Agent version for each department.
- You can use the same Agent version with several or all Agent configurations. When a new version of the Agent software is available, update only the Agent version and not every Agent configuration.

## Agent settings

The Agent has optional features specific to your license agreement that you can enable or disable. Agent settings determine which features are accessible to the Agent user. The settings contain parameters that govern the Agent backup and retrieve features, such as the backup schedule and backup type. You also can enable security features such as proxy server settings and password protection of retrievals.

## Agent rule sets

The Agent uses rule sets to determine which files to select during a backup. You can specify Agent rules in Support Center when you create or modify an Agent configuration.

Support Center includes a default rule set that you can associate with one or more Mac Agent configurations. You also can create your own rule sets. If you let users modify their backup sets, they also can create rules that determine which files the Agent selects for backup. For more information, see [Create Agent rule sets, on page 46](#).

## Default Agent configuration

The Support Center installation creates a default Agent configuration. The default configuration has a name similar to Default Mac *version* Configuration, where *version* is the Agent version number. The default configuration resides at the root level of the tree in Support Center and is available to all of your communities. You might want to create your own configuration with a unique version, settings, and rules. However, you can use the default configuration as a reference when you create your own configurations.

For more information, see Support Center Help.

The default configurations contain the following components:

- Default Agent Version
- Default Agent Settings
- Default Agent Rule Sets
- Default Profile and Website Settings

## Create an Agent configuration

Use Support Center to create the Agent configuration and its components. The technician ID that you use to log on to Support Center must include the **Modify Agent Configurations** permission.

**NOTE:**

You cannot use the Support Center application from a computer with Mac OS X. Use Internet Explorer installed on a Windows operating system to open Support Center.

### To create an Agent configuration

1. Allocate licenses.
2. Create an Agent version.
3. Create Agent settings.
4. Create Profile and Website Settings.
5. Create an Agent rule set.
6. Create the Agent configuration.

The following sections describe these steps in greater detail.

**NOTE:**

Perform the steps to create an Agent configuration in the order in which the steps appear in the guide.

## Allocate licenses

To create a new Agent configuration for a community, the community must have at least one available license.

### To verify that a community has at least one available license

1. In the left pane of the Support Center interface, click the community node.  
The Community Status page opens.
2. In the **Account Summary** section, look at the value in the **Unused** column for the **PC and Mac** license type and verify that at least one unused license is available.  
If no licenses are available, you can change your license allocations.
3. To change your license allocations, click **Allocate Licenses**.  
The Allocate Licenses page opens.
4. Select the appropriate allocation options.  
For more information, click **Help**.
5. To save your selections, click **Save**.  
Support Center displays the following message:  
The license allocation changes have been saved.

## Create an Agent version

### To create an Agent version

1. Expand the **Configurations** node in the community where you want to create the configuration.
2. Expand the **Mac** node.
3. Click **Agent Versions**.  
The Create Agent Version page opens.
4. Enter the Agent version information.  
Only Mac Agent versions are available in the **Agent** drop-down list.
5. Click **Create**.  
The Edit Agent Version - Description page opens.
6. Enter a description for the version, then click **Save and Deploy**.  
The name of the Agent version appears in the left pane under the **Agent Versions** node.

## Create Agent settings

### To create Agent settings

1. Expand the **Configurations** node in the community where you want to create the configuration.
2. Expand the **Mac** node.
3. Click **Agent Settings**.  
The Create Agent Settings - General page opens.
4. Configure the Agent Settings.  
For more information, click **Help**.
5. When you complete the Agent Settings, click **Finish**.  
The name that you assigned to the setting appears in the left pane under the **Agent Settings** node.

## Create Profile and Website settings

### To create Website settings

1. Expand the **Configurations** node in the community where you want to create the configuration.
2. Click **Profile and Website Settings**.  
The Create Profile and Website Settings - General page opens.
3. When you complete the Website settings, click **Finish**.  
The name that you assigned to the setting appears in the left pane under the **Profile and Website Settings** node.  
For more information, click **Help**.

## Create an Agent rule set

### To create an Agent rule set

1. Expand the **Configurations** node in the community where you want to create the configuration.
2. Expand the **Mac** node.
3. Click **Agent Rule Sets**.  
The Create Rule Set page opens.
4. Configure the rule set.  
For more information, click **Help** on each page of the Rules wizard.
5. When you complete the rule set, click **Finish Rule Set**.

The name that you assigned to the rule set appears in the left pane under the **Agent Rule Sets** node.

## Create the Agent configuration

### To create a new Agent configuration

1. In Support Center, expand a community node, and then expand the **Configurations** node.
2. In the right pane, clear **Use inherited configuration settings**.

If you do not clear this setting, the configurations that you create for the community are inactive. That means that you cannot download an Agent Setup file from the community.

3. Click the **Mac** subnode.
4. In the right pane, on the Configurations menu, click **Create**.
5. Enter a meaningful community name, such as "Finance Department."
6. From the drop-down lists, select the following:

- An Agent version
- Agent settings
- Profile and Website settings
- Agent rule set

Each list contains the components you previously created and the default components.

7. To create the configuration, click **Save and Deploy**.

After you create the Agent configuration, two things happen:

- The **Download** menu becomes available. If you want to distribute the Agent Setup file, use this menu to download it to your computer.
- If the Account Management Website is installed for your Data Center, a URL for Account Management Registration appears. Copy and send this case-sensitive URL to users whom you want to register and install an Agent account.

# Chapter 4: Create Agent rule sets

This chapter explains the types of rules that the Agent uses to determine which files to include and exclude in backup. It also explains how to use Support Center to create rules.

- [Rule types, below](#)
- [The rule matching process, below](#)
- [Rule categories, on page 49](#)
- [Create rules, on page 50](#)

## Rule types

The Agent uses rules to determine which files to include or exclude from backups and recoveries.

Rule types determine the order in which the Agent processes rules. The following table describes the rule types that the Agent uses and how they determine processing order:

Rule Types	Description
<b>Locked</b>	Rules that technicians define through the Support Center. Other types of rules cannot override locked rules.  The Agent tries to match files with locked rules before it examines any other type of rule.
<b>User-created</b>	Rules that users define on their local Agent and associate with files on their local system.  To define user-created rules, users must have permission to modify their backup sets.  User-created rules do not override locked rules, but they override unlocked rules.  The Agent tries to match files with user-created rules after it examines locked rules.
<b>Unlocked</b>	Rules that technicians define from the Support Center.  Locked rules and user-created rules override unlocked rules.  The Agent tries to match files with unlocked rules after it examines locked rules and user-created rules.

## The rule matching process

The Agent processes rules according to the following factors:

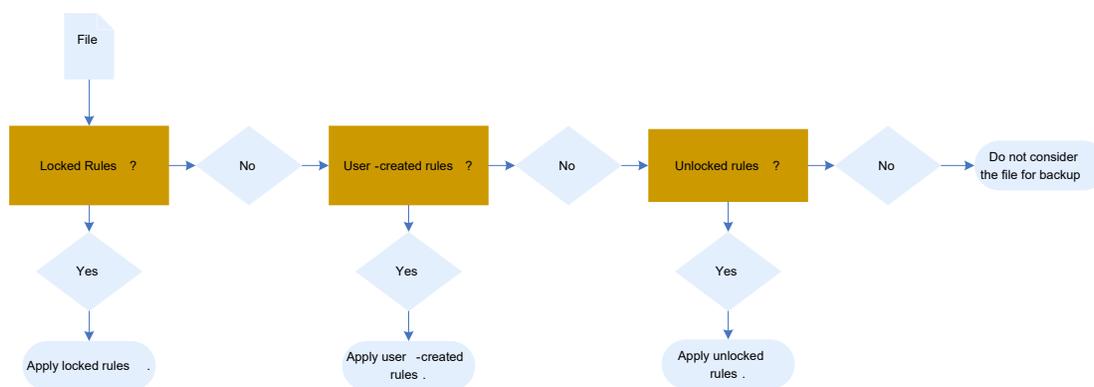
- **Rule logic.** The way the Agent processes each type of rule (locked, user-created, or unlocked). For more information about rule types, see [Rule types, on the previous page](#).
- **Rule precedence.** The position of rules in the rule list.

When the Agent scans a drive, it examines locked rules first. The Agent moves through the list of locked rules in top-down order until it finds a rule that applies to one or more files. You determine the precedence of rules in a list when you use the Support Center Rules wizard to create the rule set.

## Rule logic

If the Agent matches a locked rule to a file or group of files, the Agent stops comparing the matched file or files to other rules. However, if the Agent cannot match a file to a locked rule, the Agent compares the file to user-created rules. If the file matches a user-created rule, the Agent stops comparing that file with additional rules. If the file does not match a user-created rule, the Agent continues to compare the file to unlocked rules. If the files does not match an unlocked rule, the Agent does not include the file in the back up.

The following figure shows the logic that the Agent follows to process rules:



For example, a user creates a rule that excludes all `.mp3` files from backup. During a scan, the Agent compares the user's files against all of the locked rules in the rules set and finds no rule that pertains to `.mp3` files.

The Agent then compares the user's files to the user-created rules. The Agent finds a rule that excludes all `.mp3` files from backup. The Agent drops all `.mp3` files from the backup list. The Agent then finds an unlocked rule that includes all `.mp3` files in the backup. Because user-created rules take precedence over unlocked rules, the backup excludes `.mp3` files.

The Agent uses the following process to determine which files to select for backups:

1. The Agent determines which volumes to exclude from the backup set.

Users can use the Agent interface to exclude volumes from backup. The Agent does not scan these excluded volumes. Excluded volumes do not show up on the Backup Set tab in the Agent User interface.

2. The Agent tries to match files to rules based on rule type.

The Agent examines rule types in the following order:

- a. Locked rules
  - b. User-created rules
  - c. Unlocked rules
3. When the Agent scans the hard drive, the Agent tries to match files to the list of rules under each rule type.

The Agent examines the first rule in the list of files for each rule type. It compares the rule definition to the file location, name, and type.

If the file does not match this rule, the Agent examines the next rule in the list. The Agent continues this process until it finds a rule that matches the file. After the Agent finds a matching rule, it uses the rule category type to classify the file as user-created files, application or system files, or an excluded file. Based on the rule type and how you configure the Agent, the Agent selects or does not select a file for backup.

If a file does not match any rules, the Agent does not consider the file for backup.

## Rule precedence

Assume that you want to create a set of locked rules that cause the Agent to select most files with a .doc extension for backup and not select files that start with the letter x. The following figure illustrates how the order of rules results in different behaviors:

LOCKED RULES FOR RULE SET 1	
<b>First Rule:</b>	
<b>Category</b>	User-Created Files
<b>Rule Name</b>	Include x*.doc files
<b>Folder</b>	*
<b>Scope</b>	All folders and subfolders
<b>File name</b>	*
<b>File types</b>	doc

<b>Second Rule:</b>	
<b>Category</b>	Exclusions
<b>Rule Name</b>	Exclude x*.doc files
<b>Folder</b>	*
<b>Scope</b>	All folders and subfolders
<b>File name</b>	x*
<b>File types</b>	doc

In this example, all files with the .doc extension match the first rule in the list of locked rules. The Agent does not compare any of the files with the .doc extension to the second rule.

Using these rules, the Agent selects all files with a .doc extension. Because all of these files match the first rule, the Agent does not apply the second rule to files with a .doc extension.

LOCKED RULES FOR RULE SET 2	
<b>First Rule:</b>	
<b>Category</b>	Exclusions
<b>Rule Name</b>	Exclude x*.doc files
<b>Look in Folder</b>	*
<b>Scope</b>	All folders and subfolders
<b>File name</b>	x*
<b>File types</b>	doc

<b>Second Rule:</b>	
<b>Category</b>	User-Created Files
<b>Rule Name</b>	Include x*.doc files
<b>Folder</b>	*
<b>Scope</b>	All folders and subfolders
<b>File name</b>	*
<b>File types</b>	doc

In this example, all files that start with x and have a .doc extension match the first rule in the list of locked rules. The Agent does not select any of these files for backup.

Using these rules the Agent selects only the files that **do not** start with x **and** have a .doc extension.

## Rule categories

Rule categories determine whether the Agent considers files for backup. For more information, see Support Center Help. The following table describes each rule category:

Rule Category	Description
User-Created Files	Include user-created files, such as spreadsheets and documents, in

Rule Category	Description
rules	backups.
Exclusion rules	Exclude files from backups.  <b>NOTE:</b> If you exclude a file from a backup, you cannot retrieve it.

## Create rules

You can create rules in the following ways:

- Use the Agent Rules Wizard in the Support Center to modify a default rule set and save it under a new name.
- Use the Agent Rules Wizard in the Support Center to create a new rule set without using a default set as a template.
- Use the Agent User interface.

## Best practices for creating rules

When you create rules, consider the following best practices:

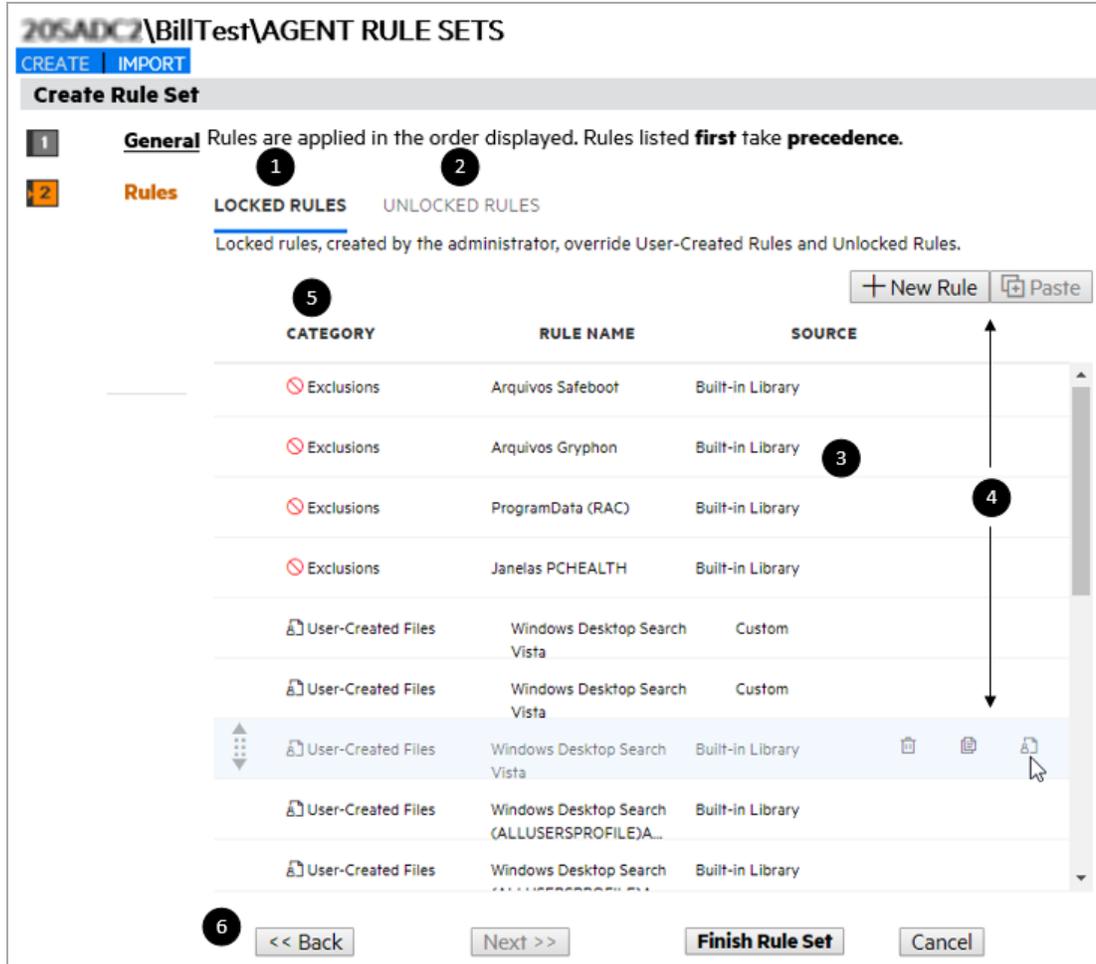
- Consider the types of files that you want to select for backup, and determine which rule category applies to the files. For example, you want the Agent to back up all .mp3 files. Because .mp3 files are files that users create, you must create User-Created Files rule to include .mp3 files in backups.
- Do not rely on the absence of a rule to exclude a file from backup. To exclude files from backup, create an exclusions rule to specify the exclusion. For example, assume you are a technician who wants to exclude all .mp3 files from backups. Because the Agent does not consider files for backup unless the file matches a rule, you decide that you can exclude .mp3 files from backup if you do not create a rule for them. However, a user creates a rule that specifies .mp3 files for backup. As a result, the Agent backs up the user's .mp3 files. To ensure that the Agent does not back up .mp3 files, create a locked exclusions rule.

## Use rule sets

Rule sets are collections of rules. You can create rule sets for different organizations, locations, or types of computer users. For example, you create a rule set for Corporate Engineering that specifies which files you want the Agent to back up and which files you want the Agent to exclude. Every Agent contains default rule sets. You can use the default rule sets as they are or as a starting point to create custom rule sets.

## Rules page

After you open the Agent Rules Wizard in Support Center and enter general properties for a rule set, you can enter rule definitions in the Rules page. The following figure is an example of the Rules page:



The following table lists the elements in the Rules page:

Element	Description
1	<b>Locked Rules tab.</b> Lists rules that the Agent evaluates before all other types of rules. Users cannot use the Agent interface to modify locked rules.
2	<b>Unlocked Rules tab.</b> Lists rules that the Agent evaluates after it evaluates locked rules and user-created rules. Users cannot use the Agent User interface to modify unlocked rules, but they can create user-created rules that override unlocked rules.
3	<b>Rules list.</b> Lists the rules for the selected rule type.

Element	Description
<b>4</b>	<b>Rule editing buttons and icons</b> <ul style="list-style-type: none"><li>• <b>New.</b> Opens the New Rule window. Use this window to specify the details for the new rule. When you save the rule, the Rules wizard places the new rule at the end of the list.</li><li>• <b>Edit.</b> Opens the Edit Rule window. Use this window to change the details of an existing rule.</li><li>• <b>Convert to Custom.</b> Lets you create a copy of a built-in rule that you can modify.</li><li>• <b>Cut.</b> Lets you remove rules from the current rule set and put them in the Support Center clipboard. You can paste these rules into another rule set.</li><li>• <b>Copy.</b> Makes a copy of the selected rules and puts them in the Support Center clipboard. You can paste these rules into another rule set or move a group of rules to a different location in the current rule set.</li><li>• <b>Paste.</b> Puts the rules in the Support Center clipboard into the current rule set.</li><li>• <b>Remove.</b> Permanently deletes a rule from the current rule set. Support Center does not put the rule in its clipboard.</li></ul>
<b>5</b>	<b>Details of selected rule.</b> The rule definitions that the Agent uses to match rules with files. The Agent uses the Category detail to determine which files to select based on the backup type.
<b>6</b>	<b>Rule set buttons</b> <ul style="list-style-type: none"><li>• <b>Back.</b> Opens the Rule Set - General page.</li><li>• <b>Next.</b> Not used on this page.</li><li>• <b>Finish Rule Set.</b> Saves the current rule set. The Rules wizard displays this button if you have permission to modify the rule set.</li><li>• <b>Close.</b> Closes the window.</li></ul>

## Use the Agent Rules wizard

To create, edit, or remove rule sets and rules, use the Agent Rules wizard. For more information, refer to Support Center Help.

### To use the Rules wizard

1. Log on to Support Center.
2. Select a community where you want to create or edit a rule set.
3. Expand the **Configurations** node and expand the **Mac** subnode.
4. Complete one of the following tasks:

- To create a new rule set
    - a. In the left pane, select **Agent Rule Sets**.  
The Create Rule Set page of the Rules wizard opens.
    - b. Use the Rule Set - General page to specify a name for the rule set and the volumes that you want the Agent to exclude.
  - To modify a rule set
    - a. Expand the **Agent Rule Sets** node and select the rule set that you want to modify.  
The View Rule Set page of the Rules wizard opens.
    - b. Save the rule set under a different name, and then follow the Rules wizard to edit or remove rules in the rules list.
5. To save all of the new or modified rules in the rule set, click **Finish Rule Set**.

# Chapter 5: Agent security features

This chapter explains how the Agent security features ensure that unauthorized users do not intercept and decode files while they travel between the Agent and the Data Center.

- [Encryption, below](#)
- [Access Control List management, below](#)
- [Unauthorized access prevention, below](#)

## Encryption

When you register an Agent, the Agent generates an encryption key (a random alphanumeric string) and stores it locally on the Agent host computer. The Agent does not store the encryption key in clear text. Instead, the Agent applies 128-bit Advanced Encryption Standard (AES) encryption to the key. You cannot change the level of encryption that the Agent uses to encrypt the key.

During Agent registration, the Agent uses Secure Sockets Layer protocol (SSL) to securely transmit the encrypted key to the Data Center. The Data Center escrows the key, in encrypted format, on its Data Center server so that you can recover the key if you need to fully recover the Agent account.

Before the Agent performs a system backup, it uses the encryption key to encrypt the files in the backup set. This ensures that hackers cannot intercept and decode the files while they travel between the Agent and the Data Center during the backup. The files remain encrypted on the Data Center. When the Agent initiates a retrieval, the Data Center sends the encrypted files to the Agent. When the Agent receives the files, it decrypts them and then downloads them to the client computer. Because the Agent stores the encryption key locally, only the Agent that encrypted the files can decrypt them.

## Access Control List management

Administrators can apply different file permissions and extended attributes to accounts to limit the access that non-administrative users have to files, folders, and drives. If configured to do so, the Agent backs up file permissions and extended attributes that are on the client computer and retrieves them along with the files the user requests.

When Agents retrieve files for computers, they reapply the file permissions and extended attributes so that only authorized users can view the files. If you have computers in your organization that multiple users share, the Agent installed on a computer can back up and retrieve files for all of the users. However, it does not let users retrieve files for which they do not have file permissions.

## Unauthorized access prevention

This section describes Agent features that prevent unauthorized access to files.

## Security certificates

To prevent unauthorized access to files during transmission from the Agent to the Data Center, Data Center Setup embeds a security certificate in the Agent. The Agent uses the security certificate to authenticate the Data Center server to perform the following tasks:

- Registration
- Upgrade
- Backup
- Retrieve
- Edit Profile

## Password protection for retrieval

To prevent unauthorized access, you can require users to supply an account ID and password to retrieve a file.

When you create Agent configurations, enable password protection for the retrieve feature. If you enable this feature, users must enter their account password to retrieve files.

For more information, see Support Center Help.

## Prevent access to files on a lost or stolen computer

### To prevent access to files on a lost or stolen computer

1. Recover the Agent account to a computer that has a name that is different from the lost or stolen computer.

The Data Center prevents access to accounts from more than one computer name. Restoring the account to a replacement computer with a name that is different from the lost or stolen computer ensures that the account is protected.

2. To allow a computer name change, do the following:
  - a. Open Support Center.
  - b. Search for the Agent account.
  - c. When Support Center displays the search results, click the account number in the Account column.
  - d. Select **Tools > Allow Computer Name Change**.  
The Allow Computer Name Change page opens.
  - e. Click **Allow Change**.

This procedure deletes the computer name that is associated with the account. The next time the Agent runs a backup, the Data Center recognizes that the account moved to a new computer.

3. Restore the account data.
4. Use Support Center to cancel the account from the lost or stolen computer, and remove the old account data from the Data Center server.

# Chapter 6: Brand product components

This chapter explains how to use Support Center to brand the Agent software, Support Center, and the Account Management Website.

- [Branding overview, below](#)
- [Branding options for Agents, on page 59](#)
- [Branding options for Support Center, on page 62](#)
- [Branding Options for the Account Management Website, on page 63](#)
- [Brand product components, on page 64](#)

## Branding overview

You can brand the product in the following ways:

- Replace the default Micro Focus product branding with your company branding.
- Display your company branding but retain the Micro Focus logo.
- Remove the default Micro Focus logo so that it is not displayed with your company branding.

You can brand the following product components:

- Agent
- Support Center
- Account Management Website

If you host your Data Center and have access to the top-level community, you can brand the entire Data Center. If you do not host your Data Center, you can use a technician ID to brand any community or subcommunity that to which you can gain access.

If you host your Account Management Website, you can brand the entire Website.

### NOTE:

Branding will unsign the Agent and the security pop-up will appear.

## Agent branding options

You can brand the following components in the following ways:

Component	Description	Branding options
Agent	The program that installs the Agent.	<ul style="list-style-type: none"><li>• Product name</li></ul>

Component	Description	Branding options
installation program		<ul style="list-style-type: none"> <li>• Default installation folder where the Agent Setup executable installs the Agent software</li> <li>• Micro Focus logo</li> </ul>
Agent User interface	<p>The application that lets you perform backups, retrievals, and otherwise manage your Agent account. The Agent User interface includes the following components:</p> <ul style="list-style-type: none"> <li>• Agent Startup Wizard</li> <li>• Welcome to the Agent window</li> <li>• Enter Password dialog box</li> </ul> <p>Used only by accounts that are not mapped to single sign-on (SSO) accounts. Agent branding does not affect the corporate sign in page for SSO accounts.</p> <ul style="list-style-type: none"> <li>• Synchronizing screen</li> <li>• Agent console</li> <li>• Agent About window</li> </ul>	<ul style="list-style-type: none"> <li>• Product name</li> <li>• Product logo for the following components:                             <ul style="list-style-type: none"> <li>◦ Agent console</li> <li>◦ Agent About window</li> <li>◦ Micro Focus logo</li> </ul> </li> </ul>
Desktop elements	Dock menu for the Agent Application icon	<ul style="list-style-type: none"> <li>• Product name</li> <li>• Micro Focus logo</li> </ul>

## Support Center branding options

You can brand Support Center in the following ways:

Component	Description	Branding options
Sign In dialog box	The dialog box that lets you enter credentials to sign in to Support Center	<ul style="list-style-type: none"> <li>• Product image</li> <li>• Micro Focus logo</li> </ul>
Change Password dialog box	<p>The dialog box that lets you change the password that you use to sign in to Support Center</p> <p>This dialog box is used only by accounts that are not mapped to single</p>	<ul style="list-style-type: none"> <li>• Product image</li> <li>• Micro</li> </ul>

Component	Description	Branding options
	sign-on (SSO) accounts. Support Center branding does not affect the corporate sign in page for SSO accounts.	Focus logo
Application header	The header that displays at the top of all application pages	<ul style="list-style-type: none"> <li>• Product image</li> <li>• Micro Focus logo</li> </ul>

## Account Management Website branding options

You can brand the Account Management Website in the following ways:

Component	Description	Branding options
Account Management Website	The web-based application that lets users perform the following tasks: <ul style="list-style-type: none"> <li>• Register a new account and download the Agent software</li> <li>• View account information</li> <li>• Modify profile information</li> <li>• Recover accounts</li> <li>• Use MyRoam to retrieve files</li> <li>• Order backed-up files on media</li> </ul>	<ul style="list-style-type: none"> <li>• Web site name</li> <li>• Product logo on the Web site</li> <li>• Micro Focus logo</li> </ul>
	<b>NOTE:</b> AMWS branding does not affect the corporate sign in page for SSO accounts.	

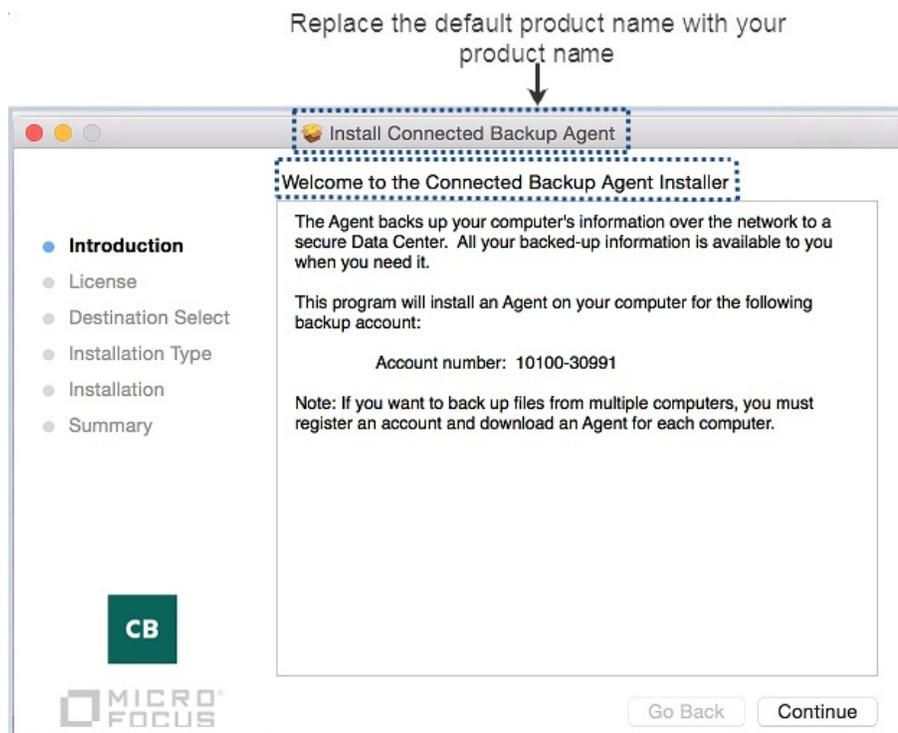
## Branding options for Agents

You can brand the following elements in the Agent User interface:

- Agent installer windows
- Agent user interface

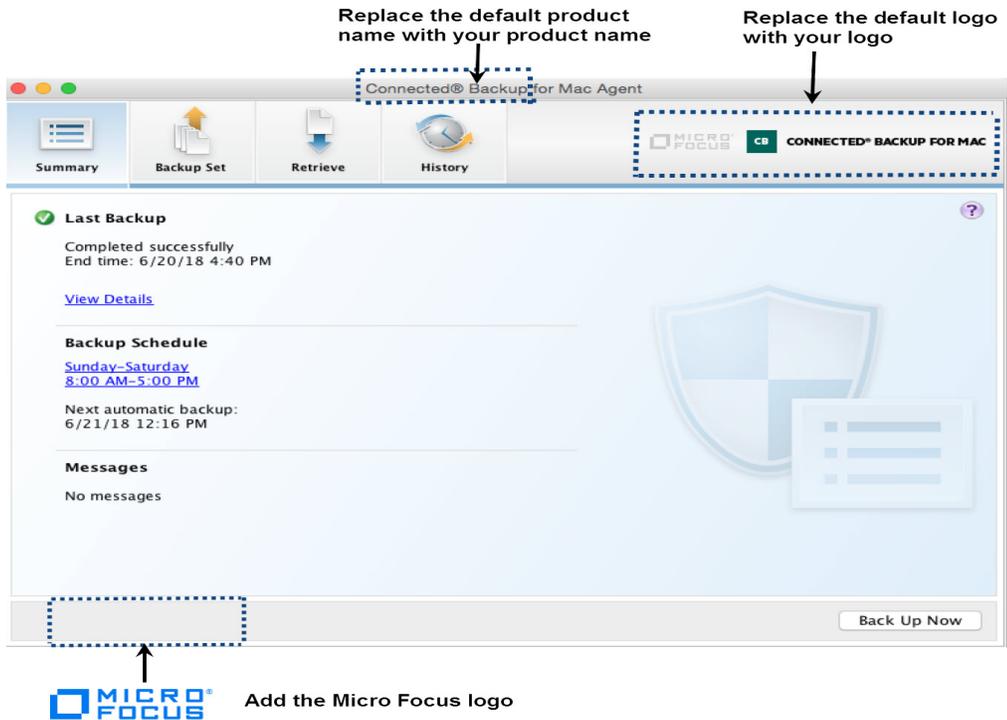
## Branding options in the Installer window

The following figure shows which elements you can brand in the Agent Installer window:



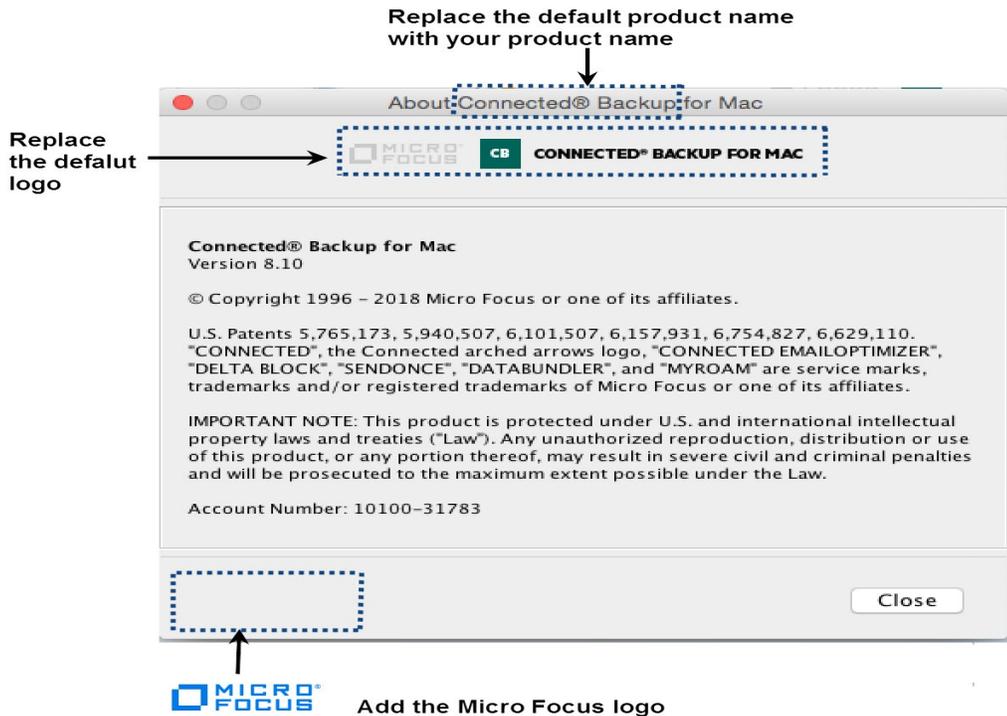
## Branding options in the Agent User interface window

The following figure shows which elements you can brand in the Agent User interface.



## Brand the About window

The following figure shows which elements you can brand in the Agent User interface About window.



## Branding options for Support Center

You can brand the following Support Center elements:

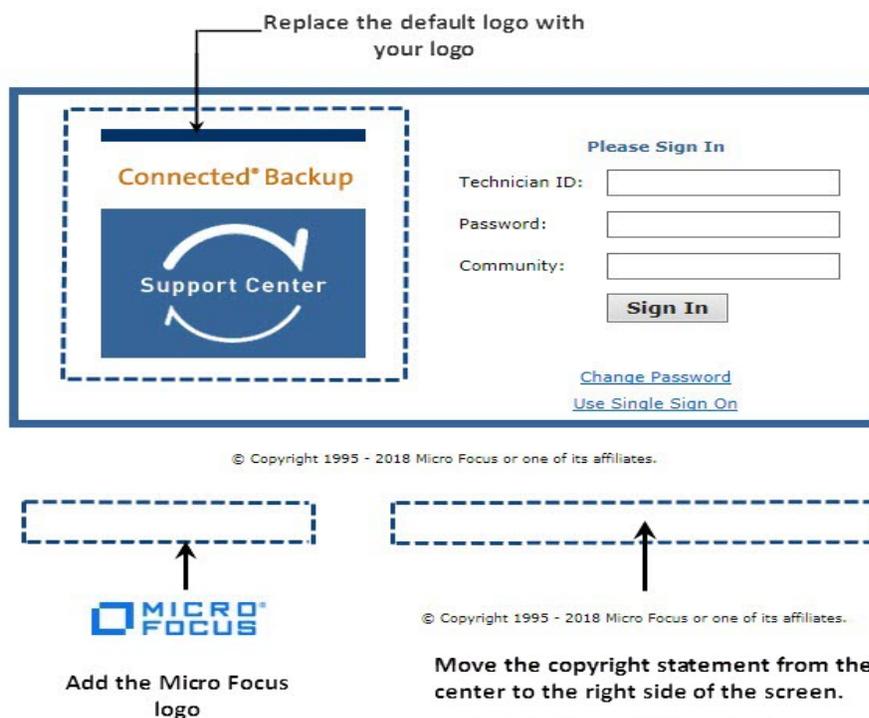
- Sign In page
- Change Password dialog box
- Support Center interface

### Inherited branding

When you brand a community, all of its subcommunities inherit the branding. However, you can brand a subcommunity differently than its parent community. For example, you brand a top-level community to match the corporate branding standards. You can brand a subcommunity under your top-level community to match the branding standards of a wholly-owned subsidiary of your enterprise.

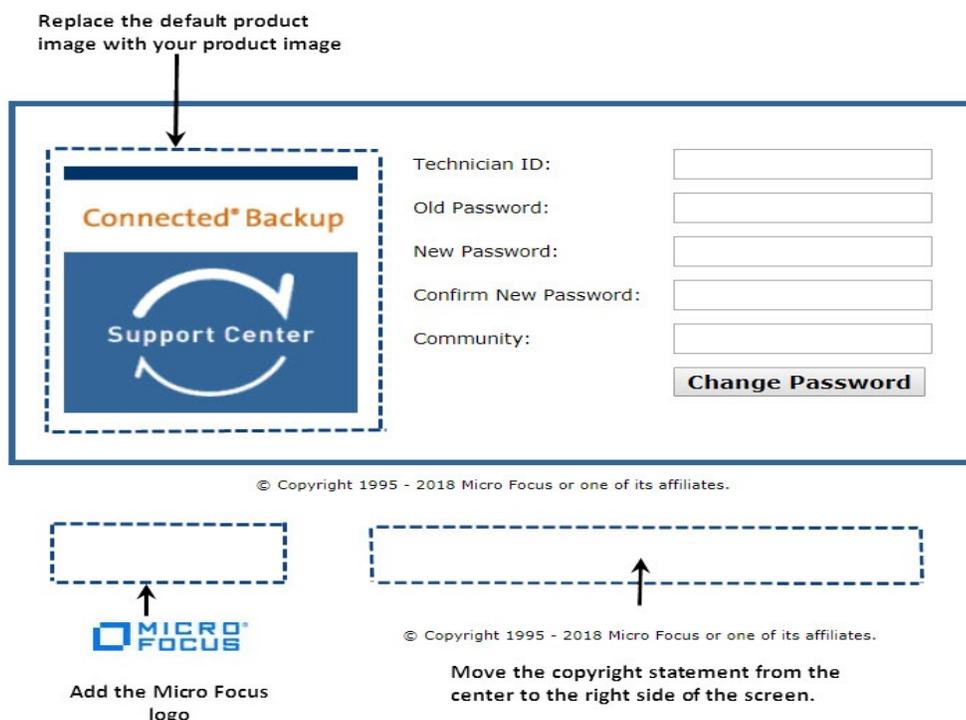
### Brand the Support Center sign in page

The following figure shows which elements you can brand in the Support Center sign in page:



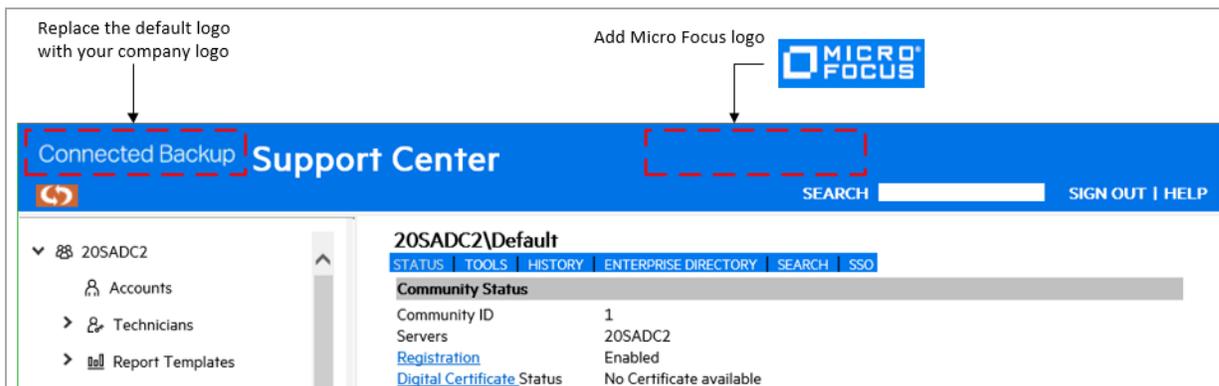
### Brand the Change Password Dialog Box

The following figure shows which elements you can brand in the Change Password dialog box:



## Brand the Support Center Interface

The following figure shows which elements you can brand in Support Center:



## Branding Options for the Account Management Website

You can brand the following elements in the Account Management Website:

- Logos
- Website name

## Brand product components

This section explains how to brand Connected Backup product components. It also describes the requirements for branding graphic elements.

### Requirements for Agent graphics

The following table lists the requirements for each graphic element that you can brand.

Branded graphic element	Requirements
Product logo in the Agent User interface (includes the About window)	<b>Format:</b> PNG (Portable Network Graphics). <b>Size:</b> 330 pixels wide by 60 pixels high. <b>Background:</b> Transparent or white.

### Requirements for Support Center graphics

The following table lists the requirements for each graphic element that you can brand in the Support Center application:

Branded graphic element	Requirements
Product logo in Support Center	<b>Format:</b> GIF (Graphics Internet Format). <b>Size:</b> 159 pixels wide by 40 pixels high. <b>Background:</b> Transparent or white. <b>Recommendation:</b> Center the logo within the 159 by 40 pixel image to ensure the appearance is balanced.
Product logo in the Support Center logon page	<b>Format:</b> GIF (Graphics Internet Format). <b>Size:</b> 170 pixels wide by 181 pixels high. <b>Background:</b> Transparent or white. <b>Recommendation:</b> Include the phrase, "Support Center" as part of the image.

### Requirements for Account Management Website Graphics

The following table lists the requirements for each graphic element that you can brand in the Account Management Website:

Branded graphic element	Requirements
Product logo in the Account Management Website	<b>Format:</b> PNG (Portable Network Graphics). <b>Size:</b> 356 pixels wide by 69 pixels high. <b>Background:</b> Transparent or white. For best results, use white.

## Technician account requirements

To use the branding feature, use a technician account that has Apply Branding and Manage Digital Certificates permission enabled.

For more information about setting permissions for technician accounts, refer to Support Center Help.

## Start the branding process

### To start the branding process

1. Ensure that you have correctly sized image files for each component that you want to brand.  
The image files for the Agent must be in PNG format. The image files for Support Center must be in GIF format. The image files for the Account Management Website must be in PNG format. The Apply Branding page specifies the format that is required for the elements that you can brand.
2. Log on to Support Center. Use a technician ID that has the Apply Branding and Manage Digital Certificates permission enabled.
3. If you use central administration to update deployed Agents, disable it until you verify the appearance of the branded Agents.

For more information, refer to Support Center Help.

4. Select what you want to brand, for example, the Data Center node (if you have permission to gain access to this node), or a community that you want to brand, or a community with Agent configurations that you want to brand.
5. Click **Tools > Apply Branding**.  
The Apply Branding page opens.
6. Enter the required information and click **Apply**.

Support Center displays the following message:

```
Community Successfully Branded. New branding settings were applied to the community. Any subcommunities without customized branding will use this community's branding. The dctomcat service can now be restarted to see any changes to Account Management branding, otherwise branding changes will refresh automatically in five minutes.
```

7. To close the message, click **OK**.

For more information about how to use the Apply Branding page, see Support Center Help.

**NOTE:**

To brand Agents that are already deployed, you must perform one of the following procedures:

- Use Support Center to enable Central Administration. When you change the branding of an Agent community, the next time an Agent in the community synchronizes with the Data Center during a backup, the Agent receives the new branding. For more information, see *Installing Agents*.
- Use the Agent Installation command-line interface to upgrade Agents with an Agent Setup file that contains new branding. For more information, refer to *Installing Agents*.

## Gain access to branding communities

If you brand Support Center at the Data Center level (if you host your Data Center), log on to Support Center to view your customized branding.

If you brand a community, use the URL for the branded community to view your customized branding. Support Center displays this URL after you brand a community and at the top of the Apply Branding page.

**NOTE:**

Sign in to Support Center as technician for the community that you want to brand, and not as a technician for the root community.

# Chapter 7: Deploy Account Management Website

This chapter explains how to deploy and use the standard Account Management Website. If you plan to create a custom Website, see *Account Management Web Services Development*.

- [Overview of Account Management Website, below](#)
- [Deploy Account Management Website, on the next page](#)
- [Account credentials, on page 70](#)
- [Account Management Website Interface, on page 70](#)
- [MyRoam , on page 74](#)

## Overview of Account Management Website

Account Management Website lets users download Agent Setup files, manage their account information, and retrieve files (if you use Support Center to enable MyRoam).

Connected Backup has two types of Account Management Websites:

- **Standard Account Management Website.** If you manage your Data Center, you install the standard Account Management Website when you install the Data Center and Support Center software.
- **Custom Account Management Website.** You use the Account Management Web Services and your development tools to create a custom Website. For more information, refer to *Account Management Web Services Development*.

If you use a Data Center that another company manages, they must provide you with the URL to gain access to Account Management Website.

**NOTE:**

The URLs for Account Management Website are case-sensitive.

The standard Account Management Website includes the following features:

- Account registration
- Agent software downloads
- Profile editing, including user password reset
- Connection to the MyRoam application for file retrieval
- Reinstallation of Agent software for account recovery

# Deploy Account Management Website

## To deploy Account Management Website

1. Install the Data Center software on the primary Data Center server.  
For more information, see *Installing the Data Center*.
2. Designate a server to host the Account Management Website software.  
For more information about system requirements, refer to *Installing the Data Center*.
3. To install the standard Account Management Website on the designated server, run Data Center Setup and select **Install Website with MyRoam**.  
For more information, refer to *Installing the Data Center*.  
For more information about creating a customized Website, refer to *Account Management Web Services Development*.
4. If necessary, edit the terms of use and privacy statements in the Website.
5. Create Agent configurations in Support Center.  
For more information, see [Create Agent configurations, on page 40](#).
6. If necessary, set the default URL for the Registration and Logon pages.
7. Distribute the Registration URL for the Website to users.  
Support Center displays this URL on the Edit Agent Configurations page in the **Mac Configurations** node. When users go to this URL, they can register an account and download the Agent software.

### NOTE:

The URLs for Account Management Website are case-sensitive.

## Ensure security

When a user with either native or enterprise directory account credentials connects to the Account Management Website (AMWS) through a Web browser and receives account information, the Web browser transmits the user's password to the Web server unencrypted. Therefore, if you support native or enterprise directory accounts, ensure that your Web server is secure unless you restrict Web access to a private network. For single sign-on accounts, AMWS does not receive or transmit the user's credentials, the third-party identity provider handles all authentication.

## Edit the Terms of Use and Privacy pages

By default, the **Terms of Use** and **Privacy** links in the generic Account Management Website display content. If you host your Website, change the terms to meet the legal requirements of your company.

### To edit the Terms of Use and Privacy statement

1. Log on to the server where you installed the standard Account Management Website.
2. Go to the following folder:  

```
\Datacenter\apache-tomcat-9.0.37\webapps\ssws\common
```
3. Use any HTML or text editor to edit the following files:
  - `policy.html`. This page contains the privacy statement content.
  - `terms.html`. This page contains the terms of use content.

## Set the Default URL for Registration and Sign In

When you create Agent configurations and Profile and Website settings in Support Center, Support Center generates URLs for the Account Management Website Registration and the standard Sign In pages. Whether these URLs are resolvable names depends on your network settings. You can use Data Center Management Console (DCMC) to set the protocol, computer name, and domain name portions of the URL.

For more information about how to set the URL, refer to DCMC Help.

## Set up user access

Users open Account Management Website in the following ways:

- Enter the URL of the sign in page in a Web browser.

After you install the Account Management Website, send the URL of the Website to your users. Support Center displays the default Website URL in the **General** page of the **Profile and Website Settings**. You can use the default URL or you can specify a URL of a different Web server.

#### **NOTE:**

The URLs for Account Management Website are case-sensitive.

- In the Agent User interface, click **Tools > Account Online**.

To enable this option, configure the Agent to allow access to the Account Management Website from the Agent User interface.

To sign in to Account Management Website, users must enter their Connected Backup account credentials. For more information, see [Account credentials, on the next page](#).

## Set up technician access

Technicians can gain access to the Account Management Website from the Account Summary page in Support Center. When technicians click the link to Account Management Website from the Account Summary page, they sign in as the account user and can use the same features as the user. Only

technicians with permission to access users' data have access to the link. For more information about how to specify technician permissions, see Support Center Help.

## Account credentials

During registration, Account Management Website (AMWS) prompts for Connected Backup account credentials. Which of the following types of credentials a user enters depends on the type that his or her community uses:

- **native Connected Backup account credentials.** The user enters an e-mail address and password to register his or her account. AMWS also prompts for user profile information and stores it along with the credentials in the user's profile.
- **enterprise directory credentials.** The user enters the credentials for his or her enterprise directory account. AMWS loads account information from the enterprise directory and stores it in the user's profile. However, it does not store the enterprise directory account credentials.
- **single sign-on (SSO) credentials.** The user enters the credentials required by his or her single sign-on network account. AMWS does not load or store account information or credentials from the SSO network account.

To sign in to AMWS after the registration process, users must enter their credentials. Users can specify the same account credentials for more than one account. If they do, after they sign in, AMWS prompts them to select which account to access. Users can sign in to and view only one account at a time.

## Account credential management

Connected Backup provides two ways to update the credentials of users in a community that uses native Connected Backup accounts:

- Users can modify their own credentials through Account Management Website  
For more information about how to edit profiles, refer to Account Management Website Help.
- Technicians can modify a user's credentials through Support Center.  
For more information about how to set passwords and change the contact information, refer to Support Center Help.

However, Connected Backup does not support credential management for users in a community that maps accounts to either an enterprise directory or single sign-on accounts. To modify credentials for these types of accounts, users must either contact their system administrator or change the values in their enterprise directory or SSO system.

## Account Management Website Interface

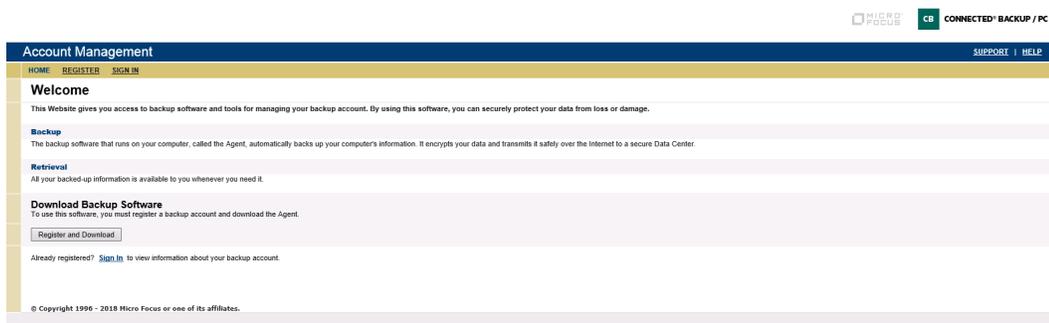
The standard Account Management Website displays the following Web pages:

- Welcome
- Registration
- Sign In
- Summary

Because you can customize any page in the web site, your website might be different from the examples in this section.

## Welcome page

The following figure shows the Welcome page that users see when they open the Account Management Registration URL.



## Registration page

The following figure shows the Registration page that users with native Connected Backup accounts see when they start the registration process.

**Account Management** [SUPPORT](#) | [HELP](#)

1. REGISTER 2. DOWNLOAD and INSTALL

## Registration - Enter Registration Information

**\* Indicates required fields.**

**Name**

\* First name:

Middle name:

\* Last name:

**Sign-In Information**

\* Email address:   You need an email address to access your account online.

\* Password:   Passwords are case sensitive and must contain at least 6 characters.

\* Confirm password:

**Contact Information**

Company:

Country:

Address line 1:

Address line 2:

Address line 3:

City:

State:

Zip Code:

Phone number:

© Copyright 1996 - 2018 Micro Focus or one of its affiliates.

## Sign In page

The following figure shows the standard Sign In page. Users with native Connected Backup credentials or enterprise directory credentials see this page when they go to the Account Management Website URL after they register and install an account.

The screenshot shows the 'Account Management' website interface. At the top, there is a dark blue header with the text 'Account Management' on the left and 'SUPPORT | HELP' on the right. Below the header is a yellow horizontal bar. The main content area has a white background with a 'Sign In' heading. Below the heading, there is a text prompt: 'To sign in using your SSO account credentials, use the [SSO Sign In page.](#)'. This is followed by a form with two input fields: 'Email Address:' and 'Password:'. The 'Password:' field has a 'Forgot password' link to its right. Below the password field, there is a note: '(Passwords are case sensitive.)'. At the bottom of the form is a 'Sign In' button. At the very bottom of the page, there is a copyright notice: '© Copyright 1996 - 2018 Micro Focus or one of its affiliates. Version 8.10'.

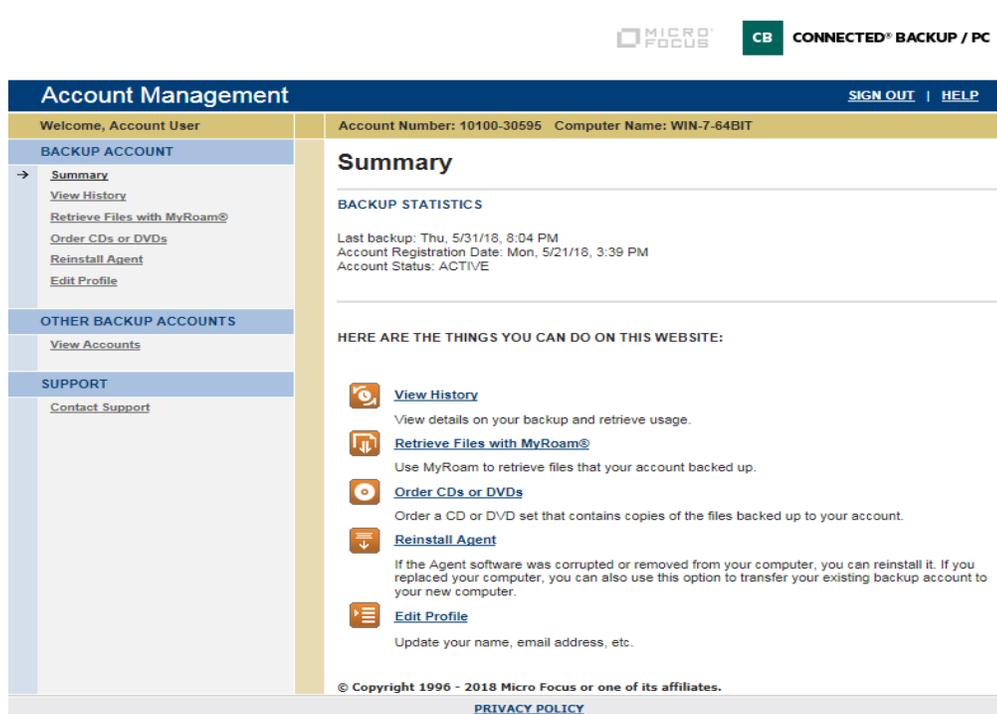
For users who access their Connected Backup account using SSO credentials, Account Management Website displays their corporate SSO Sign In page. If for some reason AMWS does not automatically display the SSO Sign In page, users can do the following to display it:

1. Click **SSO Sign In page**.
2. Type the unique SSO Provider ID that Connected Backup uses to identify the corporate Identity Provider (IdP) for the user's account, and then click **Go**.

If the user does not know this ID, they should contact their system administrator.

## Summary page

The following figure shows a typical Summary page that users see after they sign in to the Account Management Website. The exact options available depend on the Agent configuration and Connected Backup account of the user.



## MyRoam

MyRoam lets users retrieve backed-up files to any computer without using the Agent User interface. To access MyRoam, a user must sign in to Account Management Website. After the user selects files to retrieve, the Data Center creates a ZIP archive file that contains the selected files. The user downloads this file, and then extracts it to a location on his or her computer.

### NOTE:

Users cannot retrieve files if the ZIP archive file is larger than 2 GB. If MyRoam determines that the ZIP will be larger than 2 GB, it prompts the user to clear some files from the retrieval set, and then try to retrieve files again.

If you initiate the retrieval from a computer with a different type operating system than the computer on which the Agent account resides, the Data Center creates a ZIP file that contains only the files that you selected. The ZIP file does not retrieve the metadata associated with the files.

If you initiate the retrieval from a computer that runs the same type operating system as the computer on which the Agent account resides, the Data Center creates a ZIP file that contains the following files:

- MyRoam\_Expander file
- A message file
- A data file

The MyRoam\_Expander file is an executable file that retrieves your files along with metadata that is associated with the files.

For example, if you use Safari on a Mac computer to download files from an Agent account on a Windows computer, the Data Center creates a ZIP file that contains only the files that you selected for retrieval. If you use Safari on a Mac computer to download files from an Agent account on a Mac computer, the Data Center creates a ZIP file that contains the files that you selected for retrieval and the MyRoam\_Expander executable file. You extract the contents of the ZIP file, and then double-click MyRoam\_Expander.

To access MyRoam, users must log on to Account Management Website.

## License and permission requirements

To let users use MyRoam, enable MyRoam in the Support Center. You can enable MyRoam in your top-level community. You also can enable or disable MyRoam in individual subcommunities and for individual accounts.

You can enable MyRoam in one or more communities under the following conditions:

- If you host your Data Center, you need to install a license for MyRoam on the Data Center server. If your current license file does not include MyRoam, contact your sales representative to buy this license.
- To enable the MyRoam feature in a community, your technician account must have **Permission to Allocate Licenses to Sub-communities** enabled.
- To enable MyRoam for specific Agent configurations, your technician account must have **Modify Agent Configuration** enabled.

## MyRoam installation

The MyRoam installation is part of the Account Management Website installation. To install MyRoam, run Data Center Setup and select **Install Website with MyRoam**. For information on how to install software on the Data Center server, refer to *Installing the Data Center*.

## Enable MyRoam

You must enable MyRoam for each community and each configuration in the community that needs access to this feature.

### To enable MyRoam

1. Sign in to Support Center. Use a technician ID that has the Allocate Licenses to Sub-Communities and Modify Agent Configurations permissions enabled.
2. Select the community where you want to enable MyRoam.
3. On the Community Status page, click **Manage Features**.
4. On the Manage Features page, locate the row for the MyRoam feature, and then in the **Settings** column, click **Enabled**.

5. Click **Save**.
6. Expand the **Configurations** node.
7. Expand the **Profile and Website Settings** node and select the configuration for which you want to enable MyRoam.

The Edit Profile and Website Settings - General page opens.

8. Select **Options**.

The Edit Profile and Website Settings - Options page opens.

9. In the Account Management Options section, select **Allow end users to retrieve files using MyRoam**.

10. Click **Finish**.

## Enable MyRoam for individual accounts

After you enable MyRoam at the community and configuration level, you can enable it for individual accounts or account groups.

### To enable MyRoam for one or more accounts

1. Sign in to Support Center. Use a technician ID that has the Modify Agent Configurations permissions enabled.
2. Search for an account or create an account group.
3. Select **Tools > Change MyRoam State**.
4. Select the check box to enable MyRoam, and then click **Save**.

# Chapter 8: Agent interfaces

This chapter explains the interfaces that you can use to install and configure Agents.

- [Overview of the Agent interfaces, below](#)
- [Agent Startup wizard, on the next page](#)
- [Agent User Interface, on page 80](#)
- [Agent command-line interface, on page 83](#)

## Overview of the Agent interfaces

The Agent includes the following interfaces:

<b>Agent Startup Wizard</b>	A graphical interface that opens when users start their Agents for the first time installation. For more information, see <a href="#">Agent Startup wizard, on the next page</a> .
<b>Agent User interface</b>	A graphical interface that you use to perform the following tasks: <ul style="list-style-type: none"><li>• View a summary of the most recent backup results and the configured backup schedule.</li><li>• View and specify files in the backup set. The backup set contains the files you selected for back up.</li><li>• View and add rules to the Agent rule set.</li><li>• Retrieve files that the Agent previously backed up.</li><li>• View a history of Agent events and operations.</li></ul> For more information, see <a href="#">Agent User Interface, on page 80</a> .
<b>Installation command-line interface</b>	A command-line interface that you use to perform the following tasks: <ul style="list-style-type: none"><li>• Install an Agent</li><li>• Remove an Agent</li><li>• Recover an Agent</li><li>• Upgrade an Agent</li></ul> For more information, refer to <i>Installing Mac Agents</i> .
<b>Agent command-line interface</b>	A command-line interface that you use to perform the following tasks: <ul style="list-style-type: none"><li>• Activate Agents</li><li>• Update account profiles</li></ul> For more information, see <a href="#">Agent command-line interface, on page 83</a> .

## Agent Startup wizard

The Agent Startup Wizard is a graphical interface that, if enabled, guides users through set up or recovery of Agent accounts. The Agent Startup Wizard runs under the following circumstances:

- Users start an Agent for the first time after installation.

The Support Center technician must enable the Agent Startup Wizard. For more information, refer to Support Center Help.

- Users start an Agent from a disk image.

The technician who creates the disk image must create one with a running daemon. For more information, refer to *Installing Mac Agents*.

Support Center technicians enable the Agent Startup Wizard. For more information, refer to Support Center Help.

## Startup Wizard main pages



When a user starts the Agent for the first time, the Startup Wizard displays a Welcome page that describes the purpose of the Agent and the Wizard.



The user selects one of the following options:

- Create a new backup account
- Recover an existing Agent account

Create account flow...

Recover account flow...

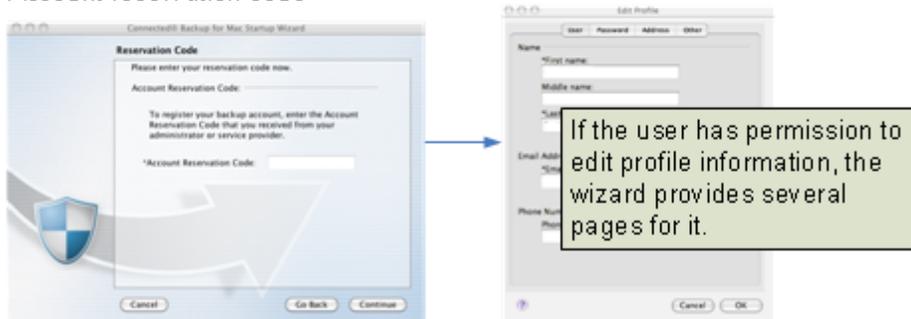
## Startup Wizard – Create Account option

Depending on Agent configuration, the wizard prompts for one of the following:

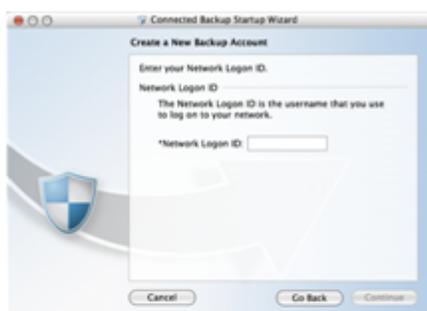
- Profile information (no account reservation code)



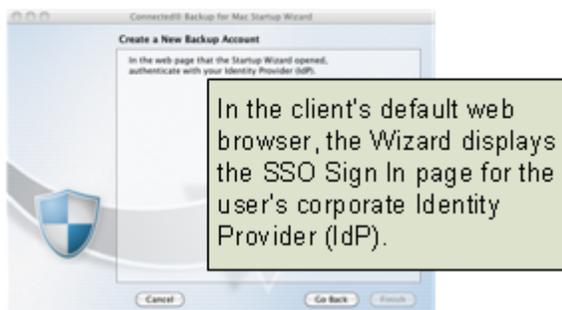
- Account reservation code



- LDAP network login credentials



- Single sign-on (SSO) credentials



## Startup Wizard – Recover Account Option

Prompts for Agent account number and credentials to recover the account:

- Native and LDAP accounts



- Single sign-on (SSO) accounts



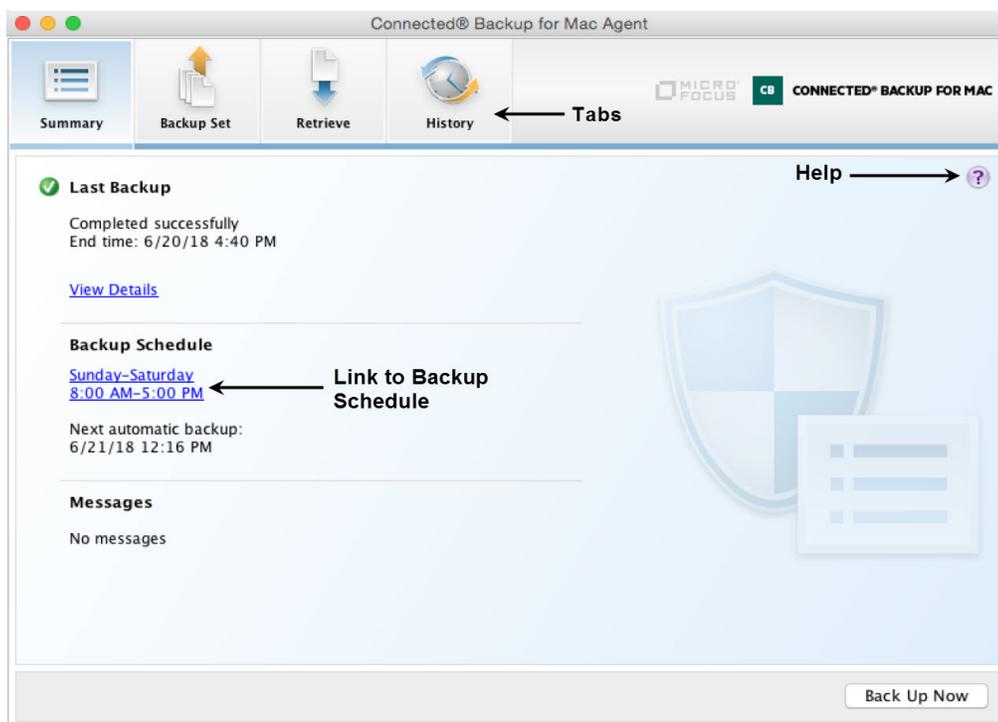
## Agent User Interface

You use the Agent user interface to perform the following tasks:

- View a summary of the most recent backup results and the configured backup schedule.
- View and specify files in the backup set. The backup set contains the files you selected for backup.
- View and add rules to the Agent rule set.
- Retrieve files that the Agent previously backed up.
- View a history of Agent events and operations.

## Agent Main window

The following figure shows the main window that the Agent displays when you open the Agent:



## Agent user interface components

The following table describes the components of the Agent user interface.

Component	Description
<p>Tabs</p>	<ul style="list-style-type: none"> <li>• <b>Summary.</b> Displays a summary of the results of the last backup and the backup schedule.</li> <li>• <b>Backup.</b> Lists the files that the Agent selects for backup. You can select or clear files in this panel.</li> <li>• <b>Retrieve.</b> Displays a list of files that you can retrieve. You can select one or more files for retrieval.</li> <li>• <b>History.</b> Displays event messages.</li> </ul> <p>For more information, see the online Help for each tab.</p>
<p>Connected Backup Menu</p>	<ul style="list-style-type: none"> <li>• <b>About Connected Backup.</b> Displays the software version number and copyright information.</li> <li>• <b>Preferences.</b> Lets users perform backups over dial-up</li> </ul>

	<p>connections and change the backup mode to either passive or aggressive.</p> <ul style="list-style-type: none"> <li>• <b>Services.</b> Lets you use features of other applications without opening the applications themselves.</li> <li>• <b>Hide Connected Backup.</b> Hides the application window.</li> <li>• <b>Hide Others.</b> Hides all application windows other than the one that is selected.</li> <li>• <b>Show All.</b> Shows all open application windows.</li> <li>• <b>Quit Connected Backup.</b> Closes the application.</li> </ul>
File Menu	<ul style="list-style-type: none"> <li>• <b>Back Up Now.</b> Lets you start a back up manually. The Agent backs up all new or changed files in the back up set.</li> </ul>
Tools Menu	<ul style="list-style-type: none"> <li>• <b>Backup Schedule.</b> If you configure the Agent to let users edit the backup schedule, this option lets users change the dates and times when backups occur.</li> <li>• <b>Advanced Rules.</b> If you configure the Agent to let users edit the backup set, this option lets users select options in the <b>Backup Set</b> tab.</li> <li>• <b>Edit Profile.</b> If you configure the Agent to let users update their profiles, this option lets users enter information in the <b>Edit Profile</b> window.</li> <li>• <b>Manage Account Online.</b> If you configure the Agent to include this link, the link lets users gain access to their account information in the Account Management Website from the Agent User interface.</li> </ul>
Help Menu	<b>Connected Backup for Mac Help.</b> Displays a list of available help topics.
Help buttons	Display information about the Agent interface.

## Use the Agent user interface

The following table explains how to use the Agent user interface:

Goal	Action
Select an Agent function	<p>Click the appropriate tab to perform the following tasks:</p> <ul style="list-style-type: none"> <li>• Select or clear files in the backup set.</li> <li>• Retrieve files.</li> <li>• View the Agent History of events.</li> </ul>

Goal	Action
	<ul style="list-style-type: none"> <li>View a summary of the most recent backup.</li> </ul>
Gain access to online help	<p>To open the Agent help, on the Agent main menu, click <b>Help &gt; Connected Backup for Mac Help</b>.</p> <p>For information about an open tab or window, click the question mark (?) in the tab or window.</p>

## Agent command-line interface

When you install the Agent software, Agent Setup program also installs the Agent command-line interface. You can use the Agent command-line interface to perform the following tasks:

- Activate Connected Backup Agents from a disk image.
- Back up files.
- Retrieve files that the Agent previously backed up.
- Get Agent configuration data.

The following table lists the commands that you can use and where to find additional information about them.

Command	Purpose	Reference
cbactivate	Activates an Agent that an administrator installed from a disk image.	<i>Installing Mac Agents</i>
cbbbackup	Initiates an unscheduled backup. This command is similar to using Backup Now in the Agent User interface.	<a href="#">File backup, on page 85</a>
cbretrieve	Retrieves one or more files from the Data Center or from an account image.	<a href="#">File retrieval, on page 95</a>
cb updateprofile	Updates registration fields according to settings that you specify in an XML file.	<a href="#">Use the UpdateProfile Command, below</a>

## Use the UpdateProfile Command

The UpdateProfile command causes the Agent to update the registration information stored on the Data Center server with information that you specify in an XML file.

### NOTE:

The UpdateProfile command does not support accounts that are mapped to an enterprise directory or use single sign-on credentials.

The UpdateProfile command uses the following syntax:

```
cbupdateprofile -f[ile] filename
```

```
[{-help | -?}]
```

Where *filename* is the full path name to the XML file that contains registration information.

The following table describes the parameter that UpdateProfile uses:

Parameter	Syntax/Description
-f [ile]	<p><b>(Required)</b></p> <p>Specifies the path name of an XML file that you create.</p> <p>Examples:</p> <pre>cbupdateprofile -f "/filename.xml"</pre> <p>Where</p> <p><i>filename</i> is the name of the XML file that contains registration information.</p> <p>The following example shows how you can use the UpdateProfile command after you recover an account:</p> <pre>sudo path/install ACCOUNTNUMBER=<i>account_number</i> TECHID=<i>technician_id</i> PASSWORD=<i>technician_password</i></pre> <pre>cbupdateprofile -f "/filename.xml"</pre>
[{-help   -?}]	<p><b>(Optional)</b> Displays help for the current command.</p>

For more information on the required fields and the maximum character length for each field in the XML file, refer to *Installing Mac Agents*.

The UpdateProfile command requires all of the registration fields.

If you do not specify information for a registration field (for example, you specify <EmployeeID></EmployeeID>), UpdateProfile clears the field in the Data Center database.

**NOTE:**

The UpdateProfile command overwrites changes that you make to these fields with Support Center.

# Chapter 9: File backup

This chapter explains the process that the Agent uses to upload data from a Mac computer to the Data Center. It also describes the backup settings in Agent configurations.

- [The backup process, below](#)
- [Back up encrypted files, metadata, and attributes, on page 89](#)
- [Backup settings, on page 90](#)

## The backup process

The following actions occur during the backup process:

- The Agent scans the host computer's hard disk and creates a list of files eligible for backup.
- The Agent analyzes the file list to identify any new files or files that have changed since the last backup.
- The Agent connects to the Data Center.
- The Agent transmits files to the Data Center.
- The Agent records the results of the backup.

**NOTE:**

The Connected Backup Agent for Mac has a selection and backup limit of 300,000 files. Selecting more than 300,000 files for backup might cause backup errors and performance degradation.

## Disk scan

When the Agent initiates a backup, either in response to a user request or according to its backup schedule, the Agent scans files on disk drive volumes. The scan excludes removable or network share drives. If your removable drive presents itself to the operating system (OS) as a fixed drive, it may be included in the backup set.

**NOTE:**

A removable drive that meets these requirements must always be connected to your computer in order for it to continue to be protected. If a backup occurs without the drive attached, the system will process the missing drive as deselected and will issue delete records for all data previously protected on this removable drive.

If you use the Agent rule set to exclude specific volumes, the Agent does not scan those drives. If you exclude volumes that have files that you do not need to back up, you reduce the amount of time that is required to back up a computer.

The scan creates a list of the files that are on the computer. The Agent uses the rules in its rule set to determine which files to select for backup. The backup set for the Agent contains all of the selected files in the list.

**NOTE:**

The next backup requires a scan of the entire hard disk under the following circumstances:

- You restart the Agent daemon or the Agent computer.
- The Agent rule set changes.
- The components of the backup set change.
- The files in the backup set have 90,000 or more changes for backup.

## File analysis

During analysis, the Agent reviews the list of files it compiled during the scan and determines whether each file is new, modified, or an exact duplicate of another file on the computer. It also determines whether the user deleted any previously backed-up files. The Agent then performs the actions described in the following table:

File type	Actions
Base	The file is new, and the Agent backed up the file in its entirety. The Agent sends the entire file for back up and designates it as a base file.
Deleted Files	The Agent uses file synchronization to notify the Data Center if a user deleted a previously backed-up file. The Data Center deletes the file after the file expiration rules determine whether the Data Center retains a file in storage.
DeltaBlock	The Agent backs up a modified file from the base file data and saves that file as a <b>delta file</b> .
MDATE	The Agent checks a file modification date (MDATE), size, directory path, and security descriptors to determine whether a file has changed since the last backup session.
SendOnce	If the file has been backed up previously, the Agent does not back up this file because at least one other account has already backed up the same file. SendOnce technology prevents multiple copies a file from being stored on the Data Center.
Size	The original size of the file in KB, MB, or GB before the Agent applied SendOnce, Delta Block, or compression.
Symbolic Link	If the file is a duplicate of another file. The Agent designates a symbolic <b>link</b> to the duplicate file and does not send the file contents.
Touch	The Agent backs up only changes to the file attributes because the data remained the same.

## Modified file identification

The Agent backs up only new files and the portions of files that changed since the last backup. This process ensures complete protection of the files and reduces use of disk space on the Data Center. To determine whether a file changed since the last backup session, the Agent checks the file's modification date (MDATE), size, directory path, and security descriptors.

The Agent determines which portions of the file changed by comparing the digital signature of the file with that of the version on the Data Center. The Agent backs up only the changed portions, or deltas, of these files.

## File preparation

The Agent compresses and encrypts file data before it transmits the data to the Data Center. It uses the ZLIB compression library to compress both base and delta file data and then uses the encryption method that you specified when you registered the Agent to encrypt the data.

## Connection to the Data Center

The following actions occur when the Agent connects to the Data Center:

1. The Agent uses a network connection to connect to the Data Center. When the Agent contacts the Data Center, the Agent account number identifies the Agent.
2. After the Data Center authorizes the connection, the Data Center creates an empty archive for the account and waits to receive files from the Agent.
3. While the Data Center waits to receive files, it downloads a list of expired files to the Agent.
4. The Agent records the file expirations in a local database on the client.
5. The Agent also checks the Data Center to determine which file sets for backup already exist in the SendOnce pool.

If an exact copy of a file exists in the SendOnce pool, the Agent does not send the file's content to the Data Center. Instead, it sends information about the file name and location. The Agent and Data Center can use this information at a later time to retrieve the file content from the SendOnce pool to restore the client's copy of the file.

### **NOTE:**

The Agent initiates connections between the client and the Data Center server. The Data Center never initiates contact with the Agent client. Even when a technician uses Support Center to modify an Agent configuration, the Data Center downloads the changes only after the Agent connects to the Data Center.

## Transmission of files

After the Agent connects to the Data Center, it initiates a backup session. The backup consists of the following tasks:

1. The Agent transmits the digital signature of the file to the Data Center. The Data Center compares this signature with other files in its database. If an identical file exists in its database, the Data Center creates a pointer to the file in the SendOnce pool when it creates the archive for the backup. The Agent does not transmit the file to the Data Center.
2. If the SendOnce does not contain the file, the Agent uses the ZLIB compression library to compress the file.
3. The Agent uses an encryption key to encrypt the file. The Agent generates the encryption key. You cannot view this key.
4. The Agent transmits the compressed and encrypted file to the Data Center.
5. As the Data Center receives the files, it puts them into archives.

For more information, see the *Product Overview* guide.

## Record of backup results

The Data Center transmits an acknowledgement (ACK) or non-acknowledgement (NACK) for each file that it receives or fails to receive from the Agent. The Agent uses these receipts to update the Agent database. To view the results of the backup, view the Agent History in the Agent User interface or Support Center.

### NOTE:

If a backup fails because of a power outage, or a backup daemon fails unexpectedly, the Agent History indicates the failure but does not provide details.

## Outlook for Mac support

The Connected Backup Agent for Mac now supports Outlook 2016 and Outlook 2019 for Mac. To use Outlook with the Connected Backup Agent for Mac, the Mac Agent file set now contains two new rules. In addition, a new procedure now explains how to perform the restore process when you include Outlook in your backup set. To use Connected Backup version 8.5.1 or later, you must restore your Outlook mailbox.

### To restore your Outlook 2016 or Outlook 2019 mailbox

1. Quit all Microsoft applications.
2. Stop the Microsoft Outlook process. To do so, complete the following steps:
  - a. Open the Activity Monitor. To do so, click the Activity Monitor icon in the Dock.
  - b. Locate the Microsoft Outlook process in the Activity Monitor window, and then click **Quit Process**. The **Quit Process** window opens.
  - c. Click **Quit**.
3. Use File Finder to locate the following location, and then rename the Main Profile folder to Main

Profile.old.

Users/\*/Library/Group Containers/\*.Office/Outlook/Outlook 15 Profiles

4. Open the Connected Backup Agent for Mac, and then select the **Retrieve** view.
5. In the **Backed-up Files** pane, locate the Data Records folder for your Identity. The location for the Data Records folder is Users/\*/Library/Group Containers/\*.Office/Outlook/Outlook 15 Profiles/Main Profile/.
6. Select the Data Records folder, and then click **Retrieve**. You receive a prompt to select a retrieve location.
7. Select **Original Location > Retrieve**.
8. Open the Outlook Profile Manager. Select the Main Profile and set it to **Default**. To do so, click **Action**, and then select **Set as Default**.
9. Start Microsoft Outlook. You receive a prompt to repair the application. Click **Repair**.
10. During the Rebuild process, the Outlook Profile Manager creates a new database.
11. Restart Microsoft Outlook.
12. Go to Outlook Profile Manager, and delete the **Main Profile.old** profile that you created earlier.

## Back up encrypted files, metadata, and attributes

You can back up the following types of files:

Data	Description
Encrypted files	The Agent backs up encrypted files using SendOnce and Delta Block technology. You must configure your system to use the NTFS file system when you back up encrypted files. For encrypted files, the Agent does not back up multiple data streams, reparse points, extended attributes, sparse files, or shared file attributes.
Resource forks	When the Agent backs up files that have resource forks, it also backs up the resource fork and, therefore, the structured data within the resource fork.
Open files	The Agent monitors files for changes at all times, whether the files are closed or open. If a file changes during the time that the Agent analyzes it for backup or before the Agent transmits it to the Data Center, the Agent identifies the file to the Data Center as one that the Agent has to back up again. The Agent also adds the following message to the Log file:  The Agent could not back up <file_name> in folder <full_folder_path> because it was modified during backup processing. Close any applications that may be modifying this file and try backing up again.  The Agent attempts to back up the file again during the next backup session.

Security descriptors	<p>Security descriptors prevent unauthorized access to files. Security descriptors include information such as the following:</p> <ul style="list-style-type: none"><li>• Owner of the file</li><li>• Permissions the owner has granted to other users</li><li>• Actions that the file system logs for auditing purposes.</li></ul> <p>If a security descriptor for a file or folder changes, the Agent considers the file or directory to be different from the previous version and backs up the security descriptors for the file or folder. The Agent backs up file content only if the Agent determines that, in addition to the security descriptors, the content changed.</p>
Sparse files	<p>Sparse files contain empty spaces (represented as strings of zeros) along with meaningful data (nonzero data). The file system allocates disk space for the meaningful data but does not allocate space for the nonmeaningful data (the strings of zeros). The file system tracks where the nonmeaningful data belongs. When an application retrieves a file, the Agent can retrieve the data and the strings of zeros. The Agent backs up all allocated blocks in a sparse file. It does not back up the unallocated block. When an application connects to the file, the correct data is available.</p>

**CAUTION:**

Do not include the Time Machine folder in your backup set. If you do, the backup process uses all available memory.

## Backup settings

When you use Support Center to create or modify an Agent, you select backup settings that suit the unique needs of your users. The following table describes the backup settings:

Backup Settings	Descriptions
Backup mode	<p>You can specify one of the following backup modes:</p> <ul style="list-style-type: none"><li>• <b>Passive.</b> The Agent does not retry backups that cannot start because of the following conditions:<ul style="list-style-type: none"><li>◦ Errors.</li><li>◦ The Agent is busy doing a retrieval.</li><li>◦ The computer cannot connect to the Data Center.</li></ul></li></ul> <p>Under these circumstances, the Agent waits for the next scheduled backup, or for a user to initiate a manual backup.</p> <ul style="list-style-type: none"><li>• <b>Aggressive.</b> The Agent retries backup periodically until a successful backup occurs. If a backup attempt generates warnings or errors, the Agent does not retry backup.</li></ul>

<p>Backup limits</p>	<p>You can limit the size of the backup set for each Agent configuration.</p> <p>You can limit the size of backups in the following ways:</p> <ul style="list-style-type: none"><li>• On the Agent computer, set a size limit of the backup set in megabytes or gigabytes. For example, you can set the backup set size limit to 30 GB.</li><li>• Configure the Agent to display a warning message when the backup set reaches a specified percentage of its limit. For example, you can configure the Agent to display a warning when the backup set size is 90% of the allowed size limit.</li></ul>
<p>Backup permissions</p>	<p>You can configure Agents to let users have the following permissions:</p> <ul style="list-style-type: none"><li>• Modify their backup sets. If you enable this permission, users have access to user-configurable backup options such as the backup mode settings.</li><li>• Allow backup over dial-up connections.</li><li>• Let users edit their backup schedules in the Agent User interface.</li></ul>
<p>Backup schedule</p>	<p>You can select one of the following backup schedules:</p> <ul style="list-style-type: none"><li>• <b>Automatic on specific days and times</b> (default). Starts a backup during the same time period each day. For example, the Agent can perform a backup each night between midnight and 6:00 A.M. You can select only a range of time and not an exact time for the backup. The Agent determines when to perform the backup within the range that you specify. This behavior balances network traffic.</li><li>• <b>Manual backup</b>. Starts a backup only when a user initiates it.</li></ul>
<p>Agent rule sets</p>	<p>To determine which files to select for backup, create rule sets. To create rule sets, use the Agent Rules wizard in Support Center.</p> <p>New Agent installations include configured rules. If you change the rules, the Agent receives the changes the next time that it connects to the Data Center.</p> <p>Users can create rules that override some rules in an Agent's default rule set. You can create overriding rules in the following ways:</p> <ul style="list-style-type: none"><li>• Select or remove files on the Backup Set tab in the Agent User interface.</li></ul>

- Use the Advanced Rules option to create rules.

For both options, users must have permission to modify their backup sets, which you set in the Agent Settings component associated with the Agent configuration.

For more information about rule sets, see [Create Agent rule sets, on page 46](#). For more information about how to create rules, refer to Support Center Help.

## Use the Agent user interface to back up files

You can use the Agent User interface to start a backup manually, specify which files are in the backup set, or monitor a backup in progress.

The Agent configuration that you create in Support Center determines how the Agent backs up data. The configuration includes all of the backup settings and versions for the Agent.

For more information about how to create Agent configurations, refer to Support Center Help.

### Backup Set tab

You can use the Backup Set tab to change the file selection for the backup set or start a backup manually. For more information, refer to Agent Help.

### Summary tab

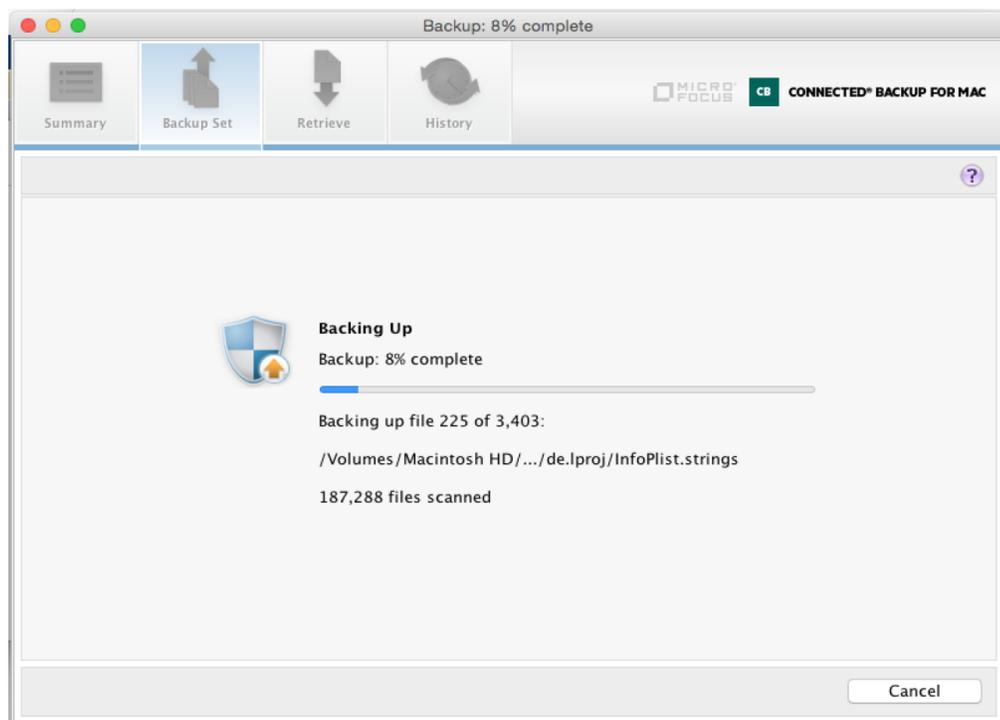
**You can use the Summary tab to start a backup and view History details about the last backup that the Agent performed.**

## Backup monitoring

If you configure the Agent to use a predetermined schedule, you do not need to open the Agent User interface. The Agent scans the system's hard disk and identifies which files to back up.

If you want to monitor progress of a backup, open the Agent User interface while the backup is in progress. The Agent displays a progress window that indicates the state of the backup. The Agent disables all other tabs and options. You can check the Agent history to determine the outcome of a backup that is complete.

The following figure shows the Agent User interface while a backup is in progress:



## Back up files using the Backup command

Rather than wait for a scheduled backup, you can use the Backup command from the Agent command-line interface to start a backup. This command is equivalent to **Backup Now** in the Agent User interface.

The Backup command backs up files based on the backup settings in the Agent configuration. You cannot use the Backup command to specify a specific file for backup.

Also use the Backup command if you use scripts to automate computer management or if you must manage computers from remote locations.

For more information about how to gain access to the Agent command-line interface, see [Agent interfaces, on page 77](#).

## Backup command syntax

The backup command uses the following syntax:

```
cbbackup
```

```
[{-firstbackup | -b}]
```

```
[{-register | -r}]
```

```
[{-endpoint | -e} url]
```

```
[-help | -?]
```

## Backup command options

The Backup command has the following options:

Option	Description
[{-firstbackup   - b}]	<b>(Optional)</b> Initiates a first backup after you install the Agent.
[{-register   -r}]	<b>(Optional)</b> Performs account registration.
[{-endpoint   -e} <i>url</i> ]	<b>(Optional)</b> Specifies the service end point. The default value is <code>http://localhost:16386/</code> .
[-help   -?]	<b>(Optional)</b> Displays help for the current command.

## Backup command example

The following example is a command that starts the first backup after you install the Agent.

```
cbbackup -firstbackup
```

The Agent uses the rules in its configuration to select files for backup.

# Chapter 10: File retrieval

This chapter explains how to retrieve files from the Data Center and from media.

- [The Retrieval Process, below](#)
- [Support for encrypted files, metadata, and attributes, on the next page](#)
- [Retrieve files using the Agent user interface, on the next page](#)

## The Retrieval Process

The following actions occur during the retrieval process:

1. The Agent connects to the Data Center to initiate a retrieval request.
2. The Data Center receives the request and packages files from one or more archives.
3. The Data Center compresses and encrypts the packaged files, and then downloads them to the Agent.
4. The Agent decompresses and decrypts the files.
5. The Agent distributes the files to the destination folders, and then applies conflict resolution rules.

## File repackaging

Many files that you retrieve have multiple versions backed up on the Data Center. These backups contain incremental changes, or deltas, that the Data Center stores in one or more archives.

During a retrieval, the Data Center collects the archives that it needs to reconstitute the requested version of the files from its server and, if applicable, from its auxiliary storage devices. The Data Center extracts the required base and delta files from the archives. It then merges them to create the file or files that the Agent requested. Before the Data Center downloads the files to the Agent, the Data Center compresses and encrypts the files again for security.

## E-mail notification

You can configure the Data Center to send an e-mail message to the Agent e-mail address when anyone retrieves files for an account that is registered in a specific community.

E-mail notification contributes to security. When a technician knows about a file retrieval, the technician can act appropriately if an unauthorized person retrieves the files.

You enable e-mail notification through Support Center at the Data Center, community, or subcommunity level. You cannot restrict e-mail notification to specific Agent configurations. You can enable e-mail notification for the entire Data Center or specific communities. For more information about how to enable e-mail notification, see Support Center Help.

## Support for encrypted files, metadata, and attributes

This section describes how Connected Backup supports encrypted files, metadata, and attributes during file retrievals.

### Retrieval of sparse files

During a retrieval, the Agent restores sparse files and all allocated sparse data that was previously backed up.

### Retrieval of resource forks

When the Agent retrieves files that have resource forks, it retrieves the resource forks and the structured data that the resource fork contains.

### Retrieval of open files

The Agent can replace a file that is open with advisory locking at the time of retrieval.

If you try to retrieve a file while it is open with advisory locking, and you selected the **Overwrite the files currently on my computer** option, the Agent renames the file that it retrieves from the Data Center. When the Agent renames files, it adds the word Restored and a number to the end of the file name.

The Agent also generates an event in Agent History to indicate that it retrieved and renamed the file. The Agent also writes the following message to the Agent log file:

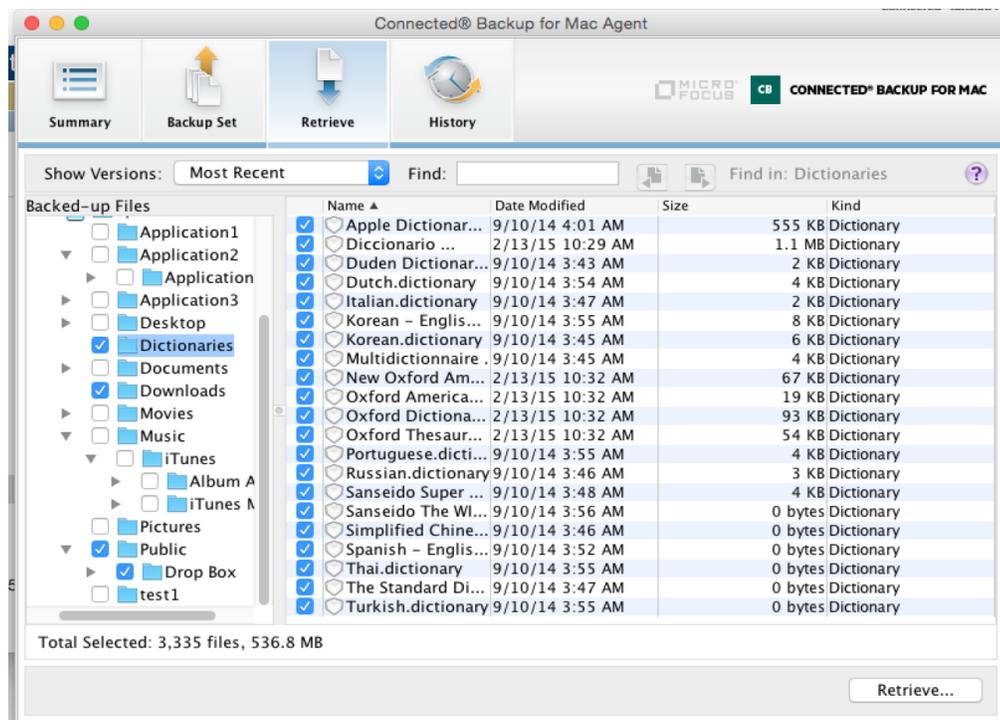
```
The Agent could not overwrite file <file_name> because it was open by another application or process. The file was retrieved as <file_name Restored x>.
```

## Retrieve files using the Agent user interface

When the Agent retrieves files, it uses the Agent account number to authenticate to the Data Center. The Agent submits the retrieval request to the Data Center and waits to receive the files. For more information about the Agent User interface, see [Agent interfaces, on page 77](#).

### Retrieve tab

The following figure shows the Retrieve tab with a list of retrievable files.



## Retrieve permissions

The Retrieve permissions that you set in the Agent configuration determine whether users need to provide credentials to gain access to the Retrieve tab. When you create Agent settings, you can specify one of the following actions:

- Do not require a password to retrieve files.
- Require a password to retrieve files. The password is the password associated with the account.

If you configured the Agent to require credentials, the Agent prompts the user for this information before it opens the Retrieve tab.

## File selection

By default, the Agent's Retrieve tab lists the most recent versions of files that the Agent created during the last backup. You can also display You can use these options to retrieve earlier versions of files as well as the most recent ones.

To select files that you want to retrieve, select the check box next to each folder or file.

For more information about how to select files, see Agent Help.

## Destination options

After you select files to retrieve, the Agent displays the Agent Options window. On the Agent Options window, you can select any of the following options as destinations for retrieved files:

- **New Location.** Lets you specify a new location for the retrieved files.
- **Original Location.** Restores the selected files to their original locations. During the Retrieve, the Agent adds missing folders as needed to recreate the original locations.

## File name conflict options

In addition to using the Agent Options window to select destinations for retrieved files, you can specify how to rename files in case a file name conflict occurs. You can choose either of the following options:

- **Rename the files being retrieved.** Renames a file when the destination folder contains a file with the same name, and adds a number to the end of the file name when it renames files.

For example, if you retrieve a file named `Report.doc` and this file exists in the destination folder, Retrieve would rename the file to `Report1.doc`. This option is available only if you select **Original Location**.

- **Overwrite the files on my computer.** Overwrites files on your computer if the retrieved files have the same name as existing files. This option is available only if you select **Original Location**.

## Retrieve files using the Retrieve command

To use the Agent command-line interface to retrieve backed up files from the Data Center, issue the Retrieve command.

### NOTE:

The Retrieve command does not support single sign-on (SSO) credentials. Therefore, if a user in an SSO community has an Agent Configuration that requires a password for retrievals, he or she cannot use the Retrieve command to retrieve files. However, a technician can use the Retrieve command to retrieve files on the user's behalf. To do so, the technician must use the Retrieve command with a Technician ID that meets the following criteria:

- has native Connected Backup credentials or is mapped to an enterprise directory
- has permission to access the SSO community in which the user's account resides

After you issue the Retrieve command, the Agent connects to the Data Center and uses its account number to authenticate. The Agent submits the retrieval request to the Data Center and waits to receive files.

If a file that the Agent retrieves has the same name as a file in the destination folder, the Agent renames the file in the destination folder. For more information about how to gain access to the Agent command-line interface, see [Agent interfaces, on page 77](#).

Use the Retrieve command in the following situation:

- You use scripts to automate computer management or to manage computers from remote locations.

For more information about performing command-line installations, see *Installing Mac Agents*.

## Retrieve command syntax

The Retrieve command uses the following syntax:

```
cbretrieve  
{-date | -d} YYYY-MM-DD  
{-time | -t} HH:MM:SS  
[{-backupdates | -bd}]  
(-techid | -id} technician_ID  
{-password | -pw} technician_password  
[{-destination | -dp} path]  
[{-source | -s} source_path | {-alldata | -a}]  
[{-norecurse | -nr}]  
[{-endpoint | -e} url]  
[{-help | -?}]
```

## Retrieve command options

The Retrieve command has the following options:

Option	Description
{-date   -d} YYYY-MM-DD	<p><b>(Optional.)</b> The date of the file that you want to retrieve.</p> <p>If you do not use the <code>-date</code> or <code>-time</code> parameters, the retrieve command retrieves the most recent version of the files.</p> <p>If you use <code>-date</code> with <code>-time</code>, you retrieve files as of the date and time that you specify.</p> <p>If you use <code>-date</code> without <code>-time</code>, you retrieve files as of midnight on the date that you specify.</p>
{-time   -t} HH:MM:SS	<p><b>(Optional.)</b> The time of the file that you want to retrieve. Use a 24-hour time format to specify the time.</p> <p>If you do not use the <code>-time</code> or <code>-date</code></p>

	<p>parameters, you retrieve the most recent version of the files.</p> <p>If you use <code>-time</code> without <code>-date</code>, you retrieve files as of the current date and the time that you specify.</p> <p>If you use <code>-time</code> with <code>-date</code>, you retrieve files as of the date and time that you specify.</p>
<p>[{-backupDates   -bd}]</p>	<p><b>(Optional.)</b> The list of dates and times of the file that you want to retrieve. Use a 24-hour time format to specify the time.</p>
<p>{-techid   -id} <i>technician_ID</i></p>	<p><b>(Required only as indicated.)</b> The ID of a valid user or technician that either has native Connected Backup credentials or is mapped to an enterprise directory.</p> <p><b>NOTE:</b> This option does not support IDs for SSO accounts.</p> <p>Required only as follows:</p> <ul style="list-style-type: none"> <li>• For users, if you run the Retrieve command from a computer that hosts an Agent configured for an account other than your own.</li> <li>• For technicians, it is always required. In addition, the technician account must have permission to access the community in which the user's account resides.</li> </ul>
<p>{-password   -pw} <i>technician_password</i></p>	<p><b>(Required only as indicated.)</b> The password associated with the user or technician account ID.</p> <p><b>NOTE:</b> This option does not support passwords for SSO accounts.</p> <p>Required only as follows:</p> <ul style="list-style-type: none"> <li>• For users, if your Agent Configuration requires passwords for file retrieval. However, if it does, and your account is mapped to an SSO account, you cannot</li> </ul>

	<p>use the Retrieve command to retrieve files.</p> <ul style="list-style-type: none"> <li>• For technicians, it is always required. In addition, the technician account must have permission to access the community in which the user's account resides.</li> </ul>
<p><code>[{-destination   -dp} <i>path</i>]</code></p>	<p><b>(Optional.)</b> Specifies where you want to put the restored files. Use the following syntax:</p> <p><code>drive:\path</code></p> <p>If the original drive does not exist, the Retrieve command creates the following path for the retrieved files:</p> <p><code>@Drive_n\original_filepath</code></p> <p>If you do not specify this parameter, the command restores files to their original locations.</p>
<p><code>[{-source   -s} <i>source_path</i>   {-alldata   -a}]</code></p>	<p><b>(Optional.)</b> Specifies the files that you want to retrieve. You can specify one of the following options:</p> <ul style="list-style-type: none"> <li>• <code>-source   -s:</code>          Specifies the path to the files that you want to retrieve.           You can use the asterisk (*) and the question mark (?) as wildcard characters. The * wildcard matches any combination of characters. The wildcard matches any single character.</li> <li>• <code>-alldata   -a:</code>          Retrieves all data from the backup specified in the <code>-date</code> parameter. This parameter is the default if you do not specify the <code>-source</code> parameter.</li> </ul>
<p><code>[{-norecuse   -nr}]</code></p>	<p><b>(Optional.)</b> Tells the Agent not to retrieve files from lower level subfolders. Use this option with the <code>-source</code> or <code>-s</code> option.</p>

[{-endpoint   -e} <i>url</i> ]	<b>(Optional.)</b> Specifies the service end point. The default value is <code>http://localhost:16386/</code> .
[{-help   -?}]	<b>(Optional.)</b> Displays help for the Retrieve command.

## Examples of how to use the Retrieve command

The following examples show ways that you can use the retrieve command.

### Retrieve a single file

This command retrieves a file named `myfile.doc` from a backup set. The example does not specify a date or time. Therefore, the command retrieves the most recent version of the files. The example does not specify a destination parameter. Therefore, the command restores the file to its original location.

```
cbretrieve -techid supt346 -password 678ioh7 -source /reports/myfile.doc
```

### Retrieve a single file and specify date and time

This command retrieves a file named `myfile.doc` from a backup set with a date of January 15, 2014 and time of 2:15 a.m. The example does not specify a destination parameter. Therefore, the command restores the file to its original location.

```
cbretrieve -date 2014-01-15 -time 02:15:00 -techid supt346 -password 678ioh7 -  
source /reports/myfile.doc
```

### Specify a retrieve location

This command retrieves a file named `myfile.doc` from a backup set with a date and time of January 15, 2014, 2:15 a.m., and saves the file to a folder named `/restore`.

```
cbretrieve -date 2014-01-15 -time 02:15:00 -techid supt346 -password 678ioh7 -  
destination /restore -source /reports/myfile.doc
```

### Retrieve files only in a top-level folder

This command retrieves files in a folder named `/reports`. In this example, the `NoRecurse` parameter indicates that the command does not retrieve files in subfolders.

```
cbretrieve -date 2014-01-15 -time 02:15:00 -techid supt346 -password 678ioh7 -  
destination /restore -source /reports -norecurse
```

## Retrieve all files in a backup set

The command retrieves all files in a backup set with a date and time of January 15, 2014, 2:15 a.m.

```
cbretrieve -date 2014-01-15 -time 02:15:00 -techid supt346 -password 678ioh7 -  
destination /restore -alldata
```

## Retrieve data using MyRoam

MyRoam lets users retrieve backed-up files to any computer without using the Agent User interface. Users must log on to the Account Management Website to have access to MyRoam. After users select the files that they want to retrieve, the Data Center creates a ZIP archive file that contains the selected files. Users download this file and extract it to a location on their computer.

To use MyRoam, the Agent account and the community where the account is registered must have MyRoam enabled.

## The MyRoam retrieval process

The process to retrieve files with the MyRoam application comprises the following steps:

1. You select a backup set that includes the files that you need.
2. The MyRoam application displays a list of files that you can select for retrieval.
3. You select the files that you want to retrieve.
4. The Data Center server creates a ZIP archive file that contains the files that you selected.

If you initiate the retrieval from a computer with a different type operating system than the computer on which the Agent account resides, the Data Center creates a ZIP file that contains only the files that you selected. The ZIP file does not restore the metadata associated with the files.

If you initiate the retrieval from a computer that runs the same type operating system as the computer on which the Agent account resides, the Data Center creates a ZIP file that contains the following files:

- MyRoam\_Expander file
- A message file
- A data file

The MyRoam\_Expander file is an executable file that restores your files along with metadata that is associated with the files.

For example, if you use Safari on a Mac computer to download files from an Agent account on a Windows computer, the Data Center creates a ZIP file that contains only the files that you selected for retrieval. If you use Safari on a Mac computer to download files from an Agent account on a Mac computer, the Data Center creates a ZIP file that contains the files you selected for retrieval and the MyRoam\_Expander executable file.

5. You download the ZIP file to a location of your choice. The ZIP file preserves the folder structure for the files that you selected. Because the folder structure remains intact, you do not have to be concerned with file name conflicts as you would if you were to use the Agent interface to retrieve the files.

**NOTE:** A pop-up message is displayed when you download a file from AMWS (install or reinstall agent) on the host system. Click **Allow** to continue with the download. Clicking **Cancel** disables the download option. Refresh the page. You will not be able to download the file till you click **Allow** in the pop-up message. The pop-up is not displayed again, once you click **Allow**. Following is an example of the pop-up message:  
`"Do you want to allow download on "Testvm1420.testlab.net"?"`

6. You extract the contents of the ZIP file, and then run the MyRoam\_Expander application, if included in the ZIP file.

**NOTE:** MyRoam has a 2 GB data limit. You cannot zip or unzip a file that has an uncompressed data size that is more than 2 GB.

## Files that you cannot retrieve

You can retrieve most backed-up files except for e-mail files that the Agent backed up with the Connected EmailOptimizer technology. You must use the Agent User interface to retrieve these files.

You can retrieve encrypted files. However, MyRoam retrieves encrypted files to an unencrypted state.

**NOTE:** You can retrieve multistream files. However, the MyRoam application retrieves the main data stream only.

## Select files for retrieval

When you select **Retrieve files using MyRoam**, the MyRoam application compiles a list of files that you can retrieve from the Data Center. When the list is ready, the MyRoam application displays a Browse view that lists the files that your Agent previously backed up. The default view for this page shows the latest version of each backed-up file.

### To select files for retrieval

1. To find the files that you want to select, use one of the following methods:
  - Browse.
  - Use a wildcard search.
  - Display specific file versions.
2. Select the check box next to each file that you want retrieve.
3. To start the retrieve process, click **Retrieve**.

### To browse for files

1. To find specific files to select for retrieval, expand the folders in the left pane of the Browse view.
2. To sort the list of files, click any column heading.

An up-arrow in the column heading indicates that the column is sorted in ascending order. A down-arrow indicates that the column is sorted in descending order.

### To use a wildcard search to find files

1. Click **Find**.

The MyRoam application displays the **Find** options.

2. In the **Name contains** field, enter the full or partial name of the file you want to find.

The names are not case sensitive.

You can use the following wildcard characters in the name:

*	Use this character to match zero or more characters. For example, *.doc matches any file that has a file extension of .doc.
?	Use this character to match a single character. For example, ab?.doc matches abc.doc and aby.doc.

3. In the **Look in folder** box, enter the full path for a folder that you want to search, or select a folder in the left pane.

Find searches all folders within the folder that you specify.

**TIP:**

The default location for the **Look in folder** box is the folder selected in the left pane. To change the folder location, select a new folder in the left pane.

4. Click **Find Next**.

In the list below the **Find** options, the Agent highlights the first file or folder that it finds.

5. Do one of the following:
  - Click **Find Next** or use the arrow buttons to highlight the next folder or file that matches the Find criteria.
  - Click **Find Previous** or use the arrow buttons to highlight a previously found file or folder.
6. From the displayed list, select the file that you want to retrieve.
7. To hide the **Find** options, click **X** in the upper right corner of the Find pane, or click **Browse**.

In the **Show** field, the Agent displays the list of files that match the criteria.

### To display different file versions

1. To change the file versions that are displayed in the Browse view, select an option from the **Show versions** list. The list includes the following options:
  - **Most Recent.** Lets you display the backed up files that were on your system at the time of the recent backup. This is the default selection.
  - **As of Backup Date.** Lets you display the backed up files that were on your system at the time of the selected backup date.
  - **All.** Lets you display all versions of the files that are currently stored on the Data Center server.
2. If you selected **As of Backup Date**, select a backup date from the displayed list and click **OK**.

## Retrieve files

After you select the files that you want to retrieve, you are ready to download the selected files.

### To download the selected files

1. In the MyRoam Browse view, click **Retrieve**.

The MyRoam application displays information about the total size of the files that you select for retrieval and the estimated download times for each file. It also includes instructions on how to download the ZIP archive file or Mac executable file that contains your retrieved files.

2. Select the type of file that you want the Data Center to generate:

- a. **Zip file.** Restores data only.

By default, if you initiate the retrieval from a computer with a different type operating system than the computer on which the Agent account resides, the Data Center creates a ZIP file that contains the files that you selected for retrieval. The ZIP file does not restore the metadata associated with the files.

If you initiate the retrieval from a computer with a different operating system than the computer on which the Agent account resides, do not select this option.

- b. **Executable.** Restores data and metadata.

By default, if you initiate the retrieval from a computer with the same type operating system as the computer on which the Agent account resides, the Data Center creates a ZIP file that includes the MyRoam\_Expander file. This executable file restores your files along with metadata that is associated with the files.

3. Click **Download**.
4. In the **File Download** box, click **Save**.
5. In the **Save As** box, specify a location for the ZIP file, and click **Save**.
6. Do one of the following:

- If the ZIP file is a standard one that contains the files that you selected for retrieval, extract the contents of the ZIP file to where you want them on your local computer.
- If the ZIP file contains the `MyRoam_Expander.exe` file, extract the contents of the file to a temporary location, and then do one of the following to run the `MyRoam_Expander` application to restore your files:
  - On computers that run Windows XP, double-click the `MyRoam_Expander.exe` file.
  - On computers that run Windows 7 or Windows 8, right-click the `MyRoam_Expander.exe` file, and then click `Run as administrator`.

The program restores the files to the root of the directory that contains the `MyRoam_Expander.exe` file.

### To use MyRoam to retrieve files

1. Log on to the Account Management Website:
2. Select **Retrieve Files with MyRoam**.
3. Select the files that you want to retrieve, and then click **Retrieve**.

The MyRoam application creates a compressed archive file (ZIP file) that contains all of the selected files.

**NOTE:**

MyRoam has a 2 GB data limit for creating zip files. You cannot zip or unzip a file whose uncompressed data is more than 2 GB.

4. Click **Download** to download the compressed ZIP file.

For more information, see MyRoam Help.

# Chapter 11: Agent history and reports

This chapter explains how to view Agent History and Support Center reports to monitor Agent activity.

- [Agent history, below](#)
- [Support Center reports, on page 111](#)
- [Use the Agent Protocol Session log, on page 115](#)

## Agent history

Use the Agent History to verify successful Agent activity or diagnose a potential problem. The Agent History lets you view details about the following events:

- Account recovery
- Account registration
- Backup
- File list synchronization
- Retrieve

The Agent records details about activities and interactions with the Data Center in a file that you can view on the Agent User interface History tab.

Each event entry contains the following information:

- The type of activity
- The outcome of the event
- The date and time that the activity started and ended

You can export the list of events to XML files that you can send to a technical support representative.

## View Agent history in the Agent interface

View Agent history from the History tab in the Agent interface.

### To view Agent history from the Agent interface

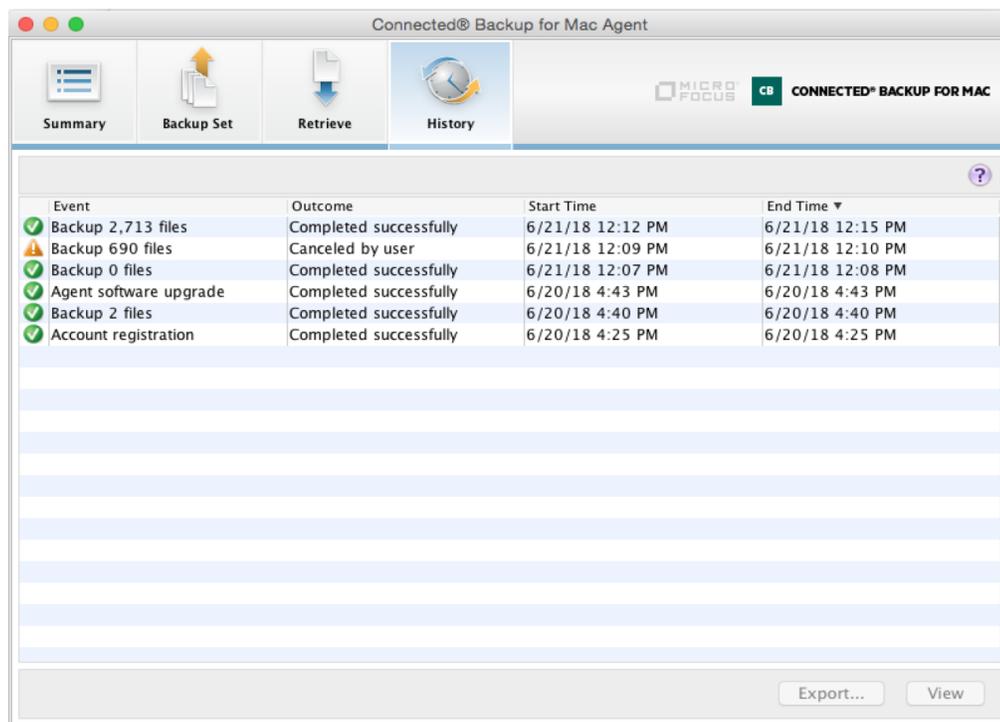
1. Open the Agent interface.
2. Click the History tab.

The History window opens.

### To export the list of events on the History tab to a file

- Click **Export**.

The following figure shows the History tab:



You can view details about a specific event, and export the details to a file.

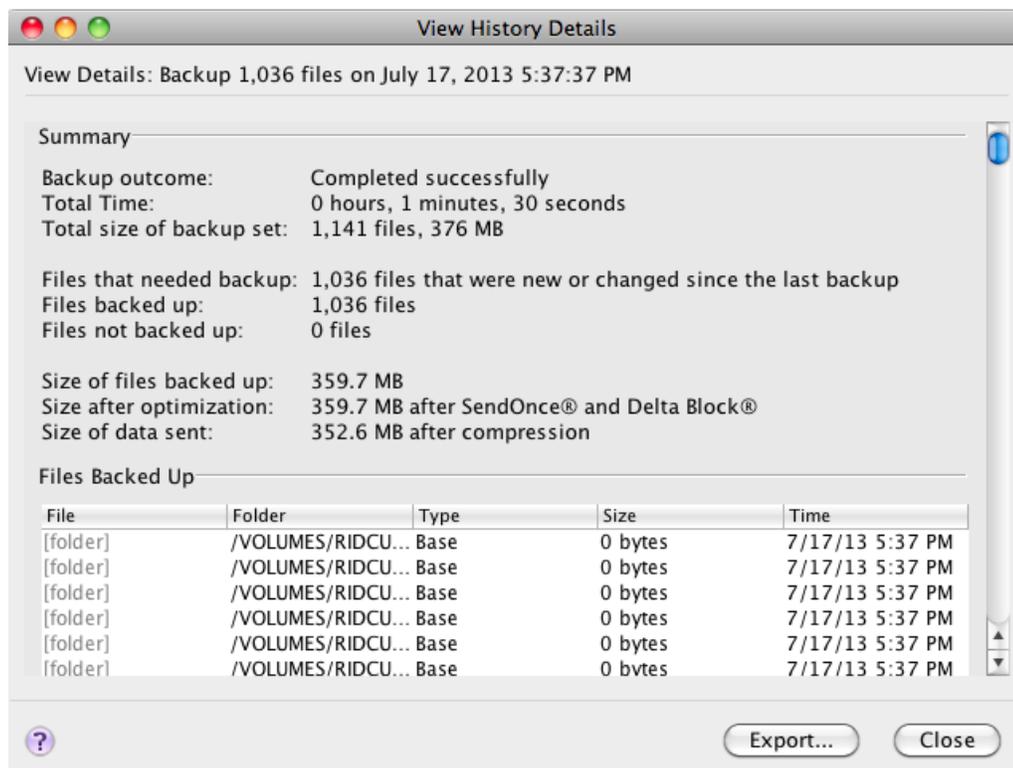
### To view details about an event

1. Open the Agent interface.
2. Click the **History** tab.  
The History window opens.
3. On the History window, select an event.
4. Click **View**.

The View History Details window opens.

5. Optionally, to save the details to a file, click **Export**.

The following figure shows an example View History Details window:



For more information, see Agent Help.

## Viewing Agent History in Support Center

You can use Support Center to view the same list of events that you view in the Agent History tab in the Agent User interface. When you select one or more events, you can display detailed information about each event.

You can also view export details in an export file. If you enable diagnostics for the account, Support Center displays the diagnostic information in the Agent History view. You can export the content to a file that you can e-mail to a technical support representative.

For more information, see Support Center Help.

### To view Agent History from Support Center

1. Open Support Center.
2. Search for the account for which you want to view the Agent History.
3. Click **Tools > View Agent History**.

The View Agent History page opens. The following image is an example of the entries in the View Agent History page:

Event	Outcome	Start Time	End Time
Backup	Failed	1/8/19, 5:44 PM	1/9/19, 5:38 PM
Internal diagnostic	Completed with Errors	1/8/19, 5:33 PM	1/8/19, 5:44 PM
Backup	Failed	1/8/19, 2:16 PM	1/8/19, 5:29 PM
Backup	Completed with Warnings	1/8/19, 1:05 PM	1/8/19, 2:16 PM
Backup	Completed with Warnings	1/8/19, 12:02 PM	1/8/19, 1:05 PM
Backup	Completed with Warnings	1/8/19, 10:46 AM	1/8/19, 12:02 PM
Backup	Completed	1/8/19, 9:44 AM	1/8/19, 10:46 AM
Backup	Completed with Errors	1/7/19, 4:48 PM	1/8/19, 9:44 AM
Backup	Failed	1/2/19, 9:06 PM	1/7/19, 4:37 PM
Internal diagnostic	Completed with Errors	1/2/19, 8:55 PM	1/2/19, 9:06 PM

4. To display the details for a particular event, select the event and click **View**.
5. To export the details to a TXT or HTML file, click **Export Selected**.

The Export dialog box opens.

6. Browse to the location on your computer where you want to store the details .txt file, and click **Save**.

The Support Center names the file `AgentLog_account_number.txt`, where `account_number` is the number associated with the Agent account.

7. To close the View History Details page, click **Close**.

## Support Center reports

You can use Support Center to report on the accounts on your Data Center. You can perform the following tasks:

- Run default reports installed with Support Center.
- Create and edit your own reports.
- View and display charts.
- Save and export reports in XML format.
- Create account groups.

## Default reports

Support Center includes a default set of report templates. You can edit a default report template to meet your needs. If you do this, save the edited default report template under a new name. Doing so ensures that you do not lose the original default configuration and that Support Center upgrades do not overwrite your customizations.

For example, a future version of Support Center has updated default report templates. When you upgrade Support Center, you overwrite the original default versions. The following tables describes the default report templates that are installed with Support Center:

Support Center report template	Description
Account List	A list of accounts in Support Center. Support Center sorts the list by community, then by account name.
Account Size	The amount of data that each account on the Data Center stores.
Account User Log Errors	The information on accounts that have failed to backup one or more consecutive times, and the type of error it encountered.
Accounts Not Backing Up	A list of PC accounts that the Data Center has not backed up for at least 10 days.
Activity Trends	A graph that shows the trends in the backup activity of accounts. The graph shows data in gigabytes (GB) backed up per day.
Backup Activity	A list of accounts by community, and the amount of data backed up month to date.
Configurations	The assigned and actual Agent configurations for each account.
Data Access by Technicians	Information about which technicians accessed a specific account and the type of activity that occurred.
Encryption Key Disclosure	Accounts with encryption keys that Support Center technicians have viewed.
FileTypeSizes	The fifty most frequently backed-up file extensions by size for accounts that have been through at least one compaction cycle.
First Backup Size	Amount of data in megabytes (MB) backed up by a group of accounts during the first backup.
Heavy Hitters	Accounts backing up the most data in MB.
Heavy Hitters	Accounts with more than 20 GB of data on the Data Center.

Support Center report template	Description
Last Backup	A list of 8.x accounts by community, with their last backup date and status.
Restore Activity	A list of accounts by community, and the amount of data restored by each account during the month to date. Restore activity includes Agent Retrieve, iRoam, and Sharing.
Restore Report	The Restore Report default report displays the information on accounts that have done the file retrievals. The report provides product restore statistics and metrics to the administrators. The report processes all the retrieve outcomes such as Successful, Completed with warning, Completed with Error, Failed and Canceled along with the type of error or warning messages if there is any. The report output can be sorted by account or community. The report processes events that are filtered by ALL(no filtering), Successful, Failed or Canceled.

## Report components

To generate reports, you use the following components:

- **Report template.** Contains the parameters you specify to generate a report.
- **Report.** Contains the actual data, based on the parameters you specify in the report template.

You can include the following types of information in reports:

Report area	Description
Account information	Name and demographic information for a group of accounts. For more information about how to create groups of accounts, see <a href="#">Create account groups, on page 115</a> .
Account summary	Status, Agent version, Agent configuration, and last backup date for a group of accounts.
Current data sizes	Total number and size of files stored on the Data Center for a group of accounts.
Account first backup sizes	Total number and size of files transferred by a group of accounts during their first backup.
Activity types	Number of backups, restores, and CD orders performed within a given time frame.

## Create report templates

### To create a new report template

1. Click the **Report Templates** node under the community for which you want to create a report.  
If you want to, you can include subcommunities in the report.  
The first Create Report Templates page opens.
2. Select the accounts for which you want to create a report.
3. Complete the subsequent report template pages to select the information that you want to display in the report and specify how to sort it.
4. After you create the report template, save the template on the Support Center server for reuse.  
You can edit the report template any time.

## Generate and view reports

After you save a report template, you can run the corresponding report at any time. You also can rerun the report in the future. Depending on the amount of data that you need to compile the report, it can take minutes or hours for the report to run. When the report is complete, Support Center displays the name of the report under the **Reports** node.

### To generate and view a report

1. Log on to Support Center.
2. Select a community.
3. Expand the **Reports** template node and select the type of report that you want to generate.
4. Click **Run Report**.  
The Report Queue page opens.
5. Expand the reports node and select the report that you want to view.  
The Report page opens. You can print the report, or download it to an XML file.

For more information, see Support Center Help.

## View charts

You can include charts in reports. Support Center uses Adobe® SVG Viewer to display charts. If your computer does not have Adobe SVG Viewer installed, you can download it through Support Center. You can display a chart for the following types of information:

- Number of accounts
- Account activity values

- Total account data size values
- First backup size values

## Save report results in XML

On the Reports page, you can view reports in XML format. Typically, you have to display the XML format only when Corporate Support requests this information. After you display the XML format, you can copy and paste the content to another file that you can send to Corporate Support.

## Create account groups

You can use the reports feature to create a group of accounts and then change all of the accounts in the group simultaneously. You can use the reports feature to change accounts in the following ways:

- Change the account status
- Change the Agent configuration
- Move the accounts to a different subcommunity

For example, you can create a report to find all accounts that have not performed a backup in the past 90 days. You can then use the list of accounts to change the status of the accounts to canceled or on hold. The account group is a temporary entity. After you close the Support Center session, or after the session times out, Support Center deletes the account group.

## Use the Agent Protocol Session log

The Agent Protocol Session log records messages that the Agent sends and receives during backups. Support representatives and technicians can use this log and the Data Center Protocol Session log to troubleshoot problems that might occur when the Agent and the Data Center communicate during backups. For example, if a problem occurs during a backup, the technician can view both Protocol Session logs to determine whether the Agent received all messages from the Data Center, and the reverse.

The Agent creates the Protocol Session log as a .log file and stores it the `Library/Application Support/AgentService` folder in the Agent installation directory. You can view the Agent protocol session log in a standard text editor.

## Enable the Agent Protocol Session log

To enable and configure the Agent Protocol Session log, open the `LogSettings.xml` file. This file is in the `Library/Application Support/AgentService` folder. You can configure the following options:

Option	Description
<b>Level Value</b>	<p>The verbosity of the log.</p> <p>You can specify the following values:</p> <ul style="list-style-type: none"> <li>• <b>Info</b>. Standard logging</li> <li>• <b>Debug</b>. Detailed logging</li> <li>• <b>Error (default)</b>. No logging</li> </ul> <p>Because the log records information only for the Info and Debug levels, use Error to disable protocol session logging.</p>
<b>Log File Name</b>	<p>A name for the file that the LogSettings.xml file generates.</p> <p>By default, the Agent stores this file in the Log folder.</p>
<b>Log Category</b>	<p>The type of log to which the level value applies.</p> <p>You can use the LogSettings.xml file to specify logging levels for other types of logs. Therefore, to apply the level value to the Protocol Session log, you must specify <b>ProtocolLog</b> as the Log Category.</p>
<b>Log Activity Type</b>	<p>How large the Agent lets the file grow.</p> <p>You can specify the following values:</p> <ul style="list-style-type: none"> <li>• <b>FileAppender</b>. Lets the Agent write to the log without ever purging its contents.</li> <li>• <b>RollingFileAppender (default)</b>. Limits the size of the log to a default size of 10 MB or a size that you specify.</li> </ul> <div style="border-left: 2px solid orange; padding-left: 10px; margin-top: 10px;"> <p><b>IMPORTANT:</b>                      If you do not specify a value for Log activity type, Protocol Session logging does not work.</p> </div>

The following text is an example of the LogSettings.xml file:

```

version="1.0" encoding="UTF-8"?>
TYPE log4j:configuration SYSTEM "log4j.dtd">
j:configuration debug="false" xmlns:log4j="http://jakarata.apache.org/log4j/">
  <appender name="RollingFile" class="org.apache.log4j.RollingFileAppender">
    <param name="File" value="Log/Agent.log"/>
    <param name="MaxFileSize" value="100MB"/>
    <param name="MaxBackupIndex" value="5"/>
    <layout class="org.apache.log4j.PatternLayout">
      <param name="ConversionPattern" value="%d{HH:mm:ss, SSS} %5p - %m%">
    </layout>
  </appender>
    
```

```
<!-- Log everything to the console by default. -->  
<root>  
<logger name="Agent.Protocol" >  
    <!--This value can be error (no output), info, or debug. -->  
    <level value="debug" />  
    <appender-ref ref="Rollingfile"/>  
</logger>  
4j:configuration>
```

## Chapter 12: Troubleshooting

This chapter helps you troubleshoot the following scenario:

- [Scenario: Mac backups might complete with errors on macOS Mojave or later version\(s\), below](#)

### Scenario: Mac backups might complete with errors on macOS Mojave or later version(s)

While running Connected Backup Mac Agent on macOS Mojave, backups might complete with errors. This may be due to the permission restrictions Mojave has introduced for user data files.

By default, any application on Mojave is restricted from accessing user's private data. Mojave requires applications to get user's approval for accessing such private data. As Connected Backup Mac Agent requires access to all such data files for backing up, it is necessary to authorize Connected Backup Mac Agent by adding it to the new 'Full Disk Access' category in the System Preferences Security and Privacy Pane. By doing so, the user authorizes the Connected Backup Mac Agent to access all of their private data. Authorization can also be preconfigured in enterprise and education environments via MDM server.

### Authorizing Connected Backup Mac Agent on single macOS Mojave or later version(s)

**To add Connected Backup Mac Agent under 'Full Disk Access' category on a macOS Mojave system, follow these steps:**

1. Click the unlock icon on the left bottom of the pane.
2. Close the System Preferences and Connected Backup applications.
3. Quit AgentService process from Activity Monitor.  
This will restart the AgentService.
4. Open the Connected Backup application and trigger backup.  
Backups would succeed now.
5. Go to **Privacy > System Preferences Security & Privacy** pane.
6. Select **Full Disk Access** category on the left hand side.
7. Click the lock icon on the left bottom of the pane.
8. Click + sign, select and add the **/Library/AgentService/AgentService**.

9. Click + sign, select and add the **/Applications/Autonomy/Connected Backup/Connected Backup.app**.

## Authorizing Connected Backup Mac agent in enterprise environments

You can also authorize these settings on all macOS Mojave systems by using administrative tools like MDM (Mobile Device Management) Server. For details configuration, see section, *Privacy Preferences Policy Control Payload in Configuration profile reference document* available at the following location:

<https://developer.apple.com/business/documentation/Configuration-Profile-Reference.pdf>

The following links provide additional details on Mojave's security enhancement:

- For 'Privacy and Security' - <https://www.apple.com/macos/mojave/>
- Apple's guidelines for deploying Mojave for enterprises/institutions - <https://support.apple.com/en-sg/HT209028>
- For explanation on enhanced security features of Mojave - <https://developer.apple.com/videos/play/wwdc2018/702/>

# Index

## A

- account groups 115
- account information, viewing 24
- Account List report 112
- Account Management Website
  - branding requirements 64
  - deploying 68
  - editing Terms of Use and Privacy 68
  - interface 70
  - logon credentials 70
  - Logon page 72
  - managing logon credentials 70
  - overview 67
  - Registration page 71
  - security 68
  - setting default URL 69
  - Summary page 73
  - technician access 69
  - user access 69
  - Welcome page 71
- account numbers 23
- Account Size report 112
- account status 24
- account status, changing 25
- accounts
  - changing primary server 26
  - description 15
  - reserving 26
  - technician 30
- Accounts Not Backing Up report 112
- accounts on hold 25
- Activate.exe 83
- active account 25
- Activity Trends report 112
- Agent 41
  - accounts 15
  - branding 57
  - branding requirements 64
  - configurations 12
  - distributing 18
- Agent About window, branding 61
- Agent accounts
  - enabling MyRoam 76
- Agent branding requirements 64
- Agent command-line interface 83
  - backup command 93

- Agent command line interface, retrieving files 98
- Agent configurations
  - overview 40
- Agent history
  - types of events 108
  - viewing in Support Center 110
  - viewing in the Agent interface 108
- Agent main window 81
- Agent rule sets 41
- Agent security 29
- Agent settings 41
- Agent Start-up Wizard 78
- Agent Status icon
  - possible appearances 29
- Agent user interface 80
  - using 82
- Agents
  - deploying 17
  - sending messages 27
- allocating licenses 34, 37

## B

- backup
  - Agent command line interface 93
  - Backup Set tab 92
  - command-line examples 94
  - command-line options 94
  - command-line syntax 93
  - encrypted files 89
  - file preparation 87
  - modified file identification 87
  - monitoring progress 92
  - outcome icons for Agent Status icon 29
  - results 88
  - security descriptors 90
  - settings and configurations 90
  - sparse files 90
  - Summary tab 92
  - using the Agent user interface 92
- Backup Activity report 112
- backup messages 28
- backup process
  - disk scan 85
  - file analysis 86
- Backup Set tab 92
- backup settings 90
- backup.exe 83
- bandwidth throttling 38
- base files 86
- branding
  - Agent 57
  - Agent About window 61

- Agent user interface 59
- communities 66
- inherited 62
- overview 57
- process 65
- requirements 64
  - Account Management Website
    - graphics 64
  - Agent graphics 64
  - Support Center graphics 64
- Support Center 62
- Support Center image requirements 64
- Support Center Logon page 62
- technician requirement 65

branding requirements

- Agent graphics 64

browsing to select files 105

## C

- canceled accounts 25
- certificates, Agent security 55
- changing the status of an account 25
- charts 114
- command-line examples
  - backup 94
  - file retrieval 102
- command-line options, retrieve 99
- command-line syntax
  - backup 93
  - retrieve 99
- communities 12, 20
  - applying bandwidth throttling 38
  - branding 66
  - creating 17
  - creating new 21
  - default 20
  - disabling registration 22
  - enabling MyRoam 75
  - primary server, changing 26
- configurations
  - Agent 12, 40
- Configurations node 17
- Configurations report 112
- configurations, enabling MyRoam 75
- conflicts during retrieval 98
- connections
  - Data Center 87
  - interruptions 17
  - properties 15
  - proxy servers 16
  - to Data Center 15

- creating communities 17
- creating technician accounts 30

## D

- Data Center
  - applying bandwidth throttling 38
  - connections during backup 87
- default
  - community 20
- default URL to Account Management Website, setting 69
- deleted accounts 25
- deleted files 86
- DeltaBlock 86
- deploying Agents 17
- destination options for file retrieval 98
- disabling registration in communities 22
- disk scan 85
- distributing the Agent software 18
- downloading files 106

## E

- email notification of file retrieval 95
- email notification to technicians 29
- enabling backup messages 28
- encrypted files
  - backup of 89
- Encryption Key Disclosure report 112
- encryption, Agent 54
- exporting Agent history to an XML file 109

## F

- features, licensed 32
- file analysis for backup 86
- file name conflicts during retrieval 98
- file repackaging during retrieval 95
- file size 86
- file transmission during backup 87
- file versions 106
- files
  - base 86
  - deleted 86
  - retrieving 96
  - selecting for retrieval 97
- FileTypeSizes report 112
- Find feature for selecting files 105
- First Backup Size report 112

## G

- generating reports 114

## H

Heavy Hitters Cumulative report 112  
Heavy Hitters report 112  
history, Agent 108

## I

informational messages 27  
inheritance  
    and Support Center objects 12  
inheritance of objects in Support Center 12  
inherited branding 62  
installation  
    MyRoam 75  
interfaces  
    Agent command-line 83  
    Agent user 82  
    Agent user interface 80

## L

licensed features 32  
licenses  
    allocating 34, 37  
    allocation 31  
    effect on accounts and communities 33  
    enabling or disabling features 38  
    expired 33  
    inheritance 31  
    managing 31  
    moving accounts 34  
    moving communities 33  
    MyRoam 75  
    used and unused 32  
locked rules 46  
logon credentials, Account Management  
    Website 70  
logon credentials, managing 70  
Logon page, Account Management Website 72

## M

managing licenses 31  
MDATE 86  
messages, backup 28  
MyRoam  
    enabling for configurations and  
        communities 75  
    enabling for individual accounts 76  
    installation 75  
    license and permission requirements 75  
    overview 74  
    retrieving files 103

## N

non-SOCKS proxy servers 16  
notification of file retrieval 95

## O

options  
    backup 94  
outcome icons for backups 29

## P

permissions  
    MyRoam 75  
    retrieve 97  
preparations  
    backup 87  
primary server, changing 26  
processing rules 47  
profile and Web site settings 41  
profile settings 41  
properties and settings 17  
proxy servers 16  
    Agent connection settings 16  
    connecting through 16

## R

Registration page, Account Management  
    Website 71  
reports 12  
    account groups 115  
    Account List 112  
    Account Size 112  
    Accounts Not Backing Up 112  
    Activity Trends 112  
    Backup Activity 112  
    components 113  
    Configurations 112  
    creating 114  
    creating and viewing 113  
    default 112  
    Encryption Key Disclosure 112  
    FileTypeSizes 112  
    First Backup Size 112  
    generating and viewing 114  
    Heavy Hitters 112  
    Heavy Hitters Cumulative 112  
    in Support Center 111  
    Restore Activity 113  
    saving as XML 115  
    saving in XML format 115  
    viewing charts 114

- requirements
  - branding 64
- reserving Agent accounts 26
- Restore Activity report 113
- Restore Report 113
- retrieval
  - file repackaging 95
  - selecting files 97
- retrieve
  - command-line examples 102
  - command-line options 99
  - command-line syntax 99
  - destination options 98
  - file name conflicts 98
  - files 104
  - permissions 97
  - procedure 106
  - sparse files 96
  - using MyRoam to retrieve files 103
  - using the Agent command line interface 98
- retrieve tab 96
- retrieving files 96
  - email notification 95
- rule sets 41
- rules 12
  - Agent Rules wizard 52
  - best practices 50
  - creating 50
  - locked 46
  - logic 47
  - page in Support Center 51
  - precedence 48
  - types 46
  - unlocked 46
  - user-created 46
  - Wizard 52

## S

- security
  - Account Management Website 68
  - Agent encryption 54
  - certificates 55
  - firewalls 16
  - password protection for retrievals 55
  - preventing unauthorized access 54
  - protecting files on stolen computers 55
- security descriptors
  - backup of 90
- security, Agent 29
- selecting files
  - browsing 105
  - displaying file versions 106

- using Find 105
- sending messages to Agents 27
- SendOnce technology 86
- server, changing primary for account 26
- settings
  - Agent 41
  - backup 90
  - profile 41
  - proxy server 16
  - Web site 41
- SOCKS 16
- sparse files
  - backup of 90
  - retrieval of 96
- Start-up Wizard 78
- status of Agent accounts 24
- stolen computers, protecting files 55
- subcommunities
  - Agent accounts 22
  - creating 22
- Summary page, Account Management
  - Website 73
- Summary tab 92
- Support Center
  - accessing, URL for 13
  - Agent configurations 12
  - branding 62
  - branding requirements 64
  - communities 12, 20
  - default community 20
  - interface 10
  - object inheritance 12
  - objects, and inheritance 12
  - opening 13
  - overview 9
  - reports 12, 111
  - rules 12
  - Rules page 51
  - subcommunities, 21
  - technicians 11
  - viewing Agent history 110
- Support Center interface
  - branding 63
- Support Center interface, 63
- Support Center logon page, branding 62
- Symbolic Link 86

## T

- tabs
  - Backup Set 92
  - Retrieve 96

- Summary 92
- technician access, Account Management Website 69
- technician accounts, creating 30
- technicians 11
- templates
  - reports 113
- templates, creating 114
- Terms of Use and Privacy, editing 68
- throttling bandwidth 38
- Touch 86
- transmission of files during backup 87

## U

- unauthorized access 54
- unlocked rules 46
- UpdateProfile command 83
- user-created rules 46
- user access, Account Management Website 69
- user interface, Agent 80

## V

- versions 41
- viewing
  - Agent History 108
  - reports 114
- viewing account information 24
- viewing account numbers 23

## W

- Web site settings 41
- Welcome page
  - Account Management Website 71
- Wizard
  - Agent Rules 52
- Wizard, Start-up 78

## X

- XML
  - Agent history file 109
  - reports 115

# Send documentation feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

## **Feedback on Administering Mac Agents (Micro Focus Connected Backup 9.0.3)**

Add your feedback to the email and click **Send**.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to [swpdl.ConnectedBackup.DocFeedback@microfocus.com](mailto:swpdl.ConnectedBackup.DocFeedback@microfocus.com).

We appreciate your feedback!