

USER GUIDE





Last modified: 2025

© 1999–2025 Faronics Corporation. All rights reserved. Faronics, Deep Freeze, Deep Freeze Cloud, Faronics Deploy, Faronics Core Console, Faronics Anti-Executable, Faronics Anti-Virus, Faronics Device Filter, Faronics Data Igloo, Faronics Power Save, Faronics Insight, Faronics System Profiler, and WINSelect are trademarks and/or registered trademarks of Faronics Corporation. All other company and product names are trademarks of their respective owners.



Contents

Preface	9
Important Information	10
About Faronics	10
Product Documentation	10
Technical Support	11
Contact Information	11
Definition of Terms	13
Definition of Terms	14
Introduction	19
Introduction to Deep Freeze Cloud Console	20
Deep Freeze Cloud Console Components	21
Diagram of Deep Freeze Cloud Console	22
System Requirements	23
Getting Started	25
Getting Started with Deep Freeze Cloud Console	26
Getting Started if you are a New Deep Freeze Cloud User	26
Installing Deep Freeze Cloud Console Components	29
Deep Freeze Cloud Console Components	30
Installing the Cloud Agent	30
Installing the Cloud Agent Using the Full Installer	31
Installing the Cloud Agent via Apple Remote Desktop (ARD)	32
Installing On Demand Cloud Relay	32
Uninstalling the Cloud Agent (Windows)	33
Uninstalling the Cloud Agent (HFS+)	33
Uninstalling the Cloud Agent (APFS)	34
User Management	37
My Profile	38
Organization Settings	40
User Management	41
Add User	41
Edit User	43
Send Invite Email	44
Send Password Reset Email	44
Clone User	45
Disable User	45
Delete User	45



Tag	45
2-Factor Authentication (2FA)	46
Active Directory Users	47
SAML Integration	49
Managing Sites	55
Overview	56
Creating a Site	57
Using Deep Freeze Cloud Console	59
Home	60
Widgets	60
Install Cloud Agent	60
Manage Policies	60
Task Status	60
Computers	62
Live Actions	62
Client Information	68
Groups	69
Adding a Group	69
Editing a Group	70
Deleting a Group	70
Active Directory Import	70
Search	70
Policies	71
Adding a Policy	72
Editing a Policy	73
Copying a Policy	73
Deleting a Policy	74
Copy to Sites	74
Uninstall Service from a Policy (some computers)	75
Scheduled Policy Updates	75
Inheriting Policy Settings	76
Applications	77
Color scheme	77
Custom Apps (Windows)	77
Custom Scripts (Windows)	78
Pending Updates/All (Windows)	79
Pending Updates/All (Mac)	83
Apps with Recent Updates	85
Failed Updates (Windows Only)	86
App Presets	86
Windows Updates	88
Pending Windows Updates/All/Online Only	88
Recent Windows Updates	90
Failed Windows Updates	90
Imaging	91
Setting Up	91



Image Caching	96
Image Computer.....	97
Capture Image.....	97
Computers	98
Imaging Servers	100
Deployment Packages	101
Install Settings.....	102
Images	103
Driver Groups	104
Inventory	105
All/Warranty Expired	105
Update Warranty Info	106
Action Toolbar.....	106
Tickets	108
All/Active/Closed	108
New Ticket.....	109
Assign Ticket/Owner	109
Ticket Actions	110
View History.....	111
General Settings.....	112
Cloud Agent Settings.....	112
Maintenance Period	112
Deep Freeze Service	114
Password Tab.....	115
Drives Tab.....	115
Workstation Tasks Tab	118
Windows Update Tab.....	124
Batch File Tab.....	126
Advanced Settings Tab.....	127
Deep Freeze Dashboard	132
Data Igloo Service	135
Folder Redirection Tab.....	136
User Profile Redirection Tab	136
Registry Key Redirection Tab.....	136
Software Updater Service (Windows).....	138
Application Tab	139
Software Deployment Tab (for Usage Stats Ultimate Only).....	139
Windows Update Tab (for Ultimate only).....	141
Advanced Options Tab.....	143
Windows Update Dashboard	144
Anti-Executable Service.....	150
Anti-Executable Terms.....	151
How to use Anti-Executable	151
Deployment Options	151
Protection Settings.....	152
Policy Control List.....	154
Ransomware Prevention	155
User Settings.....	156
Central List.....	157
Anti-Executable Dashboard	157



WINSelect Service	163
Kiosk Tab	164
System Tab	166
Application Tab	170
Printers Tab	171
Acceptable Use Policy Tab	171
Administrator Tab	171
Cloud Sync	172
Configuring Cloud Sync	172
Usage Stats Service	174
Incident Reporting Service	175
Configuring Incident Reporting	175
Ticketing Service	177
Power Save Service	178
Audit Mode	179
Power Schedule Tab	179
Critical Apps Tab	182
Windows Options Tab	182
Hardware Settings Tab	183
User Experience Tab	183
Administration Settings Tab	184
Energy Cost Tab	184
Imaging Service	186
Remote Connect Service	187
Anti-Virus Service	189
Configuring Anti-Virus	189
Security Options Tab	190
Computer Settings Tab	190
Scan Settings Tab	191
Firewall Protection Tab	193
Deep Freeze Mac Service	196
Deep Freeze Mac (HFS+)	196
Deep Freeze Mac (APFS)	199
Software Updater Service (Mac)	204
Anti-Virus Service (Mac)	205
Configuring Anti-Virus	205
Security Options Tab	205
Computer Settings Tab	206
Scan Settings Tab	206
Reports	208
General Report	208
Deep Freeze	209
Data Igloo	210
Anti-Executable	210
Software Updater	211
Usage Stats	212
Incident Reporting	213
Power Save	214



Anti-Virus	216
Utilities	220
General Utilities	220
Deep Freeze Utilities	221
Deep Freeze Mac Utilities	223
Anti-Virus Utilities	231
Software Updater Utilities	232
Anti-Executable Utilities	234
Alerts	235
Manage Alerts	235
Read and Take Action	238
Appendix A Authorized Domains and Ports	239
Using Deep Freeze On Demand	241
Overview of Deep Freeze On Demand	242
Deep Freeze Actions	243
On Demand Actions	243
Manage Schedules	247
Creating a New Schedule	247
Editing or Deleting an Existing Schedule	249
Cloud Relay	250
Tags	251
Tags	252
Assign Tags	253
Manage Tags	254
Deep Freeze Administrator Mobile App	257
Overview	258
Deploy Cloud Agent from the Mobile App	259
Manage Computers Locally from the Mobile App	260
Manage Computers Remotely from the Mobile App	261
View Details	261
Filtering by Status, Policy, or Group	261
Filtering by Tags	262
Removing Active Filters	263
Search	263
Perform Actions	263
Swipe Menu Options	265
Handout	267
Overview	268
Install, Enable and Disable Handout	269
Install Handout	269
Enable Handout	269
Disable Handout	269



Remove Handout Completely	270
Managing a Class	271
For Administrators	271
For Teachers	272
Handout files to a Class	274
Usage Stats	275
Usage Stats Overview	276
Manage Software Assets	277
Pre-defined Products Supported by Usage Stats	278
Mobile Device Management	279
Mobile Device Management (MDM) Overview	280
MDM Features for iOS Devices	280
MDM Features for Android devices	281
MDM Features for Chromebooks	281
Pre-defining Settings	283
Pre-defining Wireless Networks	283
Pre-defining Global HTTP Proxies	284
Pre-defining Web Clips	285
Pre-defining Wallpapers	287
Pre-defining Email Settings	288
Pre-defining Certificates	289
Enrolling and Removing Mobile Devices	291
Enrolling iOS Devices	291
Configuring a Connection to Android for Work	296
Enrolling Android Devices	297
Sending Android Enrollment Invitation Emails	301
Provisioning Chromebooks	301
Installing the Deep Freeze Chrome MDM Extension	302
Removing devices	302
Managing Apps	304
Adding iOS apps	304
Adding Android apps	305
Managing Chromebook Apps	307
Removing Apps	307
Managing Groups	308
Creating Groups for iOS devices	308
Creating Groups for Android Devices	310
Managing Groups for Chromebooks	312
Assigning iOS or Android Devices to a Group	314
On-Demand Actions	316
Sending Messages to Devices	316
Locking a Device	316
Assigned Apps for Devices	316
Clearing the Passcode on an iOS Device	317
Resetting the Passcode on an Android Device	317



Disabling and Re-enabling Chromebooks	317
Wiping a Device	318
Moving Chromebooks Between Organizational Units (OU)	319
Updating iOS on Devices	319
Setting Restrictions	320
Settings Restrictions for iOS Groups	320
Setting Restrictions for Android Groups	322
Configuring Universal Filtering Settings for Chromebooks	325
Managing Chromebook Work Settings	326
Chromebook Data	328
Mobile Kiosks	330
Creating Kiosks	330
Frequently Asked Questions	333





Preface

This user guide explains how to configure and use Deep Freeze Cloud Console.

Topics

[Important Information](#)

[Technical Support](#)



Important Information

This chapter contains important information about your Faronics product.

About Faronics

Faronics delivers market-leading solutions that help manage, simplify, and secure complex IT environments. Our products ensure 100% machine availability, and have dramatically impacted the day-to-day lives of thousands of information technology professionals. Fueled by a market-centric focus, Faronics' technology innovations benefit educational institutions, health care facilities, libraries, government organizations, and corporations.

Product Documentation

The following documents form the Deep Freeze Cloud Console documentation set:

- Deep Freeze Cloud Console Online Help – This is the document you are reading. This document guides you how to install, configure, deploy, and use the product.



Technical Support

Every effort has been made to design this software for ease of use and to be problem free. If problems are encountered, contact Technical Support.

support.faronics.com

800-943-6422 or +1-604-637-3333

7:00am to 5:00pm (Pacific Time)

Contact Information

- Email: sales@faronics.com
- Phone: 800-943-6422 or +1-604-637-3333
- Fax: 800-943-6488 or +1-604-637-8188
- Hours: 7:00am to 5:00pm (Pacific Time)
- Address:
Faronics Technologies USA Inc.
5506 Sunol Blvd., Suite 202
Pleasanton, CA 94566
USA

Faronics Corporation (Headquarters)
609 Granville Street, Suite 1400
Vancouver, BC V7Y 1G5
Canada

Faronics Corporation (Europe)
8, The Courtyard, Eastern Road
Bracknell, Berkshire
RG12 2XB, United Kingdom

Faronics Pte Ltd
160 Robinson Road
#05-05 SBF Center
Singapore 068914





Definition of Terms

This chapter explains the terms that occur in the product and this user guide.

Topics

[Definition of Terms](#)



Definition of Terms

Term	Definition
Deep Freeze Cloud Console	The Deep Freeze Cloud Console allows you to manage the computers on your network from a browser.
Cloud Agent	The Cloud Agent is installed on the computers that are managed by the Deep Freeze Cloud. The Cloud Agent on multiple computers report to the Cloud Relay, and the Cloud Relay reports to the Deep Freeze Cloud.
Cloud Relay	The Cloud Agent installed on the computers report to the Cloud Relay. The Cloud Relay reports to the Deep Freeze Cloud. Real-time Deep Freeze actions can be performed on the computers through the Cloud Relay.
Policy	A policy contains all the configuration settings on how services run on the computer. A policy contains the action taken by the services, schedule, error reporting and the functionality allowed to the user on the computer.
Services	The Deep Freeze Cloud Console allows installing Policies for the following Services: Anti-Executable, Anti-Virus, Deep Freeze, Power Save, and WINSelect.
Imaging Server	Deep Freeze Imaging Server contains Images and Drivers to deploy on to multiple computers.
Anti-Virus Definition Relay	Install the Anti-Virus Definition Relay on any computer on your network to download virus definitions and distribute them across your local network.
Deployment Utility	The Deployment Utility allows you to deploy Services to client computers that are available on the network and turned on. Make sure to run the Deployment utility from your computer with administrative rights.
Anti-Executable Data Import Utility	Run the Anti-Executable Data Import Utility on any computer to automatically add allowed/blocked files and publishers into the Central Control List or the Policy available on the Cloud Console.
Data Igloo	Faronics Data Igloo allows Deep Freeze users to exempt specified data folders, entire user profiles, or even registry keys from being Frozen by redirecting them to a Thawed partition (ThawSpace), while keeping the operating system partition completely protected.



Term	Definition
OTP	A One Time Password (OTP) can be useful if, for example, a Deep Freeze password is lost or if a configuration file was created without any password defined. An OTP can also be used to provide access to a computer for an individual performing maintenance duties without requiring that individual to know the permanent Deep Freeze password.
Central List	A Central List contains the names of all the executable files and Publishers on your network. Populate the Central List by adding the files and Publishers on the console computer. This Central List can then be applied to the computers via a Policy. The Central List needs to be created only once, but can be applied multiple times to more than one computer via a Policy.
Executable	Any file that can be launched by the operating system. The executable files managed by Anti-Executable have the extension .scr, .jar, .bat, .com, or .exe.
JAR file	A JAR (Java Archive) is an archive file format contains many Java class files and associated metadata and resources (text, images and so on) into one file to distribute application software or libraries on the Java platform.
Protection	When set to Enabled, this setting indicates that Anti-Executable is protecting a computer based on the Central Control List and Local Control List. When set to Disabled, any executable can be launched on the computer.
Publisher	A Publisher is the creator of a file (for example, Microsoft created wordpad.exe). A Publisher validates the file by digitally signing it. Anti-Executable uses the Publisher name, product filename, and version details to identify the files created by a Publisher.
Stealth Mode	Stealth Mode is a group of options that control visual indication of a Service presence on a system. Stealth Mode provides the option to the Administrator to hide the Service icon in the Windows system tray, and prevent the Alert from being displayed.
Unauthorized Executable	An Unauthorized executable is one that is not allowed to run by Anti-Executable.
Customization Code	The Customization Code is a unique identifier that encrypts the Configuration Administrator, the Enterprise Console, the computer installation files, the One Time Password Generation System, and Deep Freeze Command Line Control. This code is not a password that can be used to access Deep Freeze.



Term	Definition
Active Protection	Active Protection (AP) is a real-time method for detecting malware. AP sits quietly in the background as you work or browse the Internet, constantly monitoring files that are executed.
Adware	Adware, also known as advertising software, is often contextually or behaviorally based and tracks browsing habits in order to display third-party ads that are meant to be relevant to the user. The ads can take several forms, including pop-ups, pop-unders, banners, or links embedded within web pages or parts of the Windows interface. Some adware advertising might consist of text ads shown within the application itself or within side bars, search bars, and search results.
Email Protection	Email Protection is a behind-the-scenes tool that protects your computer from potentially harmful inbound and outbound email messages. As long as you have email protection enabled, your computer is protected with automatic email scanning of all attachments for malware and viruses without you having to do anything.
Firewall	A Firewall provides bi-directional protection, protecting you from both incoming and outgoing traffic. A Firewall protects your network from unauthorized intrusion.
Quarantine	The Quarantine is a safe place on your computer that Faronics Anti-Virus uses to store malware or infected files that could not be disinfected. If your computer or files on your computer are not acting normal after an item has been placed here, you have the opportunity to review the details of a risk and research it further and remove it from Quarantine, restoring it back to your computer in its original location. You can also permanently remove the risks from Quarantine.
Rogue security program	A rogue security program is software of unknown or questionable origin, or doubtful value. A rogue security program usually shows up on web sites or spam emails as intrusive warnings that claim that your computer is infected and offer to scan and clean it. These should never be trusted. Reputable anti-virus or anti-spyware companies will never use this way of notifying you. A rogue security program may appear like an ordinary anti-virus or anti-malware program, but will instead attempt to dupe or badger you into purchasing the program. While some rogue security programs are the equivalent to snake oil salesman resulting in no good, others may actually result in harm by installing malware or even stealing the credit information that you enter and possibly resulting in identity theft. Further, you need to be cautious about closing or deleting these alerts, even when you know they're fake.
Rootkits	A rootkit is software that cloaks the presence of files and data to evade detection, while allowing an attacker to take control of the machine without the user's knowledge. Rootkits are typically used by malware including viruses, spyware, trojans, and backdoors, to conceal themselves from the user and malware detection software such as anti-virus and anti-spyware applications. Rootkits are also used by some adware applications and DRM (Digital Rights Management) programs to thwart the removal of that unwanted software by users.



Term	Definition
Spyware	Spyware is software that transmits information to a third party without notifying you. It is also referred to as trackware, hijackware, scumware, snoopware, and thiefware. Some privacy advocates even call legitimate access control, filtering, Internet monitoring, password recovery, security, and surveillance software spyware because those could be used without notifying you.
Trojan	A trojan is installed under false or deceptive pretenses and often without the user's full knowledge and consent. In other words, what may appear to be completely harmless to a user is in fact harmful by containing malicious code. Most trojans exhibit some form of malicious, hostile, or harmful functionality or behavior.
Virus	A computer virus is a piece of malicious code that has the ability to replicate itself and invade other programs or files in order to spread within the infected machine. Viruses typically spread when users execute infected files or load infected media, especially removable media such as CD-ROMs or flash drives. Viruses can also spread via email through infected attachments and files. Most viruses include a payload that can be anywhere from annoying and disruptive to harmful and damaging; viruses can cause system damage, loss of valuable data, or can be used to install other malware.
Worm	A worm is a malicious program that spreads itself without any user intervention. Worms are similar to viruses in that they self-replicate. Unlike viruses, however, worms spread without attaching to or infecting other programs and files. A worm can spread across computer networks via security holes on vulnerable machines connected to the network. Worms can also spread through email by sending copies of itself to everyone in the user's address book. A worm may consume a large amount of system resources and cause the machine to become noticeably sluggish and unreliable. Some worms may be used to compromise infected machines and download additional malicious software.
Inactivity Definitions	<p>The definition of what makes a computer inactive: keyboard and mouse inactivity and one of the following parameters:</p> <ul style="list-style-type: none">• Disk Utilization – user-defined measurement of disk (hard drive) utilization; if the disk utilization is lower than this defined level, the computer is considered inactive and power saving actions will occur.• CPU utilization – user-defined measurement of CPU utilization; if the CPU utilization is lower than this defined level, the computer is considered inactive and power saving actions will occur.• Network activity – user-defined measurement of network activity; if the network activity is lower than this defined level, the computer is considered inactive and power saving actions will occur.• Applications running – user-defined list of applications; if no application from a user defined list is running, the computer is considered inactive and power saving actions will occur.



Term	Definition
Inactivity Timeout Actions	<p>Actions that Power Save can perform when a computer becomes inactive, which are:</p> <ul style="list-style-type: none">• Turn off monitor• Standby – a mode in which the operating system is suspended and stored in memory before shut down.• Hibernate – a mode in which the operating system is suspended by storing memory on the hard disk before powering down• Shut down
Local Wakeup	<p>Computers in Standby or Hibernate mode can be locally woken up by the Local Wakeup feature without using Wake-on-LAN technology (or without a network connection).</p>
Power Schedule	<p>A Power Schedule consists of:</p> <ul style="list-style-type: none">• Inactivity Timeout Actions – defines whether Power Save must turn off monitors, hard disks and shut down the computer after a pre-defined interval.• Inactivity Definitions – defines whether Power Save must manage power on the computer when the hard disk, CPU or network activities are below the specified levels. <p>Schedule when the Inactivity Timeout Actions will occur.</p>
Stay Awake	<p>Ensures that Power Save does not manage power on the computer for the specified duration.</p>
Wake-on-LAN	<p>A hardware enabled feature that allows remote activation of the computer.</p>



Introduction

Topics

[Introduction to Deep Freeze Cloud Console](#)
[Deep Freeze Cloud Console Components](#)
[Diagram of Deep Freeze Cloud Console](#)
[System Requirements](#)



Introduction to Deep Freeze Cloud Console

Deep Freeze Cloud Console allows you manage the computers and devices on your network from a browser. Since the Deep Freeze Cloud Console is a cloud-based solution, there is no installation required for the console.

The various components in a Deep Freeze Cloud Console are explained further in this chapter.



Deep Freeze Cloud Console Components

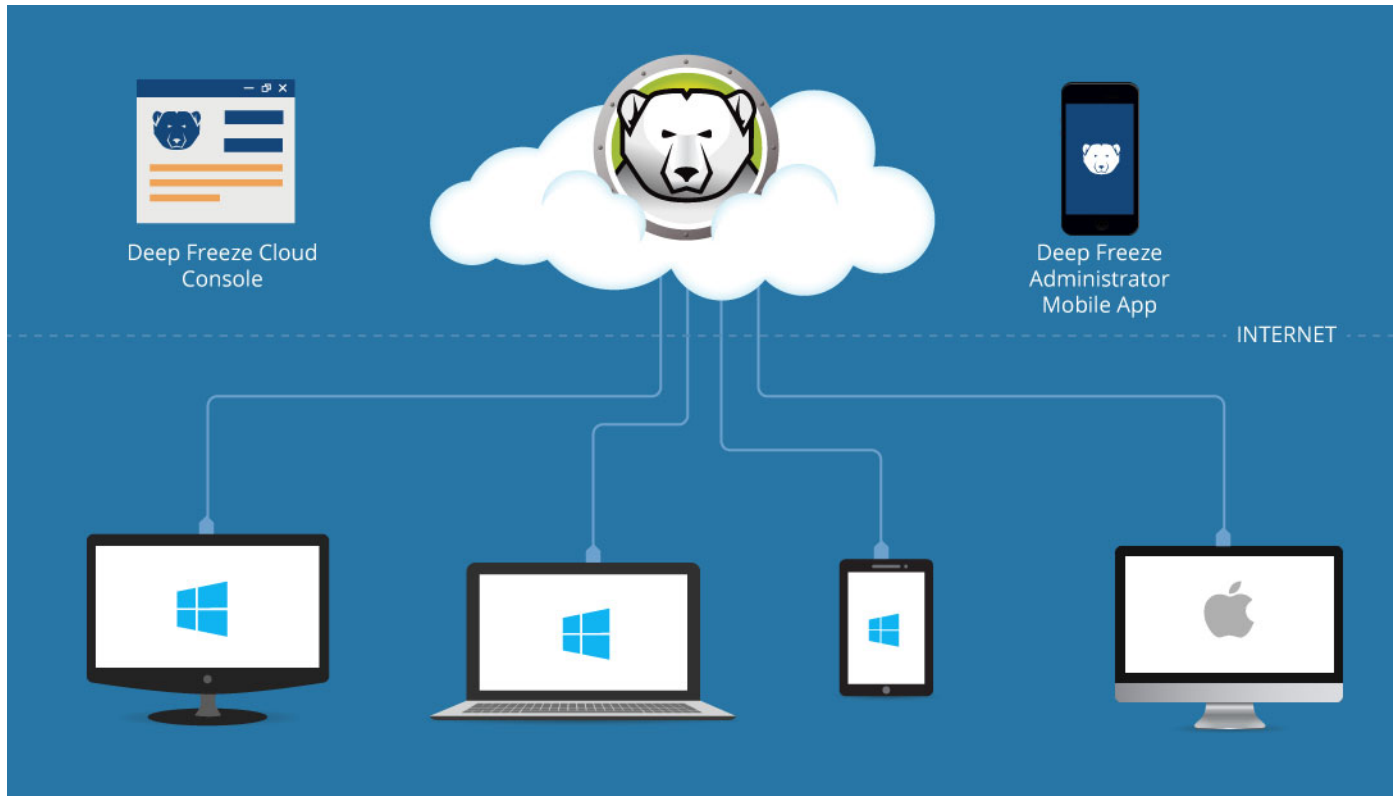
The components of the Deep Freeze Cloud Console are:

- Deep Freeze Cloud Console (hosted on the Cloud)
- On Demand Cloud Relay (inside your network)
- Cloud Agent (on the computers managed by the Deep Freeze Cloud Console)



Diagram of Deep Freeze Cloud Console

The following diagram represents the Deep Freeze Cloud Console and its components:



- Browser or Mobile App – A supported browser like Internet Explorer, Google Chrome or Firefox. You can also use the Deep Freeze Administrator Mobile App.
- Deep Freeze Cloud Console – The Cloud Console offers two distinct functions for new users – *Policies* for various *Services* and *Deep Freeze On Demand*.
- Cloud Agent – Installed on the Windows computers or tablets and Mac systems.



System Requirements

The Deep Freeze Cloud Console is a cloud-based application and does not need any installation. The Deep Freeze Cloud Console can be accessed from a browser is supported on the following:

- Internet Explorer
- Firefox
- Chrome

The Cloud Agent is supported on:

- Windows / Windows Server
32 or 64-bit Operating Systems
 - > Windows 7, 8.1, 10 (up to version 22H2), 11 (up to version 23H2)
 - > Windows Server 2016, 2019, 2022
- Mac
HFS+ File System
 - > OS X Mavericks 10.9.x
 - > OS X Yosemite 10.10.x
 - > OS X El Capitan 10.11.x
 - > OS X Server Mavericks 10.9.x
 - > OS X Server Yosemite 10.10.x
 - > OS X Server El Capitan 10.11.x
 - > macOS Sierra 10.12
 - > macOS High Sierra 10.13APFS File System
 - > macOS High Sierra 10.13.5
 - > macOS Mojave 10.14
 - > macOS Catalina 10.15
 - > macOS Big Sur 11 (on Apple Silicon and Intel architectures)
 - > macOS Monterey 12 (on Apple Silicon and Intel architectures)
 - > macOS Ventura 13 (on Apple Silicon and Intel architectures)
 - > macOS Sonoma 14 (on Apple Silicon and Intel architectures)
 - > macOS Sequoia 15 (on Apple Silicon and Intel architectures)

Deep Freeze requires 10% of the hard drive to be left as free space.





Getting Started

This chapter explains the process of getting started with very brief steps.

Topics

[Getting Started with Deep Freeze Cloud Console](#)



Getting Started with Deep Freeze Cloud Console

Before getting started with Deep Freeze Cloud, here are its components:

- Deep Freeze Cloud – hosted on the Cloud and no installation required.
- Cloud Agent – installed on computers that need to be managed by the Deep Freeze Cloud.
- Cloud Relay – installed on any computer on the network. The Cloud Agent reports to the Cloud Relay. The Cloud Relay reports to the Deep Freeze Cloud.

Make a note of the [System Requirements](#) before getting started.

Now, let's get started:

- [Getting Started if you are a New Deep Freeze Cloud User](#)

Getting Started if you are a New Deep Freeze Cloud User

Setting up and running Deep Freeze Cloud consists of the following steps:

1. Sign-up and Log in: Sign-up for Deep Freeze Cloud.

Sign in options:

- > Login with Email and Password: Select this option to sign in using your registered email and password.
- > Login with AD credentials: Select this option to sign in using Active Directory credentials. Enter your email, password, and Domain Identifier, then click *Sign In*.
- > Login with SAML: Select this option to sign in using SAML. Enter your *Login Domain* name in the *Domain Identifier* field and click *Sign In*.

2. Configure a Policy with the necessary services: Go to the *Policies* page and click *Add Policy*. Select *Add New Windows Policy* or *Add New Mac Policy*. Configure the necessary services and save as [Policy_Name]. For more information about configuring each service, see:

- > [Deep Freeze Service](#)
- > [Data Igloo Service](#)
- > [Software Updater Service \(Windows\)](#)
- > [Anti-Executable Service](#)
- > [WINSelect Service](#)
- > [Cloud Sync](#)
- > [Usage Stats Service](#)
- > [Incident Reporting Service](#)
- > [Ticketing Service](#)
- > [Power Save Service](#)
- > [Imaging Service](#)
- > [Remote Connect Service](#)



- > [Anti-Virus Service](#)
 - > [Deep Freeze Mac Service](#)
 - > [Software Updater Service \(Mac\)](#)
 - > [Anti-Virus Service \(Mac\)](#)
3. Click *Home*. Click *Install Cloud Agent*. Select the following options:
 - > Windows or Mac – Windows is selected by default. You can select Mac if you have configured a Mac policy.
 - > Group – Default is selected by default. If you have created a group, you can select it from the drop-down.
 - > Policy – select the recently created policy from the drop-down.
 - > Download the installer to install on any computer – this option is selected by default. (For other ways to deploy the Cloud Agent, see [Installing the Cloud Agent](#).)
 4. Click *Download Now*.
 5. Run *FWAWebInstaller_[Policy_Name].exe* on each computer that is to be managed by Deep Freeze Cloud.
 6. Click the *Computers* page. The computers managed by Deep Freeze Cloud are now shown on this page.





Installing Deep Freeze Cloud Console Components

This chapter describes the installation process of Deep Freeze Cloud Console components.

Topics

[Deep Freeze Cloud Console Components](#)



Deep Freeze Cloud Console Components

Before using Deep Freeze Cloud, you must install the following components: Cloud Agent and On Demand Cloud Relay.

Installing the Cloud Agent

Complete the following steps to install the Cloud Agent:

1. Log on to the Deep Freeze Cloud Console.
2. Click *Install Cloud Agent*.
3. Select *Windows*, *Windows Server* or *Mac*.
4. Select the *Group*. The computer(s) where the Cloud Agent is installed will be part of the selected Group.
5. Select the *Policy*. The computer(s) where the Cloud Agent is installed will be part of the selected Policy.



When you select a group that has an enforced policy attached to it, the option to change or select the policy is disabled.

The group and policy will be embedded in the installer and applied to the computers. A computer that joins the group with an enforced policy will be assigned with the enforced policy. (Not applicable for Windows Server.)

6. Select one of the following options:
 - > Download the installer to install on any computer.

If you select *Download the Installer to Install on Any Computer*, copy the file to the computers that need to be managed from the Deep Freeze Cloud Console, and run the installer.

When selecting the Windows Server option, the installer can only be installed on server operating systems and can not be installed on non-server operating systems.

Likewise, when selecting Windows option (non-server), the installer can only be installed on non-server operating systems and can not be installed on server operating systems.
 - > Download MSI installer to deploy via Active Directory. (Windows non-server only.)
 - > Obtain a URL for installing on other computer(s).
 - > Download the [Deployment Utility](#) to detect and install on any computer. (Windows non-server only.)
 - > Download the full installer to save bandwidth (for large deployments) – the Cloud Agent Installer includes all the services selected in the policy within the same file for deployment across the network using third party tools. This saves valuable



Internet bandwidth since each computer does not need to download the installers for each service. (Windows non-server only.)

Refer to [Installing the Cloud Agent Using the Full Installer](#) for the list of command lines.

By installing the Cloud Agent, you can configure and install the following services:

- [Deep Freeze Service](#)
- [Data Igloo Service](#)
- [Software Updater Service \(Windows\)](#)
- [Anti-Executable Service](#)
- [WINSelect Service](#)
- [Cloud Sync](#)
- [Usage Stats Service](#)
- [Incident Reporting Service](#)
- [Ticketing Service](#)
- [Power Save Service](#)
- [Imaging Service](#)
- [Remote Connect Service](#)
- [Anti-Virus Service](#)
- [Deep Freeze Mac Service](#)
- [Software Updater Service \(Mac\)](#)
- [Anti-Virus Service \(Mac\)](#)

Installing the Cloud Agent Using the Full Installer

Download the full installer *FWAWebInstaller_[Policy_Name].exe* to be able to use the following command lines for deploying the Cloud Agent with the services to the computer.

Syntax	Description
<code>/DFNoReboot</code>	Suppresses Deep Freeze reboot and does not force the computer to restart after installation. Note: Deep Freeze reboot cannot be suppressed if the policy has both Deep Freeze and Anti-Executable services enabled.
<code>FullIntaller.exe /pauseInstall</code>	Sets the computer to enter into maintenance and remain in maintenance mode for 24 hours as good as indefinitely after installation.
<code>FullIntaller.exe /pauseInstall /t 14:35</code>	Sets the computer to enter into maintenance and remain in maintenance mode until the specified time after installation.
<code>FullIntaller.exe /pauseInstall /m 300</code>	Sets the computer to enter into maintenance and remain in maintenance mode for specified minutes.



Syntax	Description
<code>FullIntaller.exe</code> <code>/finalizeInstall</code>	This will end the maintenance mode if the machine is in maintenance.
<code>/Thaw</code>	This will set the to keep Deep Freeze in Thawed status after installation.

Installing the Cloud Agent via Apple Remote Desktop (ARD)

When installing the Cloud Agent via ARD, it requires the "com.faronics.cloudagent.plist" in the same folder where the CloudAgent.pkg is run. This plist file contains the URL of the Cloud Console without which, the Cloud Agent cannot report back.

When installing using ARD, complete the following steps:

1. Send the Installer.zip to a folder on the remote computer (or copy both CloudAgent.pkg and com.faronics.cloudagent.plist manually to the same location).
2. Send the UNIX command after selecting the target computer(s). The command must follow the syntax:

```
installer -pkg <path to CloudAgent.pkg> -target <volume name>
```

If there are multiple target computers, all must have the same path and volume name, otherwise the UNIX command has to be sent to each computer customized with path and volume name for each of them.

Following is an example command:

```
installer -pkg /Users/admin/Downloads/Installer/CloudAgent.pkg -target  
/Volumes/10.9
```

Installing On Demand Cloud Relay

After installing the Cloud Agent on the computers that will be managed from the Deep Freeze Cloud Console, you can install the On Demand Cloud Relay on the same network as your computers. The On Demand Cloud Relay allows you to perform On Demand Actions for Deep Freeze Cloud.

Complete the following steps to install the On Demand Cloud Relay:

1. Click *Utilities*.
2. Click *Download* for the *On Demand Cloud Relay*.
3. Double-click the *On Demand Cloud Relay*. Click *Next*.
4. Read and accept the License Agreement. Click *Next*.
5. Specify your email and password used to log on to the Deep Freeze Cloud. Click *Install*.
6. Click *OK*.



Install the On Demand Cloud Relay on any computer on your network. Make sure the computer is on the same subnet as the managed computers. If you have multiple subnets and they are not configured to communicate with each other, you must install one On Demand Cloud Relay per subnet.



Uninstalling the Cloud Agent (Windows)

To uninstall the Cloud Agent on Windows, go to *Start > Control Panel > Uninstall a Program*, select the Cloud Agent and click *Uninstall*.

To uninstall the Cloud Agent through the console, go to *Computers* page, select at least one computer and click *Maintenance > Uninstall Cloud Agent*.

Uninstalling the Cloud Agent (HFS+)

To uninstall the Cloud Agent through the console, go to *Computers* page, select at least one computer and click *Maintenance > Uninstall Cloud Agent*.

To uninstall the Cloud Agent on Mac, create a file with the following script and run it as *sudo <filename>*:

```
#!/bin/sh

# Should be root to run this script
if [ "$EUID" != "0" ]; then
    echo "Error: script must be run as root (use sudo)." 1>&2
    exit 1
fi

# if the user didn't give a volume assume the boot (i.e. root) volume
if [ "$1" = "" ]; then
    MCAVOLUME="/"
else
    if [ -d "/Volumes/${1}" ]; then
        MCAVOLUME="/Volumes/${1}"
    else
        MCAVOLUME="${1}"
    fi
fi

if [ -d "${MCAVOLUME}" ]; then
    echo "Uninstalling Cloud Agent from \"${MCAVOLUME}\"."

    # remove Launchd plists for the daemons
    rm -rf
    "${MCAVOLUME}/Library/LaunchDaemons/com.faronics.cloudagentd.plist"

    # remove the actual daemons
    rm -rf
    "${MCAVOLUME}/Library/PrivilegedHelperTools/com.faronics.cloudagentd"
```



```
# remove bundle file for localization
rm -rf "${MCAVOLUME}/Library/Application
Support/Faronics/CloudAgent/CloudAgent.bundle"

# remove the receipt
# 10.6 or higher remove the receipt data from the database
pkgutil --forget "com.faronics.pkg.CloudAgent" --volume
"${MCAVOLUME}"

# remove preferences
rm -rf
"${MCAVOLUME}/Library/Preferences/com.faronics.cloudagent.plist"

echo "Uninstall Cloud Agent complete."
else
echo "Could not find volume \"${MCAVOLUME}\"."
fi
```

Uninstalling the Cloud Agent (APFS)

To uninstall the Cloud Agent through the console, go to *Computers* page, select at least one computer and click *Maintenance > Uninstall Cloud Agent*.

To uninstall the Cloud Agent on Mac, create a file with the following script and run it as *sudo <filename>*:

```
#!/bin/sh

# Should be root to run this script
if [ "$EUID" != "0" ]; then
    echo "Error: script must be run as root (use sudo)." 1>&2
    exit 1
fi

# if the user didn't give a volume assume the boot (i.e. root) volume
if [ "$1" = "" ]; then
    MCAVOLUME="/"
else
    if [ -d "/Volumes/${1}" ]; then
        MCAVOLUME="/Volumes/${1}"
    else
```



```
        MCAVOLUME="${1}"
    fi
fi

if [ -d "${MCAVOLUME}" ]; then
    CanRemoveStorageSpace=1;

    if [ -d
"${DFXVOLUME}/Library/PrivilegedHelperTools/com.faronics.deepfreezed.ap
p" ]; then
        BuildVersion=$(/usr/libexec/PlistBuddy -c "Print
CFBundleShortVersionString"
"${DFXVOLUME}/Library/PrivilegedHelperTools/com.faronics.deepfreezed.ap
p/Contents/Info.plist");
        IFS='. ' read -r -a DFVersion <<< "$BuildVersion"

        if [ "${DFVersion[2]}" -eq 520 ]; then
            echo "Error: Uninstall Deep Freeze before Cloud Agent can
be uninstalled."
            exit 1;
        fi

        if [ "${DFVersion[2]}" -eq 220 ]; then
            CanRemoveStorageSpace=0;
        fi
    fi

    if [ "${CanRemoveStorageSpace}" -eq 1 ]; then
        echo "Uninstalling StorageSpace from \"${MCAVOLUME}\"."

        launchctl bootout system
"${MCAVOLUME}/Library/LaunchDaemons/com.faronics.storagespaced.plist"

        rm -rf
"${MCAVOLUME}/Library/LaunchDaemons/com.faronics.storagespaced.plist"

        rm -rf
"${MCAVOLUME}/Library/PrivilegedHelperTools/com.faronics.storagespaced"

        pkgutil --forget "com.faronics.pkg.storagespace" --volume
"${MCAVOLUME}"
    fi
fi
```



```
rm -rf
"${MCAVOLUME}/Library/Preferences/com.faronics.storagespaced.plist"

diskutil apfs deleteVolume "${MCAVOLUME}/Library/Application
Support/Faronics/Private/StorageSpace"

rm -rf "${MCAVOLUME}/Library/Application
Support/Faronics/Private/StorageSpace"

echo "Uninstall StorageSpace complete."
fi

echo "Uninstalling Cloud Agent from \"${MCAVOLUME}\"."

launchctl bootout system
"${MCAVOLUME}/Library/LaunchDaemons/com.faronics.cloudagentd.plist"

rm -rf
"${MCAVOLUME}/Library/LaunchDaemons/com.faronics.cloudagentd.plist"

rm -rf
"${MCAVOLUME}/Library/PrivilegedHelperTools/com.faronics.cloudagentd"

rm -rf "${MCAVOLUME}/Library/Application
Support/Faronics/Private/StorageSpace/CloudAgent"

pkgutil --forget "com.faronics.apfs.pkg.cloudagent" --volume
"${MCAVOLUME}"

rm -rf
"${MCAVOLUME}/Library/Preferences/com.faronics.cloudagentd.plist"

echo "Uninstall Cloud Agent complete."
else
echo "Could not find volume \"${MCAVOLUME}\"."
fi
```



User Management

This chapter describes the process of editing your profile and managing users.

Topics

[My Profile](#)

[Organization Settings](#)

[User Management](#)



My Profile

Once you log on to the Deep Freeze Cloud Console, you can edit your profile. Complete the following steps to edit your profile:

1. Click [*Your_User_Name@company.com*] at the top right corner of the Deep Freeze Cloud Console. For example, *user@company.com*.
2. Select My Profile.
3. Edit the following details:
 - > First Name
 - > Last Name
 - > Job Title
 - > Company
 - > Phone
 - > Email – this field is created when the Administrator creates the account and cannot be edited.
 - > Country
 - > State
 - > Time Zone
 - > Date format (dd-MMM-yyyy/dd-MM-yyyy/MM-dd-yyyy)
 - > 2-Factor Authentication ([Enabling 2-Factor Authentication/Disabling 2-Factor Authentication](#))

Note that when the global [2-Factor Authentication \(2FA\)](#) is enabled for the whole Organization, the option to disable the *2-Factor Authentication* under *My Profile* is disabled.
 - > Password – click *Change Password* to change the current password.
 - > Email Subscriptions
 - ~ Service Expiry – select this option to enable automatic notifications via email before subscriptions expire.
 - ~ Receive Ticketing Alerts on Email – select this option to enable receiving email alerts when a ticket has been submitted.
 - > Enable Features – select Handout to enable this feature in the menu bar. By default, this feature is disabled.
4. Click *Save*.

Enabling 2-Factor Authentication

Deep Freeze Cloud optionally provides enhanced security by providing 2-Factor Authentication. On enabling 2-Factor Authentication, you will be sent a code after entering your password. This six-digit code will be sent via email. You must enter the six-digit code to log on to Deep Freeze Cloud.

Complete the following steps to enable 2-Factor Authentication:



1. Click [Your_User_Name@company.com] at the top right corner of the Deep Freeze Cloud Console. For example, *user@company.com*.
2. Select *My Profile*.
3. Click *Setup* for 2-Factor Authentication.
4. Re-enter your password and click *Enable*.
5. A six-digit code is sent to you via email. Enter the code within two minutes and click *Confirm*. 2-Factor Authentication is now enabled.

If you want Deep Freeze Cloud to trust the computer, select the *Trust this computer* checkbox. Trusted computers only ask for verification codes once every 30 days.

Disabling 2-Factor Authentication

Complete the following steps to disable 2-Factor Authentication:

1. Click [Your_User_Name@company.com] at the top right corner of the Deep Freeze Cloud Console. For example, *user@company.com*.
2. Select *My Profile*.
3. Click *Turn Off* for 2-Factor Authentication.
4. Re-enter your password and click *Turn Off*.
5. A six-digit code is sent to you via email. Enter the code within 2 minutes and click *Confirm*. 2-Factor Authentication is now disabled.



Organization Settings

The Organization Settings page allows administrators to configure the settings for retaining logs and historical data related to *Task Status*, *Alerts and Notifications*, *Reports Data*, and *Computer Usage Data*.

Specify the duration for how long to keep the data for the following:

- Task Status: 1 week (recommended), 2 weeks, 1 month
- Alerts and Notifications: 1 week (recommended), 2 weeks, 1 month
- Reports Data: 2 weeks, 1 month, 3 months (recommended), 6 months
- Computer Usage Data: 2 weeks, 1 month, 3 months (recommended), 6 months

For example, when *Reports Data* is configured to retain logs for 1 month, only data from the past month will be available when generating reports.

Note that any data outside the selected data retention period will be permanently removed and cannot be restored.



Longer duration logs will affect the performance of reports and page load time of tasks.



User Management

You can add users, invite them to use the Deep Freeze Cloud Console, and perform multiple user related administrative tasks. The configuration options for User Management are explained further in this chapter.

- [Add User](#)
- [Edit User](#)
- [Send Invite Email](#)
- [Send Password Reset Email](#)
- [Clone User](#)
- [Disable User](#)
- [Delete User](#)
- [Tag](#)
- [2-Factor Authentication \(2FA\)](#)
- [Active Directory Users](#)
- [SAML Integration](#)

Add User

Only Super Administrators and Administrators can add users.

Complete the following steps to add a user:

1. Go to [*Your_User_Name@company.com*] at the top right corner of the Deep Freeze Cloud Console.
2. Select *User Management*.
3. Click *Add User*.
4. Specify the value for the following:
 - > First Name
 - > Last Name
 - > Email
 - > Sites
 - > Groups (Deep Freeze Limited Administrator only)
 - > Features (Administrator only)
 - ~ Allow User Management
 - ~ Allow AD User Management
 - ~ Manage Handout
 - ~ Manage General Settings
 - ~ Manage Deep Freeze
 - ~ Manage Deep Freeze Mac
 - ~ Manage Data Igloo
 - ~ Manage Software Updater



- ~ Manage Anti-Executable
- ~ Manage WINSelect
- ~ Manage Cloud Sync
- ~ Manage Usage Stats
- ~ Manage Incident Reporting
- ~ Manage Power Save
- ~ Manage Anti-Virus
- ~ Manage Imaging
- ~ Manage Remote
- ~ Manage Ticketing
- > Action (Deep Freeze Limited Administrator and Teacher Administrator only)
- > Tags
- > Permission – assign the permission from the drop-down.
 - ~ Allow Deep Freeze Actions – This option is only available for Remote Connect Only Administrators. When selected, this will enable Remote Connect Only Administrators to perform Deep Freeze Actions on computers.
 - ~ Allow Upgrade Services – This option is only available for Remote Connect Only Administrators. When selected, this will allow Remote Connect Only Administrators to update outdated services on computers. When enabled, the Upgrade Services will be performed regardless of the maintenance mode configuration under the policy.

The following table explains the permission for each type of User Role:

User Roles	Super Administrator	Administrator	Reporting Administrator	Deep Freeze Limited Administrator	Teacher Administrator	Remote Connect Only Administrator
Widgets	Yes	Yes	Yes	Yes		
Manage Features	Yes	Yes				
Manage Policies	Yes	Optional				
Manage Groups	Yes	Yes				
Upgrade	Yes	Yes				
Delete Computers	Yes	Yes				
Reports	Yes	Yes	Yes			
Utilities	Yes	Yes				
My Profile	Yes	Yes	Yes	Yes	Yes	Yes
User Management	Yes	Optional				



User Roles	Super Administrator	Administrator	Reporting Administrator	Deep Freeze Limited Administrator	Teacher Administrator	Remote Connect Only Administrator
Help and Support	Yes	Yes	Yes	Yes		
Deep Freeze on Demand	Yes	Yes		Yes		
Task Management	Yes	Yes		Yes		
My Sites	Yes	Yes		Yes		
Handout	Yes	Optional			Yes	
Remote Connect	Yes	Yes				Yes

5. Disabled – When selected, the user account will be disabled and not be able to log in.
6. Click *OK*.

Edit User

Complete the following steps to edit a user:

1. Go to `[Your_User_Name@company.com]` at the top right corner of the Deep Freeze Cloud Console.
2. Select *User Management*.
3. Select a user.
4. Select *More Actions > Edit*. (Alternatively, select the edit icon for the user.)
5. Edit the value for the following:
 - > First Name
 - > Last Name
 - > Permission – assign the permission from the drop-down.
 - > Sites
 - > Groups (Deep Freeze Limited Administrator only)
 - > Features (Administrator only)
 - ~ Allow User Management
 - ~ Allow AD User Management
 - ~ Manage Handout
 - ~ Manage General Settings
 - ~ Manage Deep Freeze
 - ~ Manage Deep Freeze Mac
 - ~ Manage Data Igloo
 - ~ Manage Software Updater
 - ~ Manage Anti-Executable
 - ~ Manage WINSelect



- ~ Manage Cloud Sync
 - ~ Manage Usage Stats
 - ~ Manage Incident Reporting
 - ~ Manage Power Save
 - ~ Manage Anti-Virus
 - ~ Manage Imaging
 - ~ Manage Remote
 - ~ Manage Ticketing
 - > Action (Deep Freeze Limited Administrator and Teacher Administrator only)
 - > Tags
6. Click OK.

Send Invite Email

The administrator has the ability to send an Invite Email to Cloud Users inviting them to log on to the Deep Freeze Cloud. The Invite Email contains a link that will allow the new users to log on to the Deep Freeze Cloud.

Complete the following steps to send an invite email to the user:

1. Go to [Your_User_Name@company.com] at the top right corner of the Deep Freeze Cloud Console.
2. Select *User Management*.
3. Select a user.
4. Select *More Actions* > *Send Invite Email*.



An invite email can only be sent to users who have an email address specified. Users who do not have an email address specified (Active Directory Groups, Active Directory Organizational Units, or Active Directory users without an email address) cannot be sent an invite email.

Send Password Reset Email

Complete the following steps to send a password reset email to Cloud Users:

1. Go to [Your_User_Name@company.com] at the top right corner of the Deep Freeze Cloud Console.
2. Select *User Management*.
3. Select a user.
4. Select *More Actions* > *Send Password Reset Email*.

An email with the request to reset password is sent.



Clone User

You can clone a Cloud User if you are adding multiple users for your organization. This saves time since you can avoid entering many details that may be common between users. Complete the following steps to clone a user:

1. Go to [Your_User_Name@company.com] at the top right corner of the Deep Freeze Cloud Console.
2. Select *User Management*.
3. Select a user.
4. Select *More Actions > Clone User*.
5. Edit the value for the following:
 - > First Name
 - > Last Name
 - > Email
 - > Permission – assign the permission from the drop-down.
 - > Sites
 - > Groups (Deep Freeze Limited Administrator only)
 - > Features (Administrator only)
 - > Action (Deep Freeze Limited Administrator and Teacher Administrator only)
 - > Tags
6. Click OK.

Disable User

The Disable User option is used to temporarily restrict a Cloud User from logging on to the Deep Freeze Cloud. Complete the following steps to disable a user:

1. Go to [Your_User_Name@company.com] at the top right corner of the Deep Freeze Cloud Console.
2. Select *User Management*.
3. Select a user or multiple users.
4. Select *More Actions > Disable User*.

Delete User

Complete the following steps to delete a user:

1. Go to [Your_User_Name@company.com] at the top right corner of the Deep Freeze Cloud Console.
2. Select *User Management*.
3. Select a user or multiple users.
4. Select *More Actions > Delete User*.

Tag

Complete the following steps to add a Normal Tag, Ticket or a Location Tag:



1. Go to [Your_User_Name@company.com] at the top right corner of the Deep Freeze Cloud Console.
2. Select *User Management*.
3. Select a user.
4. Select *More Actions > Tag*.
5. Click *OK*.

2-Factor Authentication (2FA)

2-Factor Authentication (2FA) is an identity and access management security method that adds an extra layer of security for your Deep Freeze Cloud account.

Enabling 2-Factor Authentication requires you to enter your password.

When enabled, all users in the Organization logging in to Deep Freeze Cloud will need to enter a six-digit verification code (received through email).



Only users with Super Administrator and Administrator permission rights can enforce 2-Factor Authentication for the Organization.

Enabling 2-Factor Authentication

Complete the following steps to enable 2-factor authentication:

1. Go to *User Management*.
2. Click *2-Factor Authentication > Enable*.
3. Enter your password to enable 2-factor authentication.

Note that this will enable 2-factor authentication for all users in this Organization.

4. Click *Enable*.

Once enabled, users will be sent a 6-digit code through email, which they will need when signing in to Deep Freeze Cloud.



During sign-in, users have the option to *Trust This Computer*. When this option is selected, users will not be asked for a verification code when signing in for 30 days.

When the global 2-Factor Authentication (2FA) is enabled for the whole Organization, the option to enable/disable the 2-Factor Authentication under *My Profile* is disabled.

Disabling 2-Factor Authentication

Complete the following steps to disable 2-factor authentication:

1. Go to *User Management*.



2. Click *2-Factor Authentication > Disable*.
3. Enter your password to disable 2-factor authentication.
4. Click *Disable*.

When the global 2-Factor Authentication is disabled for the whole Organization, the settings in the 2-Factor Authentication under *My Profile* is retained and can be configured.

Active Directory Users

Deep Freeze Cloud provides the ability to add users directly from your Active Directory. The first step is to integrate Deep Freeze Cloud with your Active Directory domain.

Active Directory Integration

Complete the following steps for Active Directory (AD) Integration:

1. Go to *User Management*.
2. Click *AD Integration*.
3. Click *Add Domain*.
4. Click *Download AD Authenticator*.
5. Double-click *Faronics AD Authenticator.exe* to run the installer.
6. Accept the License Agreement.
7. Click *Install*.
8. Click *Finish*.

Once the AD Authenticator is installed, the domain is shown on the *AD Integration* page.



- Faronics AD Authenticator must be installed on a computer that is connected to the domain.
- Faronics AD Authenticator keeps the connection alive between the computer where it is installed and Deep Freeze Cloud.
- The computer where the Faronics AD Authenticator is installed must always be on for Deep Freeze Cloud to connect to the Active Directory.

Add Active Directory Users

Complete the following steps to add Active Directory users:

1. Select *User Management*.
2. Click *Add User > Add AD Users*.
3. In the Add Users dialog, select the *Domain*. Enter the user name in the search box and click *Search*.
4. Select the user and click *Next*.
5. Configure the permission for the user:
 - > Super Administrator
 - > Administrator



- > Reporting Administrator
 - > Deep Freeze Limited Administrator
6. Select the Site.
 7. Specify the tags.
 8. Click *Next*.
 9. Click *Add Users*.



When an Active Directory user logs on to Deep Freeze Cloud, they must enter the user name, password and Domain Identifier. The Domain Identifier is sent to the user via email once the account is created in Deep Freeze Cloud.



It is the administrator's responsibility to delete a user from the Windows Active Directory when the user is not working in your organization.

Add Active Directory Group / Organizational Unit

Adding an Active Directory Group / Organizational Unit gives the flexibility to assign permissions directly to a group of users. Different user groups can be assigned different permissions as per your requirement.

Complete the following steps to add Active Directory groups/ Organizational Units:

1. Select *User Management*.
2. Click *Add User > Add AD Groups / OU*.
3. In the Add Groups dialog, select the *Domain*. Enter the name of the group in the search box and click *Search*.



The Organizational Unit on this dialog represents a group of users.

4. Select the group and click *Next*.
5. Configure the permission for the group:
 - > Super Administrator
 - > Administrator
 - > Reporting Administrator
 - > Deep Freeze Limited Administrator
6. Select the Site.
7. Specify the tags.
8. Click *Next*.



9. Click *Add Group*.



- When a user belonging to an Active Directory Group logs on for the first time, the user is created in Deep Freeze Cloud.
- An Active Directory user belonging to a particular group inherits the permission of the group. The Inherit AD Group permissions and sites settings checkbox is automatically selected. If this checkbox is cleared manually, the user will not inherit Active Directory group permissions. The user will then be converted to a individual Active Directory user.
- If the Active Directory user is part of two groups with higher and lower permission, the user will inherit the lower permissions.
- An Active Directory user belonging to multiple groups will be able to access the Deep Freeze Cloud Sites belonging to the group with lower permission.

SAML Integration

There are 3 steps to complete SAML integration:

Step 1: Configuring Identity Providers

Step 2: Configuring SAML settings in Deep Freeze Cloud

Step 3: Assigning Access to Deep Freeze Cloud Through the Identity Providers (IdP-initiated login)

Supported Identity Providers include:

- [OneLogin](#)
- [Azure](#)
- [Google Workplace](#)
- Okta

OneLogin

Step 1: Configuring OneLogin

After logging in to OneLogin, set up Deep Freeze under *Applications*.

1. In the search field, type in *SAML Test Connector*.
2. Select *SAML Test Connector (IdP w/ attr w/ sign response)*.
3. Assign a *Display Name* and click *Save*.
4. On the left pane, click *SSO*.
5. At the top right, click *More Actions > SAML Metadata* to download the IdP Metadata.
6. After you have downloaded the IdP Metadata, go to Deep Freeze Cloud to configure [Step 2: SAML Settings in Deep Freeze Cloud](#) and obtain the *Service Provider Configuration* information.
7. After you have configured Deep Freeze and generated the Service Provider Configuration, click *Configuration* on the left pane.
8. Fill in the *Audience* field using the Deep Freeze Cloud *Audience URI*.



9. Fill in the *Recipient*, *ACS (Consumer) URL Validator*, and *ACS (Consumer) URL* fields using the Deep Freeze Cloud *Assertion Consumer URL*, then click *Save*.
10. On the left pane, click *SSO*.
11. Under *SAML Signature Algorithm*, select *SHA-256* or *SHA-512*.



Currently, only SHA-256 and SHA-512 SAML signature algorithms are supported.

12. Click *Save*.
- OneLogin setup is now completed.

Step 2: SAML Settings in Deep Freeze Cloud

Complete the following steps to configure Deep Freeze Cloud SAML settings for SAML integration:

1. Go to *User Management*.
2. Click *SAML Integration*.
3. Configure the parameters for the Identity Provider, Other Settings and Service Provider.
 - > Service Provider Configuration

Click the refresh button to update the Service Provider Configuration tab and display the assigned *Login Domain*, *Audience URI* and *Assertion Consumer URL*.
 - > Identity Provider Setup

Upload the IdP metadata or perform manual setup.

Upload IdP metadata

 - i. To upload the IdP metadata, click *Browse* and select the IdP Metadata (.xml) file that you have downloaded. All other fields will be automatically populated.
 - ii. Click *Next*.

Manual setup

To manually set up the Identity Provider:

 - i. Enter the information for the IdP Login URL and Entity ID.
 - ii. Click *Browse* and select the IdP Certificate file.
 - iii. Click *Next*.
 - > Settings
 - i. Select the permission rights for *Just in Time Provisioned* users.
 - * Allow access to all sites – Select this option to allow new users access to all sites. By default, new users do not have permission to access any site.



Attribute Mapping

The Attribute Mapping tab contains information mapped from the IdP metadata. You can choose to use the generated information as is or edit the fields by clicking the edit icon.

When editing the email, first name, and last name fields, fill in the details using the format *user.email*, *user.firstName*, *user.lastName*.

You can assign a specific identifier by selecting the *Use Custom Attribute Instead of NameID For Uniquely Identifying A User* checkbox and editing the information on the *Custom Attribute* field.

Click *Next* after you have finished editing.



You will need the *Audience URI* and *Assertion Consumer URL* to complete the setup in the Identity Provider portals.

To edit SAML settings, click *Edit* at the top right.

To reset SAML settings, click *Reset* at the top right. Note that resetting SAML settings will unlink the IdP and delete all the SAML settings.

Step 3: Assigning Access to Deep Freeze Cloud Through OneLogin (IdP-initiated login)

OneLogin Users must be assigned access to Deep Freeze before being able to access Deep Freeze through OneLogin.

To assign access to a user:

1. Go to *Users* and select a user.
2. On the *Users* page, click *Applications* on the left pane.
3. Click the + icon on the top right of the *Applications* tab.
4. Select the app from the drop-down list and click *Continue*.
5. Edit the app login details for the selected user and click *Save*.

The user can now access Deep Freeze through OneLogin.

To perform IdP-initiated access, log in to your OneLogin company portal. Click on the Deep Freeze app. You will be redirected to Deep Freeze Cloud.

Add SAML User

SAML Users are created or assigned in OneLogin. See [Step 3: Assigning Access to Deep Freeze Cloud Through OneLogin \(IdP-initiated login\)](#).

SAML users have the ability to perform the following actions:

- Edit
- Disable
- Delete
- Tag



Azure

Step 1: Configuring Azure

After logging in to the Azure Portal, click *Azure Active Directory*.

1. On the left pane, click *Enterprise Applications*, then click *New Application*.
2. Click *Create your own application*.
3. Specify a name for the app and select *Integrate any other application you don't find in the gallery*.
4. Click *Create*.
5. On the Application Overview page, under Getting Started, click on *Set up single sign on*.
6. Click *SAML*.
7. Edit the Basic SAML Configuration:
Refer to [Step 2: SAML Settings in Deep Freeze Cloud](#) for the information needed to fill in the basic SAML configuration.
 - > Fill in the *Identifier (Entity ID)* using the Deep Freeze Cloud *Audience URI*.
 - > Fill in the *Reply URL (Assertion Consumer Service URL)* using the Deep Freeze Cloud *Assertion Consumer URL*.
 - > Fill in the *Sign on URL* using the Deep Freeze Cloud *Assertion SAML Login URL*.
8. Click *Save*.
9. Under User Attributes & Claims, replace existing Claims with the following details:
 - > user.lastname – user.surname
 - > user.firstname – user.givenname
 - > user.email – user.localuserprincipalname
 - > name – user.userprincipalname
 - > Unique User Identifier – user.userprincipalname
10. Under SAML Signing Certificate, click *Add a Certificate*.



If you are resetting your SAML, you will need to create a new certificate for the new SAML. Old certificates need to be deleted.

11. Click *New Certificate*.
12. Select your preferred *Signing Option* and *Signing Algorithm*.
13. Specify the *Notification Email Address* and click *Save*.
14. Click on the Thumbprint field to display options for the certificate and select *Make certificate active*.
15. Close the SAML Signing Certificate screen to return to the SAML-based Sign-on screen.
16. Click *Download* to download the Federation Metadata XML.
17. Complete the steps for [Step 2: SAML Settings in Deep Freeze Cloud](#).



Step 3: Assigning Access to Deep Freeze Cloud Through Azure (IdP-initiated login)

1. On the left pane, click *Users and Groups*.
2. Click *Add User*.
3. On the Add Assignment page, click *Users* to display the list of all users. Select the desired users from the list and click *Select*.
4. Click *Assign*.

Google Workplace

Step 1: Configuring Google Workplace

After logging in to Google Admin, navigate to Apps.

1. Click *Add App > Add Custom SAML App*.
2. Assign the *App Name* and click *Continue*.
3. Click *Download Metadata* to download the IdP Metadata.
4. After you have downloaded the IdP Metadata, complete [Step 2: SAML Settings in Deep Freeze Cloud](#).
5. On the Google Admin console, edit the Service Provider Details:
 - > Fill in the *ACS URL* using the Deep Freeze Cloud *Assertion Consumer URL*.
 - > Fill in the *Entity ID* using the Deep Freeze Cloud *Audience URI*.
6. Click *Continue*.
7. Click *Add Mapping*. Fill in the 3 required *App Attributes* in the following format:
 - > Primary email – user.email
 - > First name – user.firstName
 - > Last name – user.lastName
8. Click *Finish*.

Step 3: Assigning Access to Deep Freeze Cloud Through Google Workplace (IdP-initiated login)

1. From the Google Admin console Home page, go to *Apps > Web And Mobile Apps*.
2. Select your SAML app.
3. Click *User Access*.
4. On the left pane, select the Organizational Unit from the left and select *On For Everyone*.
5. Click *Save*.

Logging in to Deep Freeze Cloud Using SAML (SP-initiated login)

1. On Deep Freeze Cloud sign-in page, click on *More Sign-in Options* and select *Login with SAML*.
2. Enter your *Login Domain* name in the *Domain Identifier* field.
3. Click *Sign In*.





Managing Sites

This chapter describes creating and managing Sites in Deep Freeze Cloud.

Topics

[Overview](#)

[Creating a Site](#)



Overview

A Site is a group of computers managed by Deep Freeze Cloud. Sites may be different physical locations or computers in logical groups. For example, you may create multiple Sites to classify computers California and New York. You can also create multiple sites for different departments like Accounts and Sales.

Types of Sites:

- Deep Freeze Enterprise Site – If you connect Deep Freeze Enterprise to Deep Freeze Cloud, a Deep Freeze Enterprise Site is created automatically. All computers managed by Deep Freeze Enterprise can now be managed by Deep Freeze Cloud.
- Deep Freeze Cloud Site – Computers managed exclusively by Deep Freeze Cloud form part of a Deep Freeze Cloud Site.



A unique site is created for one instance of Deep Freeze Enterprise Console. If you have x number of Deep Freeze Enterprise Consoles, you must connect each of them to Deep Freeze Cloud. Consequently, you will have x number of Deep Freeze Enterprise sites.



If you are not using Deep Freeze Enterprise Console, you will only see the Deep Freeze Cloud Sites on Deep Freeze Cloud.



To view the number of computers or devices per Site, click *Show Device Count*.



Creating a Site

Complete the following steps to create a site:

1. Go to *[Default_Site] > Create New Cloud Site*.
2. Specify the following settings:
 - > Site Name – specify a unique name for the site.
 - > Make Default Site – select the checkbox if this will be the default site.
 - > Search User – enter the name of the user to search for a particular user.
3. Select the user and click *OK*.



Computers cannot be moved between Sites.



If you are a Deep Freeze Enterprise user, you will not be able to create a Cloud Site.





Using Deep Freeze Cloud Console

This chapter describes using the Deep Freeze Cloud Console.

Topics

- [Home](#)
- [Computers](#)
- [Groups](#)
- [Policies](#)
- [Applications](#)
- [Windows Updates](#)
- [Imaging](#)
- [Inventory](#)
- [Tickets](#)
- [General Settings](#)
- [Deep Freeze Service](#)
- [Data Igloo Service](#)
- [Software Updater Service \(Windows\)](#)
- [Anti-Executable Service](#)
- [WINSelect Service](#)
- [Cloud Sync](#)
- [Usage Stats Service](#)
- [Incident Reporting Service](#)
- [Ticketing Service](#)
- [Power Save Service](#)
- [Imaging Service](#)
- [Remote Connect Service](#)
- [Anti-Virus Service](#)
- [Deep Freeze Mac Service](#)
- [Software Updater Service \(Mac\)](#)
- [Anti-Virus Service \(Mac\)](#)
- [Reports](#)
- [Utilities](#)
- [Alerts](#)



Home

The home page on the Deep Freeze Cloud helps you monitor and manage the computers on the network. The components on the home page are explained further in this chapter.

- [Widgets](#)
- [Install Cloud Agent](#)
- [Manage Policies](#)
- [Task Status](#)

Widgets

Deep Freeze Cloud provides multiple widgets to visually display the health of your managed computers. Widgets are available for all the services.

- To add a widget on the home page, click *Add Widgets*.
- Click *Add* to add a widget to the home page.
- Click *Remove* to remove a widget from the home page.

Install Cloud Agent

The Cloud Agent must be installed on the computers to manage via Deep Freeze Cloud. For detailed information, see [Installing the Cloud Agent](#).

Manage Policies

A Policy is a group of settings for various Services. You can create a Policy and apply it to the managed computers. For detailed information, see [Policies](#).

Task Status



Click *Task Status* icon to view and manage all tasks performed on the computers within the last 30 days. Executed tasks older than 30 days will be archived and kept in history for up to 365 days.

- Select one or more tasks and click *Cancel Task* to cancel the selected tasks.
- Select one or more tasks and click *Retry Task* to retry the selected tasks.
- Click *Download Archived Tasks* to download the archived tasks.
- Click *Refresh* to update the Tasks list.



The following fields are displayed:

- Computers tab
 - > Computer Name
 - > Computer Last reported
 - > Task Name
 - > Status
 - > Initiated by
 - > Initiated at
 - > Completed at
- MDM tab
 - > Device Name
 - > Task Name
 - > Status
 - > Initiated by
 - > Initiated at
 - > Completed at

The Tasks list refreshes automatically every few minutes. You can also manually refresh the page by clicking the *Refresh* button.



Computers

The Computers page lists the managed computers on your network. You can apply Policies for various services from the Computers page. The configuration options on the Computers page are explained further in this chapter.



A policy that is outdated will be displayed in red text with an *Outdated* tooltip.

- [Live Actions](#)
- [Client Information](#)

Live Actions

Deep Freeze Cloud allows you to perform Live Actions on managed computers. The Live Actions are executed on the managed computers in realtime.



The Live Actions are retrieved from Deep Freeze Cloud Console as follows:

- 1 computer reporting to the Cloud Agent – 6 minutes
- 2-9 computers reporting to the Cloud Agent – 3 minutes
- >10 computers reporting to the Cloud Agent – 1 minute

Deep Freeze Cloud can execute Live Actions on the managed computers with the Cloud Agent which are executed immediately.



The managed computers check for updated policies based on the heartbeat specified in [Cloud Agent Settings](#). This action is independent of the Live Actions.



Disabling Live Actions will cause all the live actions for all the products except Deep Freeze to stop working. It will also disable all the actions from the Deep Freeze Administrator Mobile app.



Most of the Deep Freeze actions can be performed through Live actions. Live Actions can also be performed from the Deep Freeze On Demand page by installing a Cloud Relay. For more information go to [Cloud Relay](#).



Select one or more computers and execute the following Live Actions:

Wakeup

Wakes up the selected computers.

Restart

Restarts the selected computers.

Shutdown

Shuts down the selected computers.

Maintenance

- Send Message – sends a message to the selected computers. Specify a message and click *Send*.
- Lock Keyboard and Mouse – locks the keyboard and mouse on the selected computers.
- Unlock Keyboard and Mouse – unlocks the keyboard and mouse on the selected computers.
- Run Maintenance Period – runs the Maintenance Period on the selected computers. All the settings are applied as per the settings in *General Settings > Maintenance Period* tab. *Shutdown after maintenance period* option in the Maintenance Period settings will be ignored if enabled.
- End Maintenance Period – ends the Maintenance Period on the selected computers.
- Upgrade Services – upgrades the services on the selected computers to the latest version.



Services with updates available will display the current version installed on the computer along with the latest versions available for installation. Updates will be performed automatically if enabled in the maintenance schedule.

- Delete Computers – deletes the computers from the database.
- Uninstall Cloud Agent – uninstalls the Cloud Agent from the selected computers.



For Mac computers without Cloud connection, you need to run the script to uninstall Cloud Agent.

Tag

Select one or more computers and click *Tag*. Specify the tag and click *OK*.

Move to Group

Select one or more computers and go to *Move to Group > [Group Name]*.



You can also select *Manage Groups* to create a new group.

For more information, refer to the [Groups](#) section.



Enforced Policy assigned for each group is displayed in the drop-down list. When assigning or moving computers to that group with the enforced policy, the new policy will be pushed to the computers and override the current policy.

Assign Policy

Select one or more computers and go to *Assign Policy* > [Policy Name].

You can also select *Manage Policies* to create a new policy.

For more information, refer to the [Policies](#) section.



It will not be possible to assign a normal Windows computer type policy to a Server machine through the console .

It will not be possible to move a Server machine to a group which has a policy enforcement with a computer type policy.

Deep Freeze

- Reboot Frozen – reboots the computers in Frozen state.
- Reboot Thawed – reboots the computers in Thawed state.
- Reboot Thawed Locked – reboots the computers in Thawed state and locks the computer so a non-administrator cannot log on.
- More Actions – perform more Deep Freeze actions on your computer. Refer to [Deep Freeze Actions](#).

For *Reboot Thawed* and *Reboot Thawed Locked*, you can select the *Thaw Computer(s) for Next X Restarts* and assign the number of restarts.

Selecting this option will reboot the computer in Thawed or Thawed Locked state for the assigned restarts.

For example, when you assign '3' as the number of restarts, the computer will remain in a Thawed or Thawed Locked state after rebooting the next 3 times.

The maximum number of times you can select to reboot the computer in Thawed or Thawed Locked state is 99.

WINSelect

- Enable Protection – enables WINSelect protection on the selected computers.
- Disable Protection – disables WINSelect protection on the selected computers.

Anti-Executable

- Enable Protection – enables Anti-Executable protection on the selected computers.
- Disable Protection – disables Anti-Executable protection on the selected computers.



- Enable Maintenance Mode – enables Maintenance Mode on the selected computers.
- Initiate a Local Control Scan – Initiate a Local Control List scan on the selected computer(s). You can also choose to *Add DLLs When Creating the Local Control List*.

Anti-Virus

- Scan – initiate a Quick Scan, Deep Scan or Abort, Resume and Pause an ongoing scan.
- Fix Now – downloads the latest virus definition and scans the selected computers.
- Enable Firewall – enables the firewall on the selected computers.
- Disable Firewall – disables the firewall on the selected computers.
- Enable Active Protection – enables the Active Protection.
- Disable Active Protection – disables the Active Protection.
- Review Quarantined Files – click to display the list of quarantined files across selected computers within the network. You can choose to restore or delete quarantined files.



Quarantined items will be deleted as per the assigned policy settings. Restored files will be temporarily added to the Active Protection exceptions list. To prevent the item from being quarantined again, specify safe files or folders under Scan Exception in the applied Anti-Virus Policy.

Power Save

- Enable Power Management – enables power management on the selected computers.
- Disable Power Management – disables power management on the selected computers.
- Assign Energy Consumption Profiles – assign pre-defined Energy Consumption Profiles to selected computers or add an Energy Consumption Profile.

Adding an Energy Consumption Profile

An Energy Consumption Profile is a customized set of values to specify power consumption of Monitors and Computers running in full capacity and on standby mode, and cost of per kilowatt hour.

To add an Energy Consumption Profile:

1. Select *Assign Energy Consumption Profiles > Manage Energy Consumption Profiles > Add Energy Consumption Profiles*.
2. Specify the value for the following fields:
 - > Name
 - > *Watts On* and *Watts Standby* for Monitors.
 - > *Watts On* and *Watts Standby* for Computers.
3. Click OK.

Remote Connect

- RDP – enables connecting remotely to the selected computer.



A user that is logged in will be asked for permission if the *Ask User Permission To Remotely Access Computer* is enabled in the policy. Once permission is granted, the current user will be locked out.

- VNC – enables accessing computers remotely and assisting end users

A user that is logged in will be asked for permission if the *Ask User Permission To Remotely Access Computer* is enabled in the policy.

User permission will be requested during remote connection if someone is logged into the computer.

- Remote Pro

Once access is gained, the following actions can be performed:

- > Enable/Disable Mouse Tracking

This feature tracks the movement of the cursor as the mouse points to a component or element on the screen during remote sessions. This option is enabled by default.

- > File Explorer

This feature opens the *File Explorer* on the remote computer.

- > Run

This feature opens the Run dialog to execute Run commands on the remote computer.

- > Send Alt + Tab

This action switches between applications/windows that are running/open on the remote computer and is only available during Remote sessions.

- > Send Ctrl + Alt + Delete

This action sends the CTRL + ALT + DEL command to the remote computer.

- > Show Desktop (Windows)

This feature minimizes all open windows and applications to make the desktop background visible on the remote computers.

- > Enable/Disable Clipboard Sharing

This feature minimizes all open windows and applications to make the desktop background visible on the remote computers. This option is enabled by default.

- > Upload

This feature allows sending files (up to a maximum of 25 MB) to the remote computer during Remote sessions.

- > Download

This feature allows downloading files (up to a maximum of 25 MB) from the remote computer during Remote session.



Files can only be sent to remote computers if a user is logged in. By default, transferred files are saved on the desktop of the current user on the remote computer (for example, Google Remote Desktop).



View By

Select one of the following Services:

- All Services
- [Deep Freeze Service](#)
- [Deep Freeze Mac Service](#)
- [Anti-Executable Service](#)
- [WINSelect Service](#)
- [Software Updater Service \(Windows\)](#)
- [Anti-Virus Service](#)
- [Power Save Service](#)
- [Usage Stats Service](#)
- [Data Igloo Service](#)
- [Incident Reporting Service](#)
- [Cloud Sync](#)
- [Imaging Service](#)
- [Remote Connect Service](#)
- [Ticketing Service](#)

Column Chooser

Click the *Column Chooser* icon to launch the column chooser:

- To add a column, drag and drop the required column from the column chooser to the list of computers.
- To remove a column, drag and drop the column from the list of computers to the column chooser.

Search

Click the search field at the top-right corner above the computer list and enter a search parameter. Additionally, click the search field on the top of each column and enter the search parameter. You can also click the filter on top of each column and filter using conditional parameters. Some examples of conditional parameters are:

- Contains
- Does not contain
- Starts with
- Ends with
- Equals
- Does not equal

Group By

Drag and drop the column title to the message *Drag a column header here to group by that column* to group the list of computers.



Client Information

The *Client Information* page displays the *Client Information*, *Maintenance Status*, as well as details for each of the policy assigned to the computer. Click on the name of the computer to view the *Client Information* page. Where available, click on the links under *Maintenance Status* and policy tabs to view the related reports.



Groups

The Groups page allows you to categorize the computers into different groups. For example, you could categorize computers into various departments such as Finance, Marketing, Sales etc.

The configuration options for Groups are explained further in this chapter.

- [Adding a Group](#)
- [Editing a Group](#)
- [Deleting a Group](#)
- [Active Directory Import](#)
- [Search](#)

Adding a Group

A Group or Organizational Unit refers to a group of computers.

Complete the following steps to add a Group:

1. Click *Add Group*.
2. Specify a *Group Name*. For example, you can specify *Accounts*.
3. Select a *Parent Group*. The newly added Group will be categorized under the Parent Group. The Parent Group must already exist. For example, *Sales* group can be the Parent Group for *Customer Service* since the Customer Service department is part of the Sales department.
4. Select the *Enforced Policy*. This Policy will be applied on all computers belonging to this group. (Not applicable for Windows Server.)
5. Select *Set AD based OU association for this group*. Select this option to associate this group with an Active Directory Organizational Unit. (For more information on Active Directory users and groups go to [Active Directory Users](#)). Specify the following options:
 - > Domain name – select the domain name from the drop-down.
 - > AD Machine OU – select the available Organizational Unit for the selected domain from the drop-down.



If you have upgraded to the latest Cloud Agent on all computers, the Active Directory Organizational Units are automatically visible in the *AD Machine OU* drop-down for the selected domain name.

Once you have created an association between a Group and an Organizational Unit, the Organizational Units are displayed on the *Groups* page. Active Directory integration offers the ability to assign different policies to various Organizational Units based on your requirement.

An Organizational Unit can only be assigned to one Group manually. An Organizational Unit on the Groups page refers to a group of computers.



6. Click *Add*.



If the Parent Group already has an Enforced Policy, the new Group will inherit the policy.

If the Enforced Policy is changed to *None* for a particular Group, the old *Policy* will remain on the computers.

If there was no Enforced Policy for the Group and a new Policy is added to the Group, the new Policy will be enforced on all computers in the Group.

Editing a Group

Complete the following steps to edit a Group:

1. Click the *Edit* button for the Group you want to edit.
2. Edit the *Group Name*.
3. Edit the *Parent Group*.
4. Edit the *Enforced Policy*.
5. Select *Set AD based OU association for this group*. Select this option to associate this group with an Active Directory Organizational Unit. Specify the following options:
 - > Domain name – select the domain name from the drop-down.
 - > AD Machine OU – select the available Organizational Unit for the selected domain from the drop-down.
6. Click *Update*.

Deleting a Group

Complete the following steps to delete a group:

1. Click the X icon for the Group you want to delete.
2. The message *Are you sure you want to delete this group?* is displayed.
3. Click *Yes*.



If a Group is deleted, the computers are assigned to the *Default* group.

Active Directory Import

You can import all the users and group from your Active Directory into the Deep Freeze Cloud Console. For more information, refer to [Active Directory Import Utility](#).

Search

To search a group, enter the keywords and click the search icon.



Policies

The Policies page allows you to create and apply policies on your managed computers. A Policy is a group of settings for one or more Services. The settings for each of the Services are explained further in the chapter.

- [Adding a Policy](#)
- [Editing a Policy](#)
- [Copying a Policy](#)
- [Deleting a Policy](#)
- [Copy to Sites](#)
- [Uninstall Service from a Policy \(some computers\)](#)
- [Scheduled Policy Updates](#)
- [Inheriting Policy Settings](#)



A policy that is outdated will be displayed in red text with an *Outdated* tooltip.

A Policy can be configured for the following services:

- [Deep Freeze Service](#)
- [Data Igloo Service](#)
- [Software Updater Service \(Windows\)](#)
- [Anti-Executable Service](#)
- [WINSelect Service](#)
- [Cloud Sync](#)
- [Usage Stats Service](#)
- [Incident Reporting Service](#)
- [Ticketing Service](#)
- [Power Save Service](#)
- [Imaging Service](#)
- [Remote Connect Service](#)
- [Anti-Virus Service](#)
- [Deep Freeze Mac Service](#)
- [Software Updater Service \(Mac\)](#)
- [Anti-Virus Service \(Mac\)](#)



Adding a Policy

Complete the following steps to add a Policy:

1. Go to the *Policies* page.
2. Click *Add Policy* > *Add New Policy*.
3. Select *Deep Freeze Windows*, *Deep Freeze Windows Server Policy*, *Deep Freeze Mac* or *Faronics Remote Windows*.



Windows Server Policies currently support only Deep Freeze service.

4. Specify the [General Settings](#).
5. Optionally enable and configure one or more of the following services (click each service for detailed settings):
 - > [Deep Freeze Service](#)
 - > [Data Igloo Service](#)
 - > [Software Updater Service \(Windows\)](#)
 - > [Anti-Executable Service](#)
 - > [WINSelect Service](#)
 - > [Cloud Sync](#)
 - > [Usage Stats Service](#)
 - > [Incident Reporting Service](#)
 - > [Ticketing Service](#)
 - > [Power Save Service](#)
 - > [Imaging Service](#)
 - > [Remote Connect Service](#)
 - > [Anti-Virus Service](#)
 - > [Deep Freeze Mac Service](#)
 - > [Software Updater Service \(Mac\)](#)
 - > [Anti-Virus Service \(Mac\)](#)
6. Specify the name of the Policy.
7. Click *Save*.



Select *Make Default Policy* to make the configured policy as the default policy when installing the Cloud Agent. By selecting this option, the Policy will appear under the *Policy* when installing the Cloud Agent.

Click *Restore Default Settings* to replace your current Policy configuration by the default settings.



Editing a Policy

Complete the following steps to edit a Policy:

1. Go to the *Policies* page.
2. Click *Edit Policy* icon for the policy you want to edit.
3. Edit the name of the Policy.
4. Edit one or more of the following services (click each service for detailed settings):
 - > [Deep Freeze Service](#)
 - > [Data Igloo Service](#)
 - > [Software Updater Service \(Windows\)](#)
 - > [Anti-Executable Service](#)
 - > [WINSelect Service](#)
 - > [Cloud Sync](#)
 - > [Usage Stats Service](#)
 - > [Incident Reporting Service](#)
 - > [Ticketing Service](#)
 - > [Power Save Service](#)
 - > [Imaging Service](#)
 - > [Remote Connect Service](#)
 - > [Anti-Virus Service](#)
 - > [Deep Freeze Mac Service](#)
 - > [Software Updater Service \(Mac\)](#)
 - > [Anti-Virus Service \(Mac\)](#)
5. Click *Save*.
6. Select the Policy Update Preference:
 - > Notify the user immediately when the computer checks-in and restart after 2 minutes.
 - > Schedule a time for the policy update to occur – select the date and time.
7. Click *OK*.



A Policy can be applied immediately which will take effect based on the [Cloud Agent Settings](#). Alternatively, you can schedule a Policy Update for a later date.

Copying a Policy

You can copy a policy to reuse the policy with a different name. By copying a policy, you can saving time by not having to configure all the settings again.

Complete the following steps to copy a Policy:

1. Go to the *Policies* page.
2. Click *Copy Policy* icon for the policy you want to copy.



3. Edit the name of the Policy.
4. Optionally configure one or more of the following services (click each service for detailed settings):
 - > [Deep Freeze Service](#)
 - > [Data Igloo Service](#)
 - > [Software Updater Service \(Windows\)](#)
 - > [Anti-Executable Service](#)
 - > [WINSelect Service](#)
 - > [Cloud Sync](#)
 - > [Usage Stats Service](#)
 - > [Incident Reporting Service](#)
 - > [Ticketing Service](#)
 - > [Power Save Service](#)
 - > [Imaging Service](#)
 - > [Remote Connect Service](#)
 - > [Anti-Virus Service](#)
 - > [Deep Freeze Mac Service](#)
 - > [Software Updater Service \(Mac\)](#)
 - > [Anti-Virus Service \(Mac\)](#)
5. Click *Save*.

Deleting a Policy

Complete the following steps to delete a Policy:

1. Go to the *Policies* page.
2. Click *Delete Policy* icon for the policy you want to delete.
3. Click *Yes*.



A Policy cannot be deleted if it is currently assigned to computers.

Copy to Sites

Existing policies can be copied to other sites. Other sites can use these policies for their deployments. This saves valuable time in re-creating the policy with all the settings.

Complete the following steps to copy a policy to another site:

1. Go to *Policies*.
2. Select one or more policies.
3. Click *Copy to Sites*.



4. Select the following:
 - > Site Name – select one or more sites. Alternatively, you can also search for the site in the *Search Site* field.
5. Click *OK*.

The policy is copied to the selected sites.



Password and all sensitive information in the policy will also be copied. Once the original policy is copied to other sites, any changes to the original policy will not be reflected in the copied policies.

The *Copy to Sites* button will only appear if you have more than one site.

Uninstall Service from a Policy (some computers)

If you have assigned computers to a Policy and you want to uninstall some services from a few of those computers, you can do by following a few simple steps.

Complete the following steps to uninstall Services from a Policy:

1. Go to the *Policies* page.
2. Click the [Policy_Name].
3. Click *Copy*.
4. Clear the *Enable Service_Name* checkbox for the services you want to uninstall. For example, you may clear the following checkboxes to uninstall:
 - > Enable Deep Freeze Cloud
 - > Enable Software Updater
 - > Enable Anti-Executable
 - > Enable WINSelect
 - > Enable Anti-Virus
 - > Enable Power Save
5. Edit the name of the Policy to [New_Policy_Name].
6. Click *Save*.
7. Go to the *Computers* page. Select the computers from where the Services need to be uninstalled.
8. Go to *Assign Policy* and select [New_Policy_Name].
9. The [New_Policy_Name] is applied and the Services are uninstalled.

Scheduled Policy Updates

To view the Policy updates scheduled on computers across your network, go to *Policies > Scheduled Policy Updates*.

Cascading Policies

The Scheduled Policy Updates display the list of policies when a new policy is applied on a computer or an existing policy is updated.

Scheduled Policy Updates are displayed as follows:



- Windows computers – New or updated policies are queued sequentially and stored on the computers. The policies are applied in a cascading manner as per the schedule. All new or updated policies are displayed.
- Mac computers – New or updated policies are applied on the computers. Only the latest policy is stored on the computers. The latest policy is applied as per the schedule. Only the latest policy is displayed.

Inheriting Policy Settings

Policies can be configured to inherit settings from the Faronics Default policy to quickly distribute setting changes across multiple policies. Settings can be inherited individually per service and for the Maintenance Period. Policies can inherit settings from Faronics Default policy only.

Complete the following settings to inherit the settings from the Faronics Default Policy:

1. Go to the *Policies* page.
2. Click *Add Policy* > *Add New Policy*.
3. Select *Add New Windows Policy* or *Add New Mac Policy*.
4. Go to [General Settings](#) > *Maintenance Period*. Select *Enable* (*inherit settings from Faronics Default policy*).
5. Go to each service and select *Enable* (*inherit settings from Faronics Default Policy*).
6. Save the policy.

The Maintenance Period settings and the settings for the services are inherited from the Faronics Default Policy. The current policy that inherits the settings becomes read-only.






Applications

The *Applications* page displays a list of apps and relevant information such as which computer is a particular app installed in, under which app group an app belongs, app version, or if an app that is installed in a machine is outdated.

The following options are explained further in this chapter.

- [Color scheme](#)
- [Custom Apps \(Windows\)](#)
- [Custom Scripts \(Windows\)](#)
- [Pending Updates/All \(Windows\)](#)
- [Pending Updates/All \(Mac\)](#)
- [Apps with Recent Updates](#)
- [Failed Updates \(Windows Only\)](#)
- [App Presets](#)

For each option, you can enter a parameter in the Search field to search for a computer or app.

Click  at the top right to view the full screen. To exit full screen view, click . Click  to refresh the page.

Color scheme

- Green – Green side bar indicates installed apps on the computers are all up-to-date.
- Orange – Orange side bar indicates some versions of the installed app on the computers are outdated.
- Blue – Blue side bar indicates apps are in the process of downloading and/or installation.
- Gray – Gray side bar indicates computers are offline.
- Red – Red side bar indicates the computers are on *Defer Windows Updates* status.

Custom Apps (Windows)

Custom apps are apps that are not part of the pre-defined apps included in Deep Freeze Cloud.

Create Custom Apps

To create custom apps, click the *Custom App* button then select *Create Custom App*. Complete the following steps:

1. Package Name – Assign a package name.
2. Enter URL – Start with http://, https://, sftp:// (zipped file) or \\UNC.

If using SFTP, you will need to provide the SFTP User Name and Password, and have the option to extract the compressed file and run the executable file if preferred. Specify the installer executable file name if you choose to extract the compressed file.



3. Architecture – Select the architecture type (for 32-bit, 64-bit, or for 32- and 64-bit).
4. Install Command Lines – Specify the *Install Command Line*. (Exclude /i and /qn for MSI installers.)
5. Uninstall Command Lines – Specify the *Uninstall Command Line*.
6. Restart – Specify your *Restart* options.
7. Install Timeout – Specify your *Install Timeout* options, up to a maximum of 180 minutes.
8. Run As – Select whether to run the custom app as *System Account* or *Specified User Account*. When you select to run the custom app as a *Specified User Account*, provide the *Login ID*, *Password*, and *Domain* associated with the account.
9. Select Computer to Install – Select the computer for which to install the custom app. Click *Next*.
10. First time install – Click *Install* to install the custom app on the selected computer.


Custom apps can only be installed for the first time on one computer. After a successful first-time installation, you will be able to install the custom app on other computers.

To view details of Custom Apps, refer to [Action Toolbar for Apps](#).

View Custom Apps

To view custom apps, click the *Custom App* button then select *View Custom Apps*.

This page displays the list of custom apps that have been created as well as the configurations for each custom app.

Custom apps that have been edited will need to be verified and display the  icon. Hover your mouse on the icon and click on the link to verify the custom app by installing the app on selected computers.

To search for custom apps, enter a parameter in the Search field.

To create a new custom app, click *Add*.

To edit a custom app, select the app then click *Edit*.

To delete custom apps, select the app(s) then click *Delete*. You can delete multiple apps at a time. Alternatively, in Control Grid view, click on the custom app to call up the *Action Toolbar*, and then click *Delete*.

To copy a custom app, select the app. Click *Copy* then select to *Duplicate* a custom app or *Copy to Sites*.

- Duplicate – Selecting *Duplicate* will create an exact copy of the custom app. You can only duplicate one app at a time.
- Copy to Sites – Selecting *Copy to Sites* will copy the app to your preferred Site. You can copy a single or multiple apps to a single Site or to multiple Sites at a time.

Custom Scripts (Windows)

You can create custom scripts to automate the execution of tasks to your targeted computers.

Create Custom Scripts

To create custom scripts, click the *Custom Script* button then select *Create Custom Script*.



Specify the Custom Script details. Assign a *Script Name* and *URL* (start with `http://`, `https://`, or `\\UNC`) for the custom script and select the file type: PowerShell, VB Script, Batch Script, or Executable (.exe).

Enter the command line.

Select whether to run the custom script as *System Account* or *Specified User Account*. When you select to run the custom script as a *Specified User Account*, provide the *Login ID*, *Password*, and *Domain* associated with the account.

Click *Run Once* to select the computers on which to run the custom script, or click *Save to Grid* to save the script.



Clicking *Run Once* will execute the script on the selected computer but will not save the script.

To view details of Custom Scripts, refer to [Action Toolbar for Scripts](#).

View Custom Scripts

To view custom scripts, click the *Custom Script* button then select *View Custom Scripts*.

This page displays the list of custom scripts that have been created as well as the configurations for each custom script.

To search for custom scripts, enter a parameter in the Search field.

To create a new custom script, click *Add*.

To edit a custom script, select the app then click *Edit*. Alternatively, in Control Grid view, click on the name of the custom script to call up the *Action Toolbar*, and then click *Edit Details*.

To delete custom script, select the script(s) then click *Delete*. You can delete multiple script at a time. Alternatively, in Control Grid view, click on the custom script to call up the *Action Toolbar*, and then click *Delete*.

To copy a custom script, select the script. Click *Copy* then select to *Duplicate* a custom script or *Copy to Sites*.

- Duplicate – Selecting *Duplicate* will create an exact copy of the custom script. You can only duplicate one script at a time.
- Copy to Sites – Selecting *Copy to Sites* will copy the script to your preferred Site. You can copy a single or multiple scripts to a single Site or to multiple Sites at a time.

Pending Updates/All (Windows)

The *Pending Updates/All* tab displays a list of all computers which have the Cloud Agent and all supported applications currently installed on the target computers.

To display online or all computers, click  then select *Online Only* > *All* or *Outdated Only*.

To display the list of applications in groups or ungrouped, click the *Grouped by Application* button (under *Grid Options*).

To hide unused apps, click *Hide Unused Apps* (under *Grid Options*).



Computers that are undergoing maintenance will display the **m** icon.

The following information is displayed:

- Computer – Displays the computer name.
- Policy – Displays the current policy for the computer.
- Group – Displays the group to which the computer belongs. By default, the computer is assigned to the Default group.
- Tags – Displays all tags assigned to the computer.
- Applications – Displays the list of applications. There are two ways to view the applications:

Grouped View

By default, pre-defined apps are grouped and displayed by categories along with the total number of apps for each category.

- > Custom Apps – This column will only display when custom apps have been created.
- > Custom Scripts – This column will only display when custom scripts have been created.
- > Web Browsers
- > Messaging
- > Media
- > Runtimes
- > Imaging
- > Documents
- > Utilities
- > Compression
- > Developer Tools
- > Online Storage
- > Other
- > Web Conferencing
- > Security
- > Older Versions


Under *Grouped* view, each cell displays the number of installed/outdated apps under each category.



For example, there are 3 apps under *Web Browsers*. The cell will display '3 installed' when all the web browser apps are up-to-date. If a category has both installed and outdated apps, the cell will display only the number of the outdated apps.

You can update the outdated apps by clicking on the cell containing the outdated apps and then clicking *Update* on the top right.

To view the apps for a particular category, click the app category. The apps for the selected category will be displayed as well as installed/outdated/failed update status and other information (where applicable) for each app. To return to the previous view, click the X on the category filter.

For example: Click *Custom Scripts* to view all the custom scripts and the status for each custom script. Click  to view the logs.

Ungrouped View

The grid displays each app in a column, the category each app belongs to, the app version that is installed on the computer, and app failed update status for each computer.

Outdated app versions are displayed in orange text. Failed app updates are displayed with an orange cell background.

Action Toolbar

The *Action Toolbar* provides quick access to important actions for apps and computers. Administrators can perform certain actions directly from the toolbar.

Action Toolbar for Computers

To view the *Action Toolbar* for a computer, click on the computer name.

Actions

- Outdated Applications – Displays the number of outdated apps installed on the computer. Click *Update All* to update all the outdated apps.
- Computer Actions – Click *Remote* to allow RDP or VNC on the selected computer, *Shutdown* the computer, or *Restart* the computer.
- Deep Freeze Actions – Select to reboot the computer in Frozen or Thawed state.

When selecting to reboot the computer in Thawed state, you have the option to *Thaw Computer(s) for Next X Restarts* and assign the number of restarts (up to a maximum of 99 restarts).

For example, when you assign '3' as the number of restarts, the computer will remain in a Thawed state after rebooting the next 3 times.


You also have the option to *Lock Keyboard and Mouse* after rebooting the computer.

- Windows Updates – Click *Patch Scan* to perform a scan of Windows Updates installed or outstanding on the computer.
- Tag Computer – Displays the tags assigned to the computer, or assign new tags if desired.
- Apply App Preset – Refer to [App Presets](#).



- **Remove Agent** – Click *Remove Agent* to remove the Cloud Agent and all services from the target computer. When the Cloud Agent is removed, you will need to re-install it on the computer to see the computer on the console.
- **Delete Computer** – This option is only available for offline computers. Click to delete a computer. This option will only delete the computer from the console but not uninstall the Cloud Agent from the computer.

If Cloud Agent is still installed, the computer will report back again when it comes online.

You can perform actions for multiple computers by clicking on  beside the computer name in the *Action Toolbar*. Select the computers from the drop-down list and click *Select Computers*, or click *Select All Computers* to select all the computers. Only online computers will be reflected in the *Action Toolbar*.

Action Toolbar for Apps

To view the *Action Toolbar* for an app, click on the app name.

When an app is up-to-date, the *Action Toolbar* displays the category that the app belongs to, as well as the current version of the app.

When an app has outdated versions installed on any computer, the *Action Toolbar* displays the number of computers that have the outdated app version installed. The *Action Toolbar* also displays the total number of computers that have the app installed (outdated and up-to-date), and the percentage of the up-to-date installation.

Actions

- **Update All** – Click *Update All* to update the app on the machines that have the outdated app version installed.
This option will only update the app on computers that already have the app installed and will not install the app on the computers.
- **Install All** – Click *Install All* to install the app on computers that do not have the app installed.
This option will not update any outdated versions that have been installed on the computers.
- **Uninstall All** – Click *Uninstall* to remove the app from all the computers.
This option will uninstall all versions of the app, including the outdated version, from the computer.

The *Action Toolbar* for custom apps displays the category that the app belongs to, as well as the current version of the app. Click *Delete* to delete the custom app, or click *View Details* to display the following information for each custom app:

- URL
- OS Architecture
- Install Command Line
- Uninstall Command Line
- Restart
- Install Timeout



Action Toolbar for Failed Updates (Windows Only)

To view the *Action Toolbar* for failed updates, click on the cell of the app with the *Failed* status. The *Action Toolbar* will display the reason for the update failure as well as options to clear or retry installing the failed updates.

Actions

- Clear Failed – Click this option to clear the failed app status on the selected computer.
- Retry – Click this option to retry updating/installing the failed app on the selected computer.
- Clear All Failed – Click this option to clear all failed app status on all computers.
- Retry All Failed – Click this option to retry updating/installing all failed apps on all computers.

Action Toolbar for Scripts

To view the *Action Toolbar* for script, click on the script name.

The Action Toolbar for custom scripts displays the category that the script belongs to.

Actions

- Delete – Click this option to delete the custom script.
- Edit Details – Click this option to edit the *URL*, *Type*, and *Command Line* for each custom script.
- Run All – Click this option to run the script on all computers.

Install / Uninstall / Update Apps

To install, uninstall, or update apps, click on the cell of the selected apps, and click *Install*, *Uninstall*, or *Update*.

Clicking *Install* will only install the app on computers that do not have the app installed. This option will not update any outdated versions that have been installed on the computers.

Clicking *Uninstall* will remove the app from all the computers. This option will delete all versions of the app, including the outdated version, from the computers.

Clicking *Update* will only update the app on the computers that have the outdated app version installed. This option will not install the app on the computers that do not have any previous versions of the app installed.

Pending Updates/All (Mac)

The *Pending Updates/All* tab displays a list of all computers which have the Cloud Agent and all supported applications currently installed on the target computers.

To display online or all computers, click  then select *Online Only* > *All* or *Outdated Only*.

To display the list of applications in groups or ungrouped, click the *Grouped by Application* button.

The following information is displayed:



- Computer – Displays the computer name.
- Group – Displays the group to which the computer belongs. By default, the computer is assigned to the *Default* group.
- Tags – Displays all tags assigned to the computer.
- Applications – Displays the list of applications. There are two ways to view the applications:

Grouped View

By default, pre-defined apps are grouped and displayed by categories along with the total number of apps for each category.

- > Web Browsers
- > Messaging
- > Media
- > Documents
- > Utilities
- > Compression
- > Developer Tools
- > Online Storage
- > Other
- > Security

Under *Grouped* view, each cell displays the number of installed/outdated apps under each category.

For example, there are 3 apps under *Web Browsers*. The cell will display '3 installed' when all the web browser apps are up-to-date. If a category has both installed and outdated apps, the cell will display only the number of the outdated apps.

You can update the outdated apps by clicking on the cell containing the outdated apps and then clicking *Update* on the top right.

To view the apps for a particular category, click the app category. The apps for the selected category will be displayed as well as installed/outdated/failed update status for each app. To return to the previous view, click the X on the category filter.

Ungrouped View

The grid displays each app in a column, the category each app belongs to, the app version that is installed on the computer, and app failed update status for each computer.

Outdated app versions are displayed in orange text. Failed app updates are displayed with an orange cell background.

Action Toolbar

The *Action Toolbar* provides quick access to important actions for apps and computers. Administrators can perform certain actions directly from the toolbar.




Action Toolbar for Computers

To view the *Action Toolbar* for a computer, click on the computer name.


Actions

- Outdated Applications – Displays the number of outdated apps installed on the computer. Click *Update All* to update all the outdated apps.
- Computer Actions – Click *Shutdown*, or *Restart* the computer.
- Tag Computer – Displays the tags assigned to the computer, or assign new tags if desired.
- Remove Agent – Click *Remove Agent* to remove the Cloud Agent and all services from the target computer. When the Cloud Agent is removed, you will need to re-install it on the computer to see the computer on the console.
- Delete Computer – This option is only available for offline computers. Click to delete a computer. This option will only delete the computer from the console but not uninstall the Cloud Agent from the computer.

If Cloud Agent is still installed, the computer will report back again when it comes online.

You can perform actions for multiple computers by clicking on  beside the computer name in the *Action Toolbar*. Select the computers from the drop-down list and click *Select Computers*, or click *Select All Computers* to select all the computers. Only online computers will be reflected in the *Action Toolbar*.

Install / Uninstall / Update Apps

To install, uninstall, or update apps, click on the cell of the selected apps, then click  and select to *Update*, *Install* or *Uninstall*.

Clicking *Update* will only update the app on the computers that have the outdated app version installed. This option will not install the app on the computers that do not have any previous versions of the app installed.

Clicking *Install* will only install the app on computers that do not have the app installed. This option will not update any outdated versions that have been installed on the computers.

Clicking *Uninstall* will remove the app from all the computers. This option will delete all versions of the app, including the outdated version, from the computers.

Apps with Recent Updates

The *Apps With Recent Updates* tab displays the list of managed apps with information about the latest version and release dates.

To display managed apps for Windows, click  and select *Windows*. To display managed apps for Mac, click  and select *Mac*.

You can arrange the list for each column in ascending or descending order by clicking on the column name.

The following information is displayed:

- Name – Displays the name of the app.
- Release Date – Displays the latest release date of the most current version of the app.
- Version – Displays the current version of the app.



- **Installed** – Displays the total number of computers where the current version of the app is installed.
- **Outdated** – Displays the total number of computers where an outdated version of the app is installed.

Click on the name of the app to view the [Action Toolbar for Apps](#).

Failed Updates (Windows Only)

The *Failed Updates* tab displays the list of computers with failed app updates. You can arrange the list for each column in ascending or descending order by clicking on the column name.

Click on the cell of the app with the *Failed* status to view the *Action Toolbar* for the app. Refer to [Action Toolbar for Failed Updates \(Windows Only\)](#).

App Presets

An *App Preset* is a group of selected pre-defined applications, custom applications and custom scripts. *App Presets* provide a quick way of setting up and installing multiple applications on groups of computers instantly.

Creating app presets is a one-time action. Once an app preset has been created, it is now available for deployment across all computers. You can create as many app presets as needed.

Creating App Presets

Complete the following steps to create app presets:

1. Select a computer to call up the Action Toolbar.
2. Click *Install App Presets > Create New*.
3. Assign the *Preset Name* and select the applications and scripts to be included in the package.
4. Click *Save*.

Editing App Presets

Complete the following steps to co edit app presets:

1. Select a computer to call up the Action Toolbar.
2. Click *Install App Presets > Manage App Presets*.
3. Select the app preset you want to edit and make your changes.
4. Click *Save*.

Installing App Presets

Complete the following steps to deploy app presets:

1. Select a computer to call up the Action Toolbar.
2. Click *Install App Presets* and select the app preset to be deployed to the computer.
3. Click *Install* to install the app preset to the selected computer.



If the computer is offline, the task is queued and will be executed when the computer goes online.

If the computer is online, the task is executed immediately.





Windows Updates

The *Windows Update* page allows administrators to manage Windows Updates and patch scans across all computers managed by Deep Freeze Cloud.

The following options are explained further in this chapter.

- [Pending Windows Updates/All/Online Only](#)
- [Recent Windows Updates](#)
- [Failed Windows Updates](#)

Click  at the top right to view the full screen. To exit full screen view, click .

Pending Windows Updates/All/Online Only

The *Pending Windows Updates/All/Online Only* tab displays a list of computers with the total number of Windows Updates type that are installed and pending for each computer.

When a Windows Update is pending for any computer on the network, the *Pending Windows Updates* tab will be displayed on top and the list of computers with pending Windows Updates will be displayed in the grid.

When there are no Windows Updates pending for any computer, the *All* tab will be displayed on top and all computers on the network will be displayed on the grid. You can also configure the grid to show only computers which are *Online*.

The following information is displayed:

- Computer – Displays the computer name.
- Policy – Displays the current policy for the computer.
- Group – Displays the group to which the computer belongs. By default, the computer is assigned to the *Default* group.
- Tags – Displays all tags assigned to the computer.
- Windows Update Type
 - > Critical Update – A widely released fix for a specific problem that addresses a critical, non-security-related bug
 - > Security Update – A widely released fix for a product-specific, security-related vulnerability. Security vulnerabilities are rated by their severity as critical, important, moderate, or low.
 - > Definition Update – A widely released and frequent software update that contains additions to a product's definition database often used to detect objects that have specific attributes such as malicious code, phishing websites, or junk mail.
 - > Update Rollup – A tested, cumulative set of hotfixes, security updates, critical updates, and updates packaged together for easy deployment. A rollup generally targets a specific area (such as security), or a component of a product (such as Internet Information Services (IIS)).



- > Service pack – A tested, cumulative set of all hotfixes, security updates, critical updates, and updates. Additionally, service packs may contain additional fixes for problems that are found internally since the release of the product. Service packs may also contain a limited number of customer-requested design changes or features.
- > Tool – A utility or feature that helps complete a task or set of tasks.
- > Feature pack – New product functionality that is first distributed outside the context of a product release and that is typically included in the next full product release.
- > Updates – A widely released fix for a specific problem that addresses a non-critical, non-security-related bug.
- > Drivers – Software that controls the lower level input and output of a device.



Driver Updates through Windows Updates is not supported.

- > Microsoft – Updates for Microsoft applications.
- > Upgrades – Feature updates to Windows Operating Systems.

Action Toolbar

Action Toolbar for Computers

Click on the computer name to view the *Action Toolbar*. The *Action Toolbar* displays the Windows Update Status of the computer, whether it is *Highly Vulnerable*, *Vulnerable*, or *Up-to-date*.

Click *Install Missing Patches* to install all approved updates on the computer.

Click *Patch Scan* to perform a patch scan on the computer.

Click *View Patch History* to view all the Windows Update Patches. In the *View Patch History* window, select one or more patches and click *Approve* or *Deny*, or click *Approve All* to approve all Patches.

- Computer Actions – Click *Remote* to allow RDP or VNC on the selected computer, *Shutdown* the computer, or *Restart* the computer.
- Deep Freeze Actions – Select to reboot the computer in Frozen or Thawed state.


When selecting to reboot the computer in Thawed state, you have the option to *Thaw Computer(s) for Next X Restarts* and assign the number of restarts (up to a maximum of 99 restarts).

For example, when you assign '3' as the number of restarts, the computer will remain in a Thawed state after rebooting the next 3 times.

You also have the option to *Lock Keyboard and Mouse* after rebooting the computer.

- Tag Computer – Displays the tags assigned to the computer, or assign new tags if desired.
- Remove Agent – Click *Remove Agent* to remove the Cloud Agent and all services from the target computer. When the Cloud Agent is removed, you will need to re-install it on the computer to see the computer on the console.



You can perform actions for multiple computers by clicking on  beside the computer name in the *Action Toolbar*. Select the computers from the drop-down list and click *Select Computers*, or click *Select All Computers* to select all the computers. Only online computers will be reflected in the *Action Toolbar*.

Action Toolbar for Patches

To view the *Action Toolbar* for a Patch, click on the Patch name.

When a patch is pending an update, has a failed update, or has been installed, the *Action Toolbar* displays the number of computers on which the patch is pending an update, has failed, or has been successfully installed. The *Action Toolbar* also displays the status of the Patch (Approved, Declined, or Pending), the latest release date of the patch, the Operating System, and if a Restart is required.

To approve the Patch update on the computer, click *Approve*. To decline the Patch update on the computer, click *Deny*. Click *Deny* again when prompted to confirm.

Click *View Computer List* to view the list of computers where the patch has been approved, is pending or has failed, and other information such as the *Computer Name*, *Group*, *Policy*, supported *Operating System*, *Installed Status*, and *Installed Date*.

Click *View Details* to view more information about the Patch.

Click *Approve* or *Deny* to approve or decline a Patch.

Patch Scan/Install Missing Patches

To perform a *Patch Scan* or *Install Missing Patches*, click on the cell of the selected computers and click *Patch Scan* or *Install Missing Patches*.

Recent Windows Updates

The *Recent Windows Updates* tab displays the list of *Windows Updates*. You can arrange the list for each column in ascending or descending order by clicking on the column name.

The following information is displayed:

- Patch Name – Displays the name of the Patch.
- Category – Displays the Windows Update type.
- OS – Displays the supported Operating System.
- Release Date – Displays the latest release date of the Patch.
- Approval Status – Displays whether the Patch is *Approved*, *Pending* or *Declined*.

Click on the name of the app to view the [Action Toolbar for Patches](#).

Failed Windows Updates

The *Failed Windows Updates* tab displays the list of computers with failed Windows Updates.



Imaging

The *Imaging* page provides easy access to Imaging information across all computers, as well as options for performing USB imaging, cache imaging, and pure cloud imaging. Administrators can easily create and capture images of a specific operating system from a reference computer and deploy it to other computers.

The following options are explained further in this chapter.

- [Setting Up](#)
- [Image Caching](#)
- [Image Computer](#)
- [Capture Image](#)
- [Computers](#)
- [Imaging Servers](#)
- [Deployment Packages](#)
- [Install Settings](#)
- [Images](#)
- [Driver Groups](#)

Setting Up

Set up the Imaging Server in your local network and configure the settings on the Deep Freeze Cloud Console.



Cloud Agent must be installed prior to installing the Imaging Server.

In Your local Network

1. Download and install Imaging Server.
Supported platforms for the Imaging Server:
 - > Windows 8.1, 10, 11
 - > Windows Server 2012 R2, 2016, 2019, 2022Windows Server 2012 R2 or above is required to take advantage of WDS.
2. Configure Imaging.
 - > Use Windows Deployment Services (WDS)
Select this option to utilize advanced features such as PXE booting and have access to existing images and driver repository. Imaging Server will automatically configure the Windows Deployment Service Role at the end of the setup.



> Proceed without Windows Deployment Services

Select this option to proceed without Windows Deployment Services. PXE booting is not supported in this setup, and images and drivers already set up in WDS are not accessible. You will need a Windows installation media (.iso file or DVD) at the end of the setup process.

3. Create a Local User Account to allow managed computers to communicate with this server and secure a Network Share.
4. Specify the Image Repository Location to hold images. It is recommended to choose a location with enough free space to hold multiple OS installation images.
5. Add Images (.iso or .wim files) and Drivers (.inf files).



After setting up the Imaging Server, you need to provide Volume License .iso file (with boot.wim and install.wim files) as the first image to be added. Without the boot.wim file, Imaging will not work.

Adding Images

Complete the following steps to add images.

1. Launch Imaging Server.
2. Click *Images*.
3. Select one from these options:
 - > Automatically Download Windows 11 ISO from Microsoft
 - > Manually Choose any Other Existing ISO File
4. Click *Next*.
5. Select the images you want to add to the server and click *Next*.
6. To change your selection, click *Back*. To add the selected images to the server, click *Next*.
7. Add *OEM Drivers*. Click *Continue* to add OEM drivers, or *Skip* to continue adding images.
8. You can edit the image name and description of the images by clicking the pencil icon under Action. Click X to cancel any changes, or click the save icon after editing.
9. You can delete the images by clicking the delete icon under Action.
10. To add another image, click *Add Image*.

Creating Cloud Images

Cloud Images are images exported from the Imaging Server and hosted on a publicly available server (for example, HTTP/S or SFTP servers).

Complete the following steps to create Cloud Images.

1. Launch Imaging Server.
2. Click *Images*.
3. Select the image you want to create a Cloud Image of and click *Create Cloud Image*.
4. Specify the folder for creating the Cloud Image ZIP Archive, then click *Next*.



5. After the Cloud Image ZIP Archive has been created, you have the option to:
 - > Use HTTP/S Server

To use this option, cloud images must be uploaded to a publicly accessible web server or cloud storage provider that supports HTTP/S endpoint (make note of where the images are located in your cloud storage). In the *Cloud Image ZIP Archive URL* field, enter the URL where the cloud image was uploaded, then click *Register Cloud Image*.
 - > Upload to SFTP Server

If selecting this option, cloud images will be automatically picked up and uploaded to the SFTP server. Provide the *SFTP Server Name*, *SFTP User Name*, and *SFTP Password*, then click *Upload and Register*.



Click *Open Folder* to view the list of existing cloud images in the local directory.

Click *Cancel* to view the list of images that have been added to the utility. Note that clicking *Cancel* will bring you to the images list page and any changes or progress made are not saved.



You can store multiple images in the same server, however each image must have its own link.



After the Cloud Image ZIP archive has been registered, it will appear as an image under *Cloud Images* in the Cloud console and can be used to create a Cloud Deployment Package.

Registering Existing Cloud Images

You can choose to register existing cloud images if you want to upload the images to a different HTTP/s location, different SFTP server or to register the images in a different Imaging Server.



You can only register cloud images that have been created through the Faronics Imaging solution.

Complete the following steps to register existing Cloud Images.

1. Launch Imaging Server.
2. Click *Images*.
3. In the image list page, click *Register Existing Cloud Image* and select the image zip package you want to register. Click *Open*.
4. After selecting the Cloud Image ZIP Archive to be registered, you have the option to:



> Use HTTP/S Server

To use this option, cloud images must be uploaded to a publicly accessible web server or cloud storage provider that supports HTTP/S endpoint (make note of where the images are located in your cloud storage). In the *Cloud Image ZIP Archive URL* field, enter the URL where the cloud image was uploaded, then click *Register Cloud Image*.

> Upload to SFTP Server

If selecting this option, cloud images will be automatically picked up and uploaded to the SFTP server. Provide the *SFTP Server Name*, *SFTP User Name*, and *SFTP Password*, then click *Upload and Register*.



After the Cloud Image ZIP archive has been registered, it will appear as an image under *Cloud Images* in the Cloud console and can be used to create a Cloud Deployment Package.

Adding Drivers

Complete the following steps to add drivers.

1. Launch Imaging Server.
2. Click *Drivers*.
3. Click *Browse* and select the folder where the driver packages are located.
4. Click *Next*.
5. Select the driver packages you want to add and click *Next*.
6. Select *Add Tags* if preferred and specify the tags separated by commas.
7. To change your selection, click *Back*. To add the selected drivers to the server, click *Next*.
8. You can delete the driver packages by clicking the delete icon under *Action*.
9. To add another driver, click *Add Driver*.

Creating Cloud Drivers

Cloud Drivers are driver packages stored on HTTP/S or SFTP servers.

Complete the following steps to create Cloud Drivers.

1. Launch Imaging Server.
2. Click *Drivers*.
3. Select the drivers to be included in the Cloud Driver group and click *Create Cloud Drivers*.
4. Specify the folder for creating the Cloud Driver Group ZIP Archive, then click *Next*.
5. After the Cloud Driver Group ZIP Archive has been created, you have the option to:
 - > Use HTTP/S Server

To use this option, cloud driver groups must be uploaded to a publicly accessible web server or cloud storage provider that supports HTTP/S endpoint (make note



of where the driver groups are located in your cloud storage). In the *Cloud Driver Group ZIP Archive URL* field, enter the URL where the cloud driver group was uploaded, then click *Register Cloud Driver Group*.

> Upload to SFTP Server

If selecting this option, cloud driver groups will be automatically picked up and uploaded to the SFTP server. Provide the *SFTP Server Name*, *SFTP User Name*, *SFTP Password* and *Cloud Driver Group Name*, then click *Upload and Register*.



Click *Open Folder* to view the list of existing cloud driver groups in the local directory.

Click *Cancel* to view the list of cloud driver groups that have been added to the utility. Note that clicking *Cancel* will bring you to the drivers list page and any changes or progress made are not saved.



You can store multiple driver groups in the same server, however each driver group must have its own link.



After the Cloud Driver Group ZIP archive has been registered, it will appear as a driver group in the Cloud console and can be used to create a Cloud Deployment Package.

Driver Tags

You can edit or remove tags for a single or multiple drivers.

When creating tags for a single driver select the driver then click *Edit Tags*. Specify the tags separated by commas, then click *Save*.

When creating tags for multiple drivers select the driver then click *Append Tags*. Specify the tags separated by commas, then click *Save*. The specified tags will be appended to all selected drivers.

USB Media Creator

Complete the following steps to create a bootable USB drive.

1. Launch Imaging Server.
2. Click *USB Media Creator*.
3. Select the *Deployment Package* and *Policy*.
4. Select *Target USB Drive* if creating a bootable USB flash drive, or
5. Select *USB Creator Package Path*: and specify the folder in the local computer to create the *Installation Media Creator Package*.
6. Select *Use Product Key Stored in UEFI Firmware*. When selected, the product key embedded in the UEFI firmware will be detected and automatically included in the installation media.
7. Click *Edit* to configure the partitions, assign the volume labels and partition sizes.



In addition to the EFI and Windows system partition, up to 2 more partitions can be configured. All partitions will be formatted using NTFS.

8. Click *Start*.



The created USB Media Package (.exe file) contains the policy and package that was selected during the package creation. You can use the USB Media Package to create a USB bootable media on any computer by launching the .exe file from the package and selecting a USB drive.

On the Cloud

1. Create Install Settings.
2. Create Deployment Packages.
3. Deploy the Images.

Once the Imaging Server has been set up with images, you will be able to deploy (install) a new Windows image on any computer running the Imaging Client from the Deep Freeze Cloud Console without having to physically visit the computer.

Image Caching

Image Caching stores the captured image on a partition drive so that the computer does not have to connect to the Imaging Server to download the entire image during the actual imaging process.

Select at least one computer from the grid to prepare the computer for image caching. Click *Image Caching* and select a Deployment Package to initiate the image caching task of the targeted computers.



The Image selected in the Deployment Package should have caching enabled. To enable, select the image under *Images* section and click *Enable Caching*.

Installation Settings configured in the Deployment Package should not have Wipe Disk enabled.

Once initiated, the computer will go through the following steps:

1. Map the network share folder (FISShare) to check whether the Imaging Server is reachable or not.
2. Check whether sufficient disk space is available to deploy a given image.
3. Download BSInstaller.exe and PIMAUtil.exe.
4. Create a Cache Image partition.
5. Copy boot.wim file from the Imaging server.
6. Prepare the PE Image by copying all required files and data to the boot.wim (WinPE) file, and copying the install.wim file to the cache partition.

Once the above steps are completed successfully, the computer will be *Ready for Imaging*.



Image Computer

Deploy Windows installation images to the computers through *Image Computer*.

Select at least one computer from the grid. Click *Image Computer* to deploy the images to the targeted computers.



Images cannot be deployed on to computers connected to Wi-Fi networks. Computers must be connected to the Internet via LAN connection.

To image the selected computer:

1. Click *Image Computer*.
2. Select a *Deployment Package* and set the maximum number of computers to be imaged at the same time under *Queueing Option*.
3. Select *Are You Sure You Want to Continue?*
4. Click *Image Caching*.

Capture Image

Initiate the task of creating Images of the selected computers through Deep Freeze Cloud Console through *Capture Image*. The selected computers will undergo a system preparation procedure that will require configuring the OS settings again.



Computer imaging can not be performed on:

1. Computers with pending reboot after performing Windows Updates.
2. Computers with no user logged in.
3. Computers connected to Wi-Fi networks. Computers must be connected to the Internet via LAN connection.
4. A 32-bit computer.

To capture the image of a selected computer:

1. Click *Capture Image*.
2. Select pre-configured Install Settings to automate the Windows Out-of-Box Experience.
3. Specify the *Image Name* and *Description*, and enter the *Product Key* (optional).
4. Select *Reboot Computer Before Capture* to reboot the computer before proceeding with the *Capture Image* task.
5. Select *Install All Windows Updates* to install all pending Windows Updates before proceeding with the *Capture Image* task.
6. Select *Are You Sure You Want to Continue?*
7. Click *Capture Image*.

Once complete, the image will be shown in the list of *Images* on the imaging server and can then be deployed to client systems using a *Deployment Package*.



Computers

The Computers tab displays the list of all computers with the Imaging service enabled in the policy.

To display each stage of the deployment in the order of the deployment status for easier monitoring, click on *Grid Options > Detailed View* slider.

Click on *Grid Options > View Search And Filter* slider and right-click on the header of each column to sort. Enter a parameter in the Search field to search a particular column. You can also filter by clicking the filter icon.

The following information is displayed:

- Computer Name – Displays the computer name.
- Policy – Displays the current policy for the computer.
- Group – Displays the group to which the computer belongs. By default, the computer is assigned to the *Default* group.
- Tags – Displays all tags assigned to the computer.
- OS Type – Displays the Operating System installed on the computer.
- Image Caching – Displays when the computer is *Ready for Imaging*.

Hover your mouse on the cell to display the tooltip that lists the image caching information for the targeted computer. When the computer is *Ready for Imaging*, you have the option to *Image Computer* or *Delete Image*.

- Last Deployment Package – Displays the last package deployed to the computer.
- Last Deployed On – Displays when the last deployment was performed.
- Toolkits – WinPE Debug Mode, Remove Specific Appx Packages



When an imaging action is initiated, an XML file containing the Imaging action (Apply or Capture Image), Imaging Server name, and FICAgent user password is created in the Windows Temp folder. The Imaging utility parses this file and prepares the machines for the specified imaging action by communicating with the Shared folder on the Imaging Server and copying the boot.wim file to the machine.

When the Imaging task fails, detailed logs are created under the Windows Temp folder and copied to Imaging Server Network share under a specific folder.

Once the machine RAM boots in the WinPE, it again communicates with the network share folder on the Imaging Server.

When performing *Apply Image*, a shared network folder is required to fetch the actual image (install.wim).

When performing *Capture Image*, a shared network folder is required to copy the captured image onto the shared network folder.

During WinPE Mode, ImagingHelper.exe is run from drive X (the RAM Drive). The ImagingHelper.log is also created under drive X and copied to C: under the Windows Temp folder.

- Prerequisites – Required Conditions, BitLocker Check, User Profile Redirections, Network Check



- Server Connection – Contacting Imaging Server, Calculating Disk Space Requirement, Downloading Agent, Copying Boot Image
- Pre-install – Preparing PE Image, Sysprep is in Progress, About to RAM Boot
- Installation Status – Started Pre-install Environment, Contacting Imaging Server, Preparing Disk, Applying/capturing Image, Installing Device Drivers, Editing Captured Image, Uploading Captured Image, Finalizing

A failed task during the imaging process will be displayed with an orange cell background. Hover over the cell with the failed task to display the tooltip describing the failed action. A warning status will be displayed in orange text. You can choose to *Retry*, *Clear Status*, view/download *Logs*, or *Override Warning*.

Click *Retry* to retry the failed task on the selected computer.

Click *Clear Status* to clear the failed status on the selected computer.

Click *Logs* > *View Sysprep Errors* to view detailed information.

Click *Logs* > *Download Sysprep Logs* to download the log files.

Click *Override Warning* to clear the warning status on the selected computer.

Action Toolbar

Action Toolbar for Computers


To view the *Action Toolbar* for a computer, click on the computer name.

Actions

- Computer Actions – Click *Remote* to allow RDP or VNC on the selected computer, *Shutdown* the computer, or *Restart* the computer.
- Deep Freeze Actions – Select to reboot the computer in Frozen or Thawed state.
When selecting to reboot the computer in Thawed state, you have the option to *Thaw Computer(s) for Next X Restarts* and assign the number of restarts (up to a maximum of 99 restarts).
For example, when you assign '3' as the number of restarts, the computer will remain in a Thawed state after rebooting the next 3 times.
You also have the option to *Lock Keyboard and Mouse* after rebooting the computer.
- Windows Updates – Click *Patch Scan* to perform a scan of Windows Updates installed or outstanding on the computer.
- Image Computer – Click *Image Computer* and select the Deployment Package to image the selected computer.
 - > Queueing Options – Set the maximum number of computers to be imaged at the same time. We recommend setting up to 5 computers for simultaneous deployment at a time.
- Capture Image – Click *Capture Image* to create an Image of the selected computer. Note that capturing 32-bit image is not supported.
- Image Caching
 - > Prepare for Imaging – Click this option to prepare the computer for image caching. by selecting a Deployment Package. The image will be stored in a partition on the local drive.



- > Image from Cache – This option will be available once the computer has the image cached. Select this option to image the computer from the cache.
- > Delete Cached Image – Select this option to delete the cached image from the local drive.
- Tag Computer – Displays the tags assigned to the computer, or assign new tags if desired.
- Remove Agent – Click *Remove Agent* to remove the Cloud Agent and all services from the target computer. When the Cloud Agent is removed, you will need to re-install it on the computer to see the computer on the console.

You can perform actions for multiple computers by clicking on  beside the computer name in the *Action Toolbar*. Select the computers from the drop-down list and click *Select Computers*, or click *Select All Computers* to select all the computers. Only online computers will be reflected in the *Action Toolbar*.

Imaging Servers

The Imaging Servers tab provides a list of servers where the Imaging Server has been installed.

To add Imaging Servers, download and install the Imaging Server to your local network. Servers that have the Imaging Server installed are automatically reflected under Imaging Servers.

Imaging Server status must show Online for the targeted computers to have access to the Server and the Images and Drivers that have been added to that Server.



Deleting Imaging Servers will remove all associated Images and Drivers information. On WDS, images will not be deleted.



Deep Freeze Cloud uses the Windows Imaging Format (WIM) for storing images for deployment.

PXE Mode

PXE mode is disabled by default. You can enable or disable PXE mode for Imaging Servers that support PXE Booting. Imaging Servers must be online to enable/disable PXE mode.

To enable, select the Imaging Server(s) and then click *Enable PXE Mode*, and configure the [PXE Settings](#).



PXE mode will always wipe the disk and will not honor the disk settings in the selected Deployment Package.



To disable, select the Imaging Server(s) and then click *Disable PXE Mode*.



PXE mode works only for WDS Imaging Servers.

PXE Settings

PXE settings are assigned to the *Default Group*, *Manual Policy*, and the first available *Deployment Package* by default.

Complete the following steps to configure the PXE settings associated with each Imaging Server.

1. Select the Imaging Server.
2. Click *Edit PXE Settings*.
3. Select your preferred *Policy*, *Group*, and *Deployment Packages* from the drop-down list.
4. Disk Options – Select to *Choose Partition* or *Wipe Disk*.

When you select to *Choose Partition*, specify the identification number of the disk to configure from the *DiskID* drop-down list, and the identification number of the partition to modify from the *PartitionID* drop-down list.

Selecting *Wipe Disk* will erase all data from the target computer.

5. Require the user to press the F12 key to continue PXE boot – When this option is enabled, users will be required to press the F12 key to be able to continue PXE boot.
6. Click *Save*.


Deployment Packages

The Deployment Packages tab provides a list of Deployment Packages containing all the necessary components for a network-based deployment.

Deployment Packages are used to push an image on to targeted computers.

Creating Deployment Packages


To add Deployment Packages:

1. Click .
2. Assign a Package Name.
3. Select the Imaging Server, Image Name, and Install Settings.
4. Select the Driver Group.
5. Select to *Specify Product Key*, *Use Evaluation Product Key* or *Use OEM Product Key from Firmware*.
6. Configure pre-imaging tasks – Select the App Preset with the scripts you would like to run before Imaging, or create an App Preset by clicking *Manage App Preset*.
7. Configure post-imaging tasks – Select the App Preset you would like to install after Imaging is completed.



8. Windows Updates – Selecting this option will install all pending Windows Updates after the imaging task is completed.
9. Click *Save*.

Editing Deployment Packages

To edit Deployment Packages, click  and click on the name of the Deployment Package you want to edit. Click *Save* after changes have been made.

Deleting Deployment Packages

To delete Deployment Packages, click . Hover your mouse on the name of the Deployment Package you want to delete and click the delete icon.

Install Settings


The Install Settings tab provides a list of available install settings pre-configured to automate the Windows Out-of-box experience.



There is a pre-defined *Default Installation Settings* set up with an assigned Administrator and a randomly-generated administrator Password user under Local User Accounts. You can customize the settings for the Default Installation Settings and change the administrator Password.

Creating Install Settings

To add Install Settings:

1. Click .
2. Assign an Install Settings Name.
3. Edit the Settings.

General Settings

- > Organization Name – Select to keep the existing name or customize the name of your organization.

Regional Settings

- > Keyboard or input method – Select the preferred input method.
- > Currency and Date Format – Select the preferred currency and date format.
- > Time Zone – Select the preferred time zone.
- > System Language – Select the preferred system language.

Out-of-Box Experience

- > Protect Your Computer – Select to *Turn On Express Settings* or to *Turn Off Express Settings* during Windows installation.

Choose *Turn On Express Settings* to proceed with installing Windows on the target machines with default Windows Express Settings. Choose *Turn Off Express Settings* to disable Windows Express Settings on target machines.

Disk Settings



- > Wipe Disk – When you choose *Yes* to Wipe Disk, you will be able to create partitions and specify the size in GB or percentage (%), assign the drive letter and file system, and assign a label or name to the partition.

Note that when you choose *Yes* to Wipe Disk, all data will be erased from the target computer.



By default, the system drive letter is assigned to C:, and the file system is set as NTFS. You can only assign a label or name to the system drive and change the size.

When you choose *No* to Wipe Disk, you have the option to format the drive and assign a label or name to the partition.

When you choose to format the drive, any pre-existing information on it is lost. You can assign a label or name to the partition, but the file system is set to NTFS by default.



To enable image caching, Installation Settings configured in the Deployment Package should not have Wipe Disk enabled.

Local User Accounts


- > Set up administrator, guest or local users on the machine during the installation process. Assign a user name, display name, group (access status) and password for each user account created.

Domain


- > Assign the domain name, domain admin user name, password, and DNS Server.

4. Click *Save* after changes have been made.

Editing Install Settings

To edit Install Settings, click  and click on the name of the Install Settings you want to edit. Click *Save* after changes have been made.

Deleting Install Settings

To delete Install Settings, click . Click on the name of the Install Settings you want to delete and click the delete icon.

Images

Images are discrete files containing a compressed set of information such as system files, applications, data, settings, and properties captured from a reference machine.

The Images tab provides a list of available Images for deployment across all computers.

Add Images through Imaging Server installed in your local network or through Capture Images on the Console.



There are 2 types of images:

- Install image – ISO images extracted through the Imaging Server.
- Captured image – Images of selected computers captured through the Cloud via the Capture Image page.

Delete Images by clicking the delete icon on the top right of the *Images* tab.



Cloud Images are displayed with a link icon which displays the URL where the images have been stored in the server.

Enable Caching

Images selected in the Deployment Package should have caching enabled. To enable, select an image from the grid and click *Enable Caching*.



Installation Settings configured in the Deployment Package should not have Wipe Disk enabled.


Driver Groups

Driver groups can be created for use in Deployment Packages. Add drivers into the repository via the Imaging Server, group multiple drivers from the repository, and add to Deployment Packages.



For WDS: Drivers that have been added in the Imaging Server or in WDS are not reflected on the Cloud. WDS manages the drivers, automatically assigning them to the images.

For non-WDS: Drivers that have been added in the Imaging Server will be reflected on the Cloud under Drivers. The user needs to specify which drivers to be installed when creating a deployment package.

To create a group, click  and assign a group name. Select at least one Driver and click *Save*.

To search for Drivers, enter a parameter in the Search field.

You can add drivers to WinPE by selecting the WinPE checkbox for each preferred driver.



Cloud Driver Groups are displayed with a link icon which displays the URL where the driver groups have been stored in the server.



Inventory

The *Inventory* page provides a quick overview of the general information, hardware details, and other details of each computer found in the network. Administrators can tag computers, view installed applications, as well as delete computers.

The following options are explained further in this chapter.

- [All/Warranty Expired](#)
- [Update Warranty Info](#)
- [Action Toolbar](#)

Click the *Column Chooser* icon (☰) to launch the column chooser. To add a column to the grid, drag and drop the column from the column chooser to the grid. To remove a column from the grid, drag and drop the column from the grid to the column chooser.

All/Warranty Expired

You can configure the grid to show all computers or computers which have expired warranties. Click (☰) and select *All* or *Warranty Expired*.

The following information is displayed:

- Computer Name
- Policy
- Group
- Tags
- Notes
- Domain
- AD Group Membership
- OU Membership
- Current User
- Last Updated
- Manufacturer
- Service Tag
- Processor(s)
- Display
- Disks
- RAM
- System Drive Usage
- Operating System
- Computer Model
- BIOS Version
- BIOS Release Date
- IP Address



- Public IP Address
- Location
- MAC Address
- Network Adapter
- Apps with Pending Updates
- Pending Windows Updates
- Warranty Start
- Warranty End
- Warranty Term

Update Warranty Info

You can add or update the warranty information for single or multiple computers in your network.

To update the warranty information, click the *Update Warranty Info* then click *Download CSV* to download the CSV file containing information about the computers.

Add or update the warranty information in the CSV file. After you have updated the warranty information, click *Upload CSV* to upload the updated CSV file.



When adding warranty start and end dates, follow the format mm/dd/yyyy. Blank entries will be ignored.

Action Toolbar


Action Toolbar for Computers

To view the *Action Toolbar* for a computer, click on the computer name.

Actions

- Computer Actions – Click *Remote* to allow RDP or VNC on the selected computer, *Shutdown* the computer, or *Restart* the computer.
- Tag Computer – Displays the tags assigned to the computer, or assign new tags if desired.
- View Installed Applications – Click to view applications installed on the computer.
- Computer Details – Click *View Details* to view computer details.
- Refresh Computer Details – Click *Refresh Details* to refresh inventory details.
- Get Microsoft System Information (Msinfo32.exe) – Click *Get Microsoft System Information* of the selected computer. After the Msinfo has been obtained, click *Click Here* to download the .zip file and save it locally.
- Remove Agent – Click *Remove Agent* to remove the Cloud Agent and all services from the target computer. When the Cloud Agent is removed, you will need to re-install it on the computer to see the computer on the console.



You can perform actions for multiple computers by clicking on  beside the computer name in the *Action Toolbar*. Select the computers from the drop-down list and click *Select Computers*, or click *Select All Computers* to select all the computers. Only online computers will be reflected in the *Action Toolbar*.



Tickets

The Tickets page displays submitted tickets for the current Site. You can view, manage, and create IT support tickets from the Tickets page.



The following options are explained further in this chapter.

- [All/Active/Closed](#)
- [New Ticket](#)
- [Assign Ticket/Owner](#)
- [Ticket Actions](#)
- [View History](#)

All/Active/Closed





The *All/Active/Closed* tab displays a list of all tickets that have been submitted through the computer and console. Refer to New Tickets for details on submitting tickets.

Perform a search by entering a parameter in the search field or clicking the *View Search and Filter* slider. When *View Search and Filter* is enabled, you can click on the filter icon on each column to filter the list, right click on the header of each column to sort, or enter a parameter in the Search field of each column to search a particular column.

Click  at the top right to view the full screen. To exit full screen view, click .

To display tickets, click  and select *All*, *Active*, or *Closed*.

The following information is displayed:

- Computer
- Groups
- Tags
- Ticket ID
- Ticket Status
- Owner
- Assigned To
- Username (Windows)
- User Email
- Description – Click  or  to view the full description and attached files (if there are any). To download the attached files, click .
- Notes – Click  to view and edit notes.
- Date Added
- Last Modified On
- Last Modified By




Action Toolbar

Action Toolbar for Computers

Click on the computer name to view the *Action Toolbar* where you can perform the following actions.

- Computer Actions – Click *Remote* to allow RDP or VNC on the selected computer, *Shutdown* the computer, or *Restart* the computer.
- Ticket Actions – This option allows you to change the ticket status of the selected computer.

You can perform actions for multiple computers by clicking on  beside the computer name in the *Action Toolbar*. Select the computers from the drop-down list and click *Select Computers*, or click *Select All Computers* to select all the computers. Only online computers will be reflected in the *Action Toolbar*.

New Ticket

Creating new tickets can be done in two ways:

- Locally from the computer
- Through Deep Freeze Cloud console

To Submit Tickets from the Computer

The Ticketing Service must be enabled in the policy to allow computers to be able to submit tickets. Once the policy is enabled, After the installation is complete, tickets can be created by clicking the Ticket icon that appears on the system tray and filling out the ticketing form. Refer to [Ticketing Service](#) for information on how to create a ticketing form template.

To Create Tickets through the Cloud Console:

1. Click *New Ticket*.
2. Select a computer (optional).
3. Owner – Click *Add* and select an owner from the list, then click *Assign Selected User as Owner*.
4. Assigned To – Click *Add* and select a single or multiple users from the list, then click *Assign to Selected Users*.
5. Description – Enter a description for the ticket.
6. Attach File – Click *Upload* to attach a file. Supported file types are txt, csv, jpg, png, doc, pdf, xls, xlsx, zip up to a maximum size of 5 MB.
7. Notify User (Optional) – Enter the email of the user you wish to receive notification of the ticket.
8. Click *Save*.

Assign Ticket/Owner

Complete the following steps to assign a ticket:

1. Select a ticket.



2. Click *Assign > Assign Ticket*.
3. Select the user(s) you wish to assign to this ticket.
4. Click *Assign to Selected Users*.

Complete the following steps to assign an owner:

1. Select a ticket.
2. Click *Assign > Assign Owner*.
3. Select the user you wish to assign as owner of this ticket.
4. Click *Assign Selected User as Owner*.

Ticket Actions

Select a ticket and click *Ticket Actions*, then select whether to *View Ticket*, *Edit Ticket* or *Delete Ticket*.

Change the status of a single or multiple tickets by clicking on the name of a ticket or using CTRL+CLICK or SHIFT+CLICK (CMD+CLICK for Mac) to select multiple tickets. Click *Ticket Actions* on the top right and select *Open*, *In Progress* or *Closed*.

Alternatively, click on the Computer name to call up the Action Toolbar where you can change the ticket status of the selected computer.

Open tickets can be changed to *In Progress* or *Closed* status.

In Progress tickets can be changed to *Closed* status.

Closed tickets can be changed to *Open* status.

When closing a ticket, you can choose to send an email to the user who submitted this ticket confirming that the ticket has been closed.

View Ticket

Complete the following steps to view a ticket:

1. Select a computer.
2. Click *Ticket Actions > View Ticket*.
3. Click *Edit* to edit the ticket, or click *Close Ticket* to close the ticket.

Alternatively, double-click on a cell of the selected ticket to view the ticket details and click *Edit* to edit the ticket.

Edit Ticket

Complete the following steps to edit a ticket:

1. Select a computer.
2. Click *Ticket Actions > Edit Ticket*.
3. Edit the *Status*, *Owner*, *Assigned To*, and *Description*.
4. Attach or remove files and user.
5. Click *Save*.



Alternatively, double-click on a cell of the selected ticket to view the ticket details and click *Edit* to edit the ticket.

View History

The *View History* page displays the history of the ticket starting from the creation date and every subsequent update. Select a ticket and click *View History*.



General Settings

Configure the following settings under General Settings:

- [Cloud Agent Settings](#)
- [Maintenance Period](#)

Cloud Agent Settings

- Check for Policy updates every x hours – select the duration when the computers must check with the Cloud Console to sync policy settings. If you are using a Deep Freeze Mac policy, select *Enable Live Actions* to perform real-time actions from the Computers and Deep Freeze on Demand page.
- Enable password protection for uninstalling the Cloud Agent – specify a password for the Cloud Agent to prevent unauthorized users from uninstalling it from the computers. Specify and confirm the password.
- Enable Proxy – select the checkbox if you are using a proxy server to connect to the Internet. You must specify the proxy server settings since your computer(s) will communicate with Deep Freeze Cloud server through the proxy server. Configure the following settings:
 - > Proxy Server Information – specify the values for Address and Port.
 - > User Authentication – if your server requires authentication, select *My proxy server requires authorization*. Select or specify values for Authentication Type, User Name, Password, and Domain.

Maintenance Period

Select one of the following options for the Maintenance Period:

- Disable – This is the default option. The Cloud Agent Maintenance Period will be disabled.
- Enable (Inherit settings from Faronics Default policy) – select this option to inherit the maintenance settings from the Faronics Default policy. Selecting this option allows you to automatically distribute Maintenance Period settings across multiple policies.
- Enable (Use below settings) – select this option if you do not want to inherit settings from Faronics Default policy and customize the settings. Select *Disable all services* or *Disable selected services*. This setting is useful when you want to perform maintenance activities and you don't want the Services to interfere in any way.
- Select the services to be disabled for maintenance activities:
 - > Deep Freeze
 - > Anti-Virus
 - > Power Save
 - > Anti-Executable
 - > WINSelect
 - > Cloud Sync



- Start Time – select when the maintenance will start.
- End Time – select when the maintenance will end.



Specify the Maintenance Period Start Time/ End Time such that it does not conflict with the Start Time/End Time of the Deep Freeze Workstation Task. If there is a conflict between the Maintenance Period and Deep Freeze Workstation Task, you cannot save the policy without removing the conflict. Deep Freeze Cloud will display a warning message if there is a conflict.

- Repeat on – select the days when the maintenance will repeat.
- Automatically upgrade installed services if update is available – select this option if you want Deep Freeze Cloud to automatically upgrade the services on the computers if an update is available. If this option is selected, the administrator does not have to update the service manually or check for updates.
- Perform service installs and updates only during this period – select this option if the services must be updated only during a maintenance period. If this option is selected, the services will not be updated when the computers check-in as per the heartbeat.
- Perform Software Updater tasks – select this option to perform Software Updater tasks during the maintenance period.
- Allow user to snooze task – Select this option to allow user to snooze maintenance mode.
- Disable keyboard and mouse – select this option to disable the keyboard and mouse during the maintenance period.
- Shutdown after maintenance period – select this option to shut down the computer after the maintenance period ends.
- Show Message x minutes before the maintenance period starts – select this option and select the minutes before which the users must be notified.
 - > Display this message before the maintenance period – specify a message. This field cannot be blank.
 - > Display this message during the maintenance period – specify a message. This field cannot be blank.



Deep Freeze Service

Deep Freeze Service helps eliminate computer damage and downtime by making computer configurations indestructible. Once Deep Freeze is installed on a computer, any changes made to the computer—regardless of whether they are accidental or malicious—are never permanent.



To enable communication between the computer and Deep Freeze Cloud Services through the firewall, ensure that outbound traffic is permitted on specified ports, and access is allowed on certain domains and IP addresses on both the console and client computer. Refer to [Authorized Domains and Ports](#).



If you are using the Deep Freeze Enterprise Console, the Deep Freeze Service will be unavailable within the Policy when you log on to Deep Freeze Cloud.

To add Deep Freeze to the Policy, go to *Add Policy > Deep Freeze > select Enable (install and inherit settings from Faronics Default policy) or Enable (Install and use below settings)*. Selecting this option installs Deep Freeze on all computers using this Policy.



Selecting *Enable (install and inherit settings from Faronics Default policy) or Enable (Install and use below settings)* installs Deep Freeze on the computers whenever the computers check-in. The computers check-in based on the heartbeat specified in [Cloud Agent Settings](#).

- **Enable (install and inherit settings from Faronics Default policy)** – installs the service and inherits settings from the Faronics Default policy. Selecting this option saves time in configuring all the policy settings. Selecting this option makes the settings for the current policy read-only.
- **Enable (Install and use below settings)** – installs the service and uses custom settings. Selecting this option will allow you to customize the settings for this service in the current policy.
- **Disable** will not install the service or will uninstall the service from the computers whenever the computers check-in.

You can configure settings for Deep Freeze through various tabs. The configuration settings for Deep Freeze through various tabs are explained further in this chapter.

- [Password Tab](#)
- [Drives Tab](#)
- [Workstation Tasks Tab](#)
- [Windows Update Tab](#)



- [Batch File Tab](#)
- [Advanced Settings Tab](#)
- [Deep Freeze Dashboard](#)

Password Tab

Deep Freeze allows the administrator to choose up to 15 passwords.

To create a password, complete the following steps and click *Add*:

1. From the *Type* drop-down list, choose the preferred kind of password. The following options are available:
 - > Workstation: designated for use at the computer when the *Login Screen* is launched.
 - > Command Line: for use with Command Line Controls. The Command Line Control tool (DFC.exe) does not function unless at least one Command Line password is defined.
2. Optional: For passwords, select the *Allow Change* checkbox to allow a user to change the password at the computer.
3. Enter the password.



The password entered in the *Password* field is not hidden.
Do not use the same password for Command Line and the GUI.

4. To set a password to become active and expire on specified dates, select the *Timeout* checkbox and use the drop-down calendars to specify an *Activation date* and *Expiration date*.

Drives Tab



After editing the settings in the Installer Settings Tab, save the Policy and select the *Enable Deep Freeze* checkbox to install the Deep Freeze Cloud Service. The Deep Freeze Cloud Service will be installed from the computers based on the heartbeat specified in [Cloud Agent Settings](#).

Configure the following settings:

Drives

By default, all drives are Frozen. To put a drive in a Thawed state, clear the checkbox of the preferred drive.



While only local drives (partitions or physical drives) can be Frozen, all drive letters are shown because the pre-configured installation file may be installed on many computers with various hardware and software setups.

ThawSpace

ThawSpace is a virtual partition that can be used to store programs, save files, or make permanent changes. All files stored in the ThawSpace are retained after a restart, even if the computer is Frozen. A ThawSpace can be created on a drive that is configured to be Frozen or Thawed.

To create a single ThawSpace or multiple ThawSpaces, complete the following steps:

1. Select the Drive Letter. The default letter is T:. However, it can be changed to any available letter. The next available letter is automatically used if the selected drive letter already exists on a computer when Deep Freeze is installed.
 - > When a Drive Letter is selected from the drop-down and used to create a ThawSpace, it is removed from the drop-down.
 - > When a ThawSpace is removed, the corresponding Drive Letter is added back to the drop-down.
 - > The Drive Letter cannot be same as the Host Drive.
2. Enter the Size. This is the size of the ThawSpace. The maximum size is 1024 GB and the minimum size is 16 MB.
 - > If the computer does not have enough free space to accommodate the selected ThawSpace size, the size of the ThawSpace is adjusted downward to ensure proper operation of the computer.
 - > If you select the Size less than 16 MB, the ThawSpace is set to 16MB.
 - > If you select the Size more than 1024 GB (1 TB), the ThawSpace is set to 1024 GB (1 TB).
3. Select the ThawSpace storage unit in MB or GB.
4. Select the Host Drive.
 - > The Host Drive is the drive where the ThawSpace is created.
 - > The storage required for the ThawSpace is used from the total storage available on the Host Drive.
5. Select *Visible* or *Hidden* from the *Visibility* drop-down.
 - > If you select *Visible*, the drive will be visible in Windows Explorer.
 - > If you select *Hidden*, the drive will not be visible in Windows Explorer.
 - > However, the hidden drive can be accessed by typing the drive letter in *Start > Run*.



6. Click *Add* to add the ThawSpace.



It is recommended to assign Drive Letters towards the end of the alphabet (X, Y, Z) in order to avoid automatic reassignment when a removable drive is unplugged.

Removing a ThawSpace

To remove a ThawSpace, locate it in the list of ThawSpaces and click the associated delete button. The ThawSpace is removed and the drive letter is now added back to the Drive Letter drop-down.



Before removing a ThawSpace, remove any profile redirections or Symbolic Links.

Removing a ThawSpace will also remove the data stored in it.

A ThawSpace is not protected by Deep Freeze. Deploy standard data protection options such as, Anti-Virus and backup procedures.

Configuring Existing ThawSpaces

The *Retain existing ThawSpace* checkbox is selected by default to prevent ThawSpaces created during previous installations from being deleted.

A dialog is always displayed asking if the ThawSpace should be retained or deleted during an Attended Uninstall, regardless of whether *Retain existing ThawSpace* has been selected. This option is not displayed if the uninstall is performed through the Console.

Select *Delete during policy update* to delete and re-create all existing ThawSpaces on the computer while applying the new configuration. All data in the existing ThawSpaces will be deleted as part of this process.

The *Honor Group Policy settings for Hidden Drives* ensures that the Group Policy settings for hidden drives do not conflict with the Deep Freeze settings for hidden drives.

Hidden drive settings for Group Policies are user-specific. Hidden drive settings for Deep Freeze are global if the *Honor Group Policy settings for Hidden Drives* option is disabled.



If there are no Group Policies for hidden drives, it is recommended to disable this option.



If the *Retain Existing ThawSpace* option is selected, the updated policy can be applied to the computers.



If the *Delete during policy update* option is selected, all data in existing ThawSpaces will be deleted when you apply the policy!

Workstation Tasks Tab

Workstation Tasks allow you to schedule various tasks that run at the computer.



Specify the Workstation Task Start Time/ End Time such that it does not conflict with the Start Time/End Time of the Maintenance Period. If there is a conflict between the Maintenance Period and Deep Freeze Workstation Task, you cannot save the policy without removing the conflict. Deep Freeze Cloud will display a warning message if there is a conflict.

The following Workstation Tasks are available:

- Windows Update – schedule Windows updates. You can configure additional settings in the Windows Update tab.
- Batch File – run a batch file on the target computer. You can configure additional settings in the Batch File tab.
- Idle Time – shut down or restart the computers if they are idle for a specified period of time.
- Restart – periodically restart computers to bring them to the original configuration or erase unwanted data.
- Shutdown – shut down the computers at a specified time every day to save power.
- Thawed Period – reboot Thawed for a specified period to perform manual software installs, automated software installs via third party tools or other permanent configuration changes.



For Windows Update, Thawed Period, and Batch File Tasks, all services will go into Maintenance Mode. Additional settings of the Maintenance Mode will not be applied.



Each task is covered in detail in the following sections.



Overlapping tasks cannot be created in the Workstation Tasks tab. If a newly created task overlaps with an existing task, a message is displayed.



A message can be displayed to the user for a maximum of 5 minutes. There must be a gap of a minimum of 5 minutes between any two tasks.



A Workstation Task is triggered only when Deep Freeze is in a Frozen state.

Windows Update

Windows Update tasks are scheduled for downloading Windows Updates on the computer. Windows Updates can be downloaded even when the computer is in a Frozen state. A Windows Update task has a Start Time and an End Time. After downloading Windows Updates, the computer reboots in a Thawed state to apply.

The Windows Update task can be scheduled by completing the following steps:

1. Select *Windows Update* from the *Task Type* drop-down and click *Add*.
2. The following options are displayed:
 - > Name – Specify a name for the task.
 - > Day – Select the day, or specify if the task will occur on Weekdays or Weekends.
 - > Start – Select the Start Time.
 - > End – Select the End Time. The minimum interval is 15 minutes. Alternatively, you can select *When Windows Update Completes*. If the Windows Update Task is not completed in 6 hours, Deep Freeze will end the task gracefully.



If a Windows Update task is set to end *When Windows Update Completes*, and the computer is turned off at the scheduled start time of the task, the Windows Update task will be triggered for the computer if the computer is powered on within 15 minutes after the scheduled start time.

For example, a computer is turned off when the Windows Update task is set to start at 11:40 pm. If the computer is powered on between 11:40 pm to 11:55 pm, the Windows Update task will automatically execute on the computer.

- > Allow user to cancel task- Select the checkbox if the user is allowed to cancel the task before it starts.



- > Attempt to wake up locally – Select this option to wake up the computer locally without requiring any communication from the Deep Freeze Cloud Console.
Note that certain hardware profiles do not support this option. If this option is selected, but the computer hardware does not support it, the computer will not wake up automatically.
 - > Shut down after task – Select the checkbox to shutdown the computer after the task.
 - > Disable keyboard and mouse – Select the checkbox to disable keyboard and mouse during the task.
 - > Show message – Select the checkbox to display a message on the computer *Before* and *During* the task. Specify the time interval in minutes and enter a brief message to be displayed before the task starts.
3. Click OK. You will be taken to the [Windows Update Tab](#) to configure additional settings if it has not been configured earlier.



The message *This computer will reboot in %d for Windows Update* is displayed in the *Message to be displayed before the task* field. This message can be edited. Add the word *minutes* in the message after %d to include the word minutes as part of the message.



When scheduling the Windows Update task select the *When Windows Update completes* option or ensure that you allow a sufficient time frame to permit all required update activities. Review of Microsoft Security Bulletins from the TechNet web site (<http://technet.microsoft.com/en-us/security/bulletin>) to consider the appropriate time frame based upon the Critical and Security updates being released.



If you are not using WSUS, Deep Freeze Windows Update process will only apply non-user-intervention Critical and Security updates, as well as Feature updates for Windows 10 and above. If you are using WSUS, all WSUS approved updates will be applied.

If you are not using WSUS, Windows Update task will always try to install Feature updates whenever available starting from Windows 10. You can defer installing Feature updates by selecting Choose when updates are installing under Advanced Options of Windows Updates system settings, or enabling local computer policy Select when Preview Builds and Feature Updates are received located in *Computer Configuration > Administrative Templates > Windows Components > Windows Update > Windows Update for Business*.

Alternatively, to apply other available updates visit the Microsoft Update Catalog site (<http://catalog.update.microsoft.com>) to obtain KB downloads which can then be applied using a Deep Freeze Batch File Workstation Task. Batch File tasks can also be used to apply other third party software updates.



The Deep Freeze Windows Update tab settings override the Windows Update settings on the computer.

Batch File

Batch File tasks are scheduled for executing batch files on the computer. A Batch File task has a Start Time and an End Time. During this period, the batch file is executed on the computer. You must configure additional settings in the Batch File tab for the Batch File Task to work. You can configure to shutdown the computer after the Batch File Task is completed. Computers will reboot Frozen after the batch file has been executed.

The Batch File task can be scheduled by completing the following steps:

1. Select *Batch File* from the *Task Type* drop-down and click *Add*.
2. The following options are displayed:
 - > Name – Specify a name for the task.
 - > Day – Select the day, or specify if the task will occur on Weekdays or Weekends.
 - > Start – Select the Start Time.
 - > End – Select the End Time. The minimum interval is 15 minutes.
 - > Allow user to cancel the task – Select the checkbox if the user is allowed to cancel the task before it starts.
 - > Attempt to wake up locally – Select this option to wake up the computer locally without requiring any communication from the Deep Freeze Cloud Console.
Note that certain hardware profiles do not support this option. If this option is selected, but the computer hardware does not support it, the computer will not wake up automatically.
 - > Shut down after task – Select the checkbox to shutdown the computer after the task.
 - > Disable keyboard and mouse – Select the checkbox to disable keyboard and mouse during the task.
 - > Show message – Select the checkbox to display a message on the computer *Before* and *During* the task. Specify the time interval in minutes and enter a brief message to be displayed before the task starts.
3. Click *OK*.
4. Go to [Batch File Tab](#) to configure additional settings.



The message *This computer will reboot in %d for Batch File* is displayed in the *Message to be displayed before the task* field. This message can be edited. Add the word *minutes* in the message after %d to include the word minutes as part of the message.

Idle Time

The Idle Time task can be scheduled by completing the following steps:

1. Select *Idle Time* from the *Task Type* drop-down and click *Add*.



2. The following options are displayed:
 - > Name – Specify a name for the task.
 - > Restart or Shutdown – Select *Restart* or *Shutdown* and specify the idle time in minutes after which the task must take place.
 - > Start countdown only after the first keyboard and mouse activity – Select this option for the timer to start counting only after the first keyboard or mouse activity. For example, if the idle time is specified as 20 minutes, and this option is selected, the computer task will shut down the computer 20 minutes after the first keyboard and mouse activity.
This option is only available if the Shutdown task is selected.
 - > Show message – Select the checkbox to display a message. Specify the time interval in minutes and enter a brief message.



After the computer is started, the Idle Time counter becomes active only after the first keyboard or mouse activity has been initiated. During a Remote Desktop session, the Idle Time of the controlling computer is used to activate the task.

3. Click OK.

Restart

The Restart task can be scheduled by completing the following steps:

1. Select *Restart* from the *Task Type* drop-down and click *Add*.
2. The following options are displayed:
 - > Name – Specify a name for the task.
 - > Day – Select the day, or specify if the task will occur on Weekdays or Weekends.
 - > Start – Select the Start Time.
 - > Allow user to cancel the task- Select the checkbox if the user is allowed to cancel the task before it starts.
 - > Show message – Select the checkbox to display a message on the computer before the task starts. Specify the time interval in minutes and enter a brief message to be displayed before the task starts.
3. Click OK.



The message *This computer will reboot in %d seconds* is displayed in the *Message to be displayed before the task* field. This message can be edited. Add the word *minutes* in the message after %d to include the word minutes as part of the message.

Shutdown

The Shutdown task can be scheduled by completing the following steps:

1. Select *Shutdown* from the *Task Type* drop-down and click *Add*.
2. The following options are displayed:



- > Name – Specify a name for the task.
- > Day – Select the day, or specify if the task will occur on Weekdays or Weekends.
- > Start- Select the Start Time.
- > Allow user to cancel the task – Select the checkbox if the user is allowed to cancel the task before it starts.
- > Show message – Select the checkbox to display a message on the computer before the task starts. Specify the time interval in minutes and enter a brief message to be displayed before the task occurs.

3. Click OK.



The message *This computer will shutdown in %d seconds* is displayed in the *Message to be displayed before the task* field. This message can be edited. Add the word *minutes* in the message after %d to include the word minutes as part of the message.

Thawed Period

Thawed Period tasks are scheduled to reboot the computer is in a Thawed state. A Thawed Period is useful for some applications that update automatically at regular intervals. A Thawed Period is also useful for administrators to schedule maintenance and make permanent changes to the computers. This may include installing new software, updating software, configuration changes, and other maintenance functions. A Thawed Period has a Start Time and an End Time.

The Thawed Period can be scheduled by completing the following steps:

1. Select *Thawed Period* from the *Task Type* drop-down and click *Add*.
2. The following options are displayed:
 - > Name – Specify a name for the task.
 - > Day – Select the day, or specify if the task will occur on Weekdays or Weekends.
 - > Start – Select the Start Time.
 - > End – Select the End Time. The minimum interval is 15 minutes.
 - > Allow user to cancel task – Select the checkbox if the user is allowed to cancel the task before it starts.
 - > Attempt to wake up locally – Select this option to wake up the computer locally without requiring any communication from the Deep Freeze Cloud Console.
Note that certain hardware profiles do not support this option. If this option is selected, but the computer hardware does not support it, the computer will not wake up automatically.
 - > Shut down after task – Select the checkbox to shutdown the computer after the task.
 - > Disable keyboard and mouse – Select the checkbox to disable keyboard and mouse during the task.
 - > Show message – Select the checkbox to display a message on the computer *Before* and *During* the task. Specify the time interval in minutes and enter a brief message to be displayed before the task starts.



3. Click OK.



The message *This computer will reboot in %d for Maintenance* is displayed in the *Message to be displayed before the task* field. This message can be edited. Add the word *minutes* in the message after %d to include the word minutes as part of the message.

To ensure that the virus definitions are applied permanently, schedule the virus definition update for your Anti-Virus program so that it starts after Deep Freeze successfully starts the Thawed Period task and ends before Deep Freeze ends the Thawed Period task. This ensures that the virus definitions downloaded and updated by the Anti-Virus program stay permanently on the system. Hence the system is fully protected by Anti-Virus and Deep Freeze.



Faronics Anti-Virus: Faronics Anti-Virus works with Deep Freeze and does not require a Thawed Period task for updating virus definitions. Faronics Anti-Virus can update virus definitions even when the computers managed by Deep Freeze are in a Frozen state.

Other Anti-Virus Programs: All other Anti-Virus programs require scheduling a Thawed Period task to update virus definitions. Refer to your Anti-Virus program user guide for information on how the virus definitions are downloaded. Alternatively, virus definitions can be applied manually when the computers managed by Deep Freeze are in a Thawed state. You can also schedule a *no user intervention* install of your virus definitions through a Batch File Task.

Windows Update Tab

The Windows Update tab allows you to customize settings for Windows Update. When you first create a Windows Update Task, you will be given an option to modify the default settings in the Windows Update tab. Modifying the default settings is not mandatory. Windows Update will be performed even with the default settings. The settings in the Windows Update tab will apply to all Windows Update tasks.



The Deep Freeze Windows Update tab settings override the Windows Update settings on the computer.

The settings in the Windows Update tab can be customized as follows:

Allow Deep Freeze to choose how Windows updates are downloaded: – select this checkbox to allow Deep Freeze to choose how Windows updates are downloaded. The following options are available:

- Select the Windows Updates download options:
 - > Do not cache Windows updates – select this option to download Windows updates only during the Windows Update task.



- > Cache Windows updates –select this option to download when the computer is in a Frozen or Thawed state and install during the Windows Update Task. This option creates a 10 GB ThawSpace and the Windows Updates are stored in the ThawSpace to ensure that Windows Update files are persistent across multiple reboots.

For Windows 10 and above: When Cache Windows updates is selected, the drive letter drop-down list is enabled. Select a drive letter from the drop-down list to assign as the hidden drive letter for storing Windows Updates cache. The assigned hidden Windows Updates cache drive letter will not be visible in Windows Explorer.



The hidden drive letter is not visible on the workstations and is only available for Windows 10 and above.

- Always retrieve updates from:
 - > Microsoft Windows Update web site – select this option to download updates directly from the Microsoft Windows Update web site.

You can opt to download *Critical and Security Updates*, *Critical*, *Security*, and *Features Updates* or *All Updates*.

 - ~ Critical and Security updates – Select this option to download Critical and Security updates.
 - ~ Critical, Security, and Features updates – Select this option to download Critical, Security as well as Features updates.
 - ~ All updates – Select this option to download all updates.
 - > Windows Server Update Services (WSUS) – select this option to download from WSUS server. Specify the SUS/WSUS Server. Optionally, select *Use WSUS Target* and specify the target. Microsoft SUS client and SUS/WSUS server can be downloaded at: <http://www.microsoft.com/wsus>.



A log file is created for each individual computer and is stored locally on the computer.

The default name for the Deep Freeze Windows Update Log file is *DFWuLogfile.log* and can be found at:

C:\Program Files\Faronics\Deep Freeze\Install C-[X]\DFWuLogfile.log (32-bit systems) and C:\Program Files (x86)\Faronics\Deep Freeze\Install C-[X]\DFWuLogfile.log (64-bit systems).

- You cannot change the name or location of the log file.
- The Deep Freeze Log file and the Windows Update log file (at c:\windows\windowsupdate.log) are very useful for troubleshooting your Windows updates.
- X is an incremental value depending on how many times you have installed Deep Freeze on the computer.

Contact Faronics Support for help troubleshooting the DFWuLogfile.log (at <http://support.faronics.com>).

Contact Microsoft Support for troubleshooting Windows Update Errors. (See <http://support.microsoft.com/kb/906602>).

Also see Microsoft KB 902093 *How to read the Windows Update log file* found at: <http://support.microsoft.com/kb/902093/> or visit <http://support.microsoft.com>.

Batch File Tab

The Batch File tab allows you to customize settings for the Batch File task. When you schedule a Batch File task from the Workstation Tasks tab, you must configure the settings in the Batch File tab.

Configure the following options:

- Batch File Authentication

Select Microsoft Network and select if the account to be used is a System account or a Specified user account. If you select Specified user account, specify the Login ID, Password, and Domain. For Novell Network, select Novell, specify the Login ID, Password, Tree, Context, and Server.



The default configuration using the Microsoft Network/System Account authentication must be tested prior to using alternative credentials. Using this machine level account often is sufficient to complete the task. Use of a specified user account may be required if the batch file requires network access to secure resources.



- Batch File Contents

Enter a custom batch file to run during the Batch File task. The same batch file applies to all Batch File tasks. The following options are available when running custom batch files:

- > To clear the current batch file, click *Clear*.
- > To load an existing file, click *Import* and browse to the location of the file.
- > To save the contents of the field, click *Export* and browse to the preferred save location.

The batch file can be any command or series of commands that the command processor can run. You can run custom scripts that require the use of a third-party scripting engine by calling the script from the batch file as if it was being run from the command line.



Batch Files allow you to use VB Scripts, PowerShell scripts, Ninite and other third party solutions. Contact your software vendor or refer to your third party solution user guide to know more about scripting solutions that include *no user intervention* options.

Advanced Settings Tab

Configure the following settings:

Advanced Options

- Disable Command Line options – This option is selected by default. Clearing this checkbox allows for further customization of the Deep Freeze installation program when using the Silent Install System. Selecting this option prevents the pre-existing configuration choices from being changed during installation.
- Protect MBR/GPT – Select this checkbox if you want Deep Freeze to protect the Master Boot Record. If this option is selected, changes to the Master Boot Record are reversed on reboot when the computer is in a Frozen state.
- Enable Deep Freeze local policies – For enhanced security, Deep Freeze removes the following local privileges: debugging programs, modifying firmware, and changing the system time; clear this option to use existing privileges.
- Allow user to change the clock – Select this option to allow Frozen users to adjust the system clock. Enable this feature during Daylight Savings to allow Windows to update the time automatically each season.
- Manage Virtual Memory – Enable this for rare cases where hardware with limited RAM may experience performance issues. Selecting this option allows Deep Freeze to manage the page file size.



This option is disabled by default. The page file size will be adjusted to match the RAM size if this option is enabled, which will allocate more hard drive space on the workstation.



- Manage Secure Channel Password – Secure Channel Password is a feature of all Windows operating systems and only applicable if the system is running in Windows Server Domain Environment. Secure Channel Password is used for secure communication between the server and computers. The Secure Channel Password is automatically changed based on the operating system settings. While using Deep Freeze, the newly changed Secure Channel Password is lost on reboot. The *Manage Secure Channel Password* option avoids this situation. The *Manage Secure Channel Password* feature of Deep Freeze changes the value of the Group Policy *Maximum machine account password age* based on the Deep Freeze state (Frozen or Thawed).
 - > Select the *Manage Secure Channel Password* option if you want Deep Freeze to manage Secure Channel Password.

When the computer is Frozen: The computer will not change the Secure Channel Password. This ensures that the secure communication between the server and the computer is always maintained.

When the computer is Thawed: The computer will change the Secure Channel Password and sync the password with the server.
 - > Do not select the *Manage Secure Channel Password* option if you do not want Deep Freeze to manage the Secure Channel Password.

When the computer is Frozen: When the Secure Channel Password is changed and synced with the server, it resets to the old password on reboot.

When the computer is Thawed: If the computer is Thawed on the day the Secure Channel Password is changed, the new password takes affect and the computer is synced with the server.
- Restart on Logoff – Select this checkbox to Restart the computer automatically when it is logged off. If this option is selected, the computer is restarted when a user logs off in a Frozen state.



The Manage Secure Channel Password feature of Deep Freeze always overrides the Group Policy *Maximum machine account password age*.

Set the following in the Group Policy for the *Manage Secure Channel Password* feature to work:

Domain Controller: Refuse machine account password changes to Not Defined.

Domain Member: Disable machine account password changes to Disabled.

- Delay Frozen reboot to complete Windows updates – Select this option to delay reboot into a Frozen state if configuration or installation for Windows updates are pending. If you select this option and perform Windows updates (through means other than Deep Freeze), rebooting into a Frozen State will ensure that all Windows updates installation and configuration are completed before rebooting into a Frozen state.



If you select *Delay Frozen reboot to complete Windows updates* and install Deep Freeze, the installer checks if all Windows updates are completed. If the Windows updates are not completed, Deep Freeze installation will not proceed. Complete Windows updates and try installing Deep Freeze again.

If you disable *Delay Frozen reboot to complete Windows updates* and install Deep Freeze, ensure that all Windows updates are completed manually. Disabling this option may result in the computer being stuck in a reboot cycle due to incomplete Windows updates.

- **Retain Windows Event Logs** – Select this option to retain Windows Event Logs. Deep Freeze creates a 100 MB ThawSpace and stores all Windows Event Logs so they are not erased upon reboot even when the computer is in a Frozen state. The log file is recycled once it reaches 100 MB. The log files contain events related to Application, Hardware, System and Security.
- **Manage Local Administrator Password Solution** – Local Administrator Password Solution (LAPS) is a Windows feature that automatically manages and backs up the password of a local administrator account on Active Directory-joined or Windows Server Active Directory-joined machines.

When this option is enabled on systems where LAPS setup is detected, Deep Freeze will disable the ability of LAPS to change the configured local admin password in Frozen state and allow to do so in Thawed state. This feature ensures that the current admin password can be rotated only in Thawed state and remain synchronized with Active Directory.

On Demand Cloud Relay Configuration (Optional)

The Cloud Agent installed on the computers report to the Cloud Relay. The Cloud Relay reports to the Deep Freeze Cloud. Real-time Deep Freeze actions can be performed on the computers through the Cloud Relay.

The following two methods are available to identify the Cloud Relay:

- Specify the Cloud Relay IP, which must be static.
- Specify the Cloud Relay Name, in which case the IP can be dynamic (if valid DNS name resolution is available as part of the domain infrastructure).

When the Cloud Relay is behind a firewall or a NAT (network address translation) router, the firewall or router must be configured to allow traffic to pass through to the Enterprise Console. Depending on the firewall or router, computers may need to be configured with the IP address of the firewall so that traffic can be forwarded.



Deep Freeze automatically configures the required exceptions in the Windows Firewall. It is not required to configure the Windows Firewall manually.

Stealth Mode

- **Show Frozen icon in system tray** – Select this option to display the icon to indicate that Deep Freeze is installed and the computer is Frozen.



- Show Thawed icon in system tray – Select this option to display the icon to indicate that Deep Freeze is installed but the computer is Thawed.



If the options to show the Deep Freeze icon in the System Tray are unchecked, the keyboard shortcut CTRL+ALT+SHIFT+F6 must be used to access the logon dialog.

Deep Freeze Command Line Control (DFC.EXE)

Deep Freeze Command Line Control (DFC) offers network administrators increased flexibility in managing Deep Freeze computers. DFC works in combination with third-party enterprise management tools and/or central management solutions. This combination allows administrators to update computers on the fly and on demand.



Using Deep Freeze Command Line will render the computers out of sync with the policy currently applied. To get the computers back in sync, reapply the policy.

It is important to note that DFC is not a stand-alone application. DFC integrates seamlessly with any solution that can run script files, including standard run-once login scripts.

DFC commands require a password with command line rights. OTPs cannot be used.

List all commands by calling DFC without parameters.

The files are copied to (32-bit)

```
<WINDOWS>\system32\DFC.exe
```

The files are copied to (64-bit)

```
<WINDOWS>\syswow64\DFC.exe
```

DFC Return Values

On completion of any DFC command, the DFC returns the following values:

Syntax	Description
0	SUCCESS or Boolean FALSE, for commands returning a Boolean result
1	Boolean TRUE
2 ERROR	User does not have administrator rights
3 ERROR	DFC command not valid on this installation
4 ERROR	Invalid command
5 - * ERROR	Internal error executing command



Deep Freeze Command Line Syntax



Deep Freeze has a maximum password limit of 63 characters. If a longer password is entered, the command will not be successful.

Syntax	Description
DFC password /BOOTTHAWED	Restarts computer in a Thawed state; only works on Frozen computers.
DFC password /THAWNEXTBOOT	Sets computer to restart Thawed the next time it restarts; only works on Frozen computers and does not force computer to restart.
DFC password /BOOTFROZEN	Restarts computer into a Frozen state; only works on Thawed computers.
DFC password /FREEZENEXTBOOT	Sets up computer to restart Frozen the next time it restarts; only works on Thawed computers and does not force computer to restart.
DFC get /ISFROZEN	Queries computer if it is Frozen. Returns error level 0 if Thawed. Returns 1 if Frozen.
DFC get /CLONE	Sets the clone flag for the purpose of imaging.
DFC password /CFG=[path] depfrz.rdx	Replaces Deep Freeze configuration information. Works on Thawed or Frozen computers. Password changes are effective immediately. Other changes require restart.
DFC get /version	Displays Deep Freeze version number.
DFC password /UPDATE=[path to installer file]	Sets up computer to restart in a Thawed state and install a Deep Freeze update.
DFC password /LOCK	Disables keyboard and mouse on computer. Works on Frozen or Thawed computer and does not require a restart.
DFC password /UNLOCK	Enables keyboard and mouse on computer. Works on Frozen or Thawed computer and does not require a restart.
DFC password /THAWLOCKNEXTBOOT	Sets up computer to restart in a Thawed state with keyboard and mouse disabled; only works on Frozen computers.



Syntax	Description
DFC password /BOOTTHAWEDNOINPUT	Restarts computer in a Thawed state with keyboard and mouse disabled; only works on Frozen computers
DFC password /WU [/UNLOCK] [/NOMSG /NOMESSAGE] [/THAW]	Windows Updates will be downloaded and installed on the computer. [/UNLOCK] Optional parameter to enable the Keyboard and Mouse during Windows Update. [/NOMSG /NOMESSAGE] Optional parameter to suppress all informational/warning messages from Deep Freeze during Windows Update. [/THAW] Optional parameter to return the machine into Thawed State after completion of Windows Update.
DFC password /ENDTASK	Ends the ongoing Workstation Task and reboots into Frozen state. Batch File Task and Thawed Period Task end immediately. Windows Update Task is completed.
DFC password /ENDTASK [/SHUTDOWN]	Ends the ongoing Workstation Task and reboots into Frozen state. Batch File Task and Thawed Period Task end immediately. Windows Update Task is completed. [/SHUTDOWN] Optional parameter to shut down the computer.
DFC password /FORMATTHAWSPACE	Formats all the ThawSpaces on the computer. Data stored on the ThawSpaces will be deleted permanently.
DFC password /DELETETHAWSPACE	Deletes all the ThawSpaces on the computer. Data stored on the ThawSpaces will be deleted permanently.

Deep Freeze Dashboard

Deep Freeze Dashboard is a visual representation of important Deep Freeze related information. To access the dashboard, go to *Home > Deep Freeze Dashboard*.

The dashboard provides the following key functionality:

- **Interconnected widgets:** All the widgets are interconnected and selecting the values in one widget automatically changes all widgets and the values in the computer grid. For example, if you select Deep Freeze Status as Frozen, the computer grid will show the computers that are Frozen.
- **Multiple Selections:** You can select values in multiple widgets to filter the output. For example, you can select Deep Freeze Status as Frozen and select a Tag. The result in computer grid will reflect all computers that are Frozen with the specific tag. Click the *Clear Filter* icon to clear multiple selections.



- On Demand actions: You can select one or more computers in the computers grid to perform actions.

The following tabs are available:

Dashboard Tab

The dashboard is a visual representation of the following parameters:

- Deep Freeze Status – shows the number of computers that are Frozen versus Thawed.
- Deep Freeze Thawed Time – shows the number of computers that are in a Thawed state for specified intervals.
- Deep Freeze Install Status – shows the number of computers where Deep Freeze is installed and whether they are up-to-date.
- Groups with Deep Freeze – shows the number of computers assigned to each group.
- Policies with Deep Freeze – shows the number of computers assigned to each policy.
- Tags – select or clear the tags to filter the widgets and computers grid accordingly.

Select one or more computers in the computers grid and perform the following On demand actions:

- Freeze – click the Freeze button
- Thaw – click the Thaw button
- More Actions
 - > Wakeup
 - > Restart
 - > Shutdown
 - > Reboot Thawed Locked
 - > Maintenance
 - ~ Run Windows Updates
 - ~ Lock Keyboard and Mouse
 - ~ Unlock Keyboard and Mouse
 - ~ Format ThawSpace
 - ~ End Workstation Task
 - ~ Delete Computer
 - > Send Message
 - > Tag
 - > Move to Group
 - > Assign Policy
 - > Assign Schedule



- > Remote Launch
- > Push and Launch
- > Control with RDC

Workstation Status Tab

This tab shows the computer status for all the computers where Deep Freeze Service is installed. The following information is displayed:

- Computer Name
- Tag
- Group
- Policy
- IP Address
- MAC Address
- Last Reported
- Version
- Status

Enter a parameter in the Search field to search a particular column. You can also filter by clicking the filter icon and tag computers by selecting the computers and clicking on the Tag button.

Workstation Task Summary Tab

This tab shows the Deep Freeze tasks that are scheduled, running and completed on the computers.

The following information is displayed:

- Computer Name
- Tags
- Group
- Policy
- Task name
- Last Reported
- Start Time
- End Time
- Status

Enter a parameter in the Search field to search a particular column. You can also filter by clicking the filter icon.



Data Igloo Service

The Data Igloo Service helps you map your data to different folders or drives. This service is especially useful if you are using Deep Freeze on your computer, ensuring that folders, user profiles, and registry key changes are retained across reboots.

To add Data Igloo to the Policy, go to *Add Policy > Deep Freeze Windows > Data Igloo* > select *Enable (install and inherit settings from Faronics Default policy)* or *Enable (Install and use below settings)*. Selecting this option installs Data Igloo on all computers using this Policy.



Selecting *Enable (install and inherit settings from Faronics Default policy)* or *Enable (Install and use below settings)* installs Data Igloo on the computers whenever the computers check-in. The computers check-in based on the heartbeat specified in [Cloud Agent Settings](#).

- *Enable (install and inherit settings from Faronics Default policy)* – installs the service and inherits settings from the Faronics Default policy. Selecting this option saves time in configuring all the policy settings. Selecting this option makes the settings for the current policy read-only.
- *Enable (Install and use below settings)* – installs the service and uses custom settings. Selecting this option will allow you to customize the settings for this service in the current policy.
- *Disable* will not install the service or will uninstall the service from the computers whenever the computers check-in.

You can configure settings for the Data Igloo Service through various tabs. The configuration settings for Data Igloo through various tabs are explained further in this chapter.

- [Folder Redirection Tab](#)
- [User Profile Redirection Tab](#)
- [Registry Key Redirection Tab](#)



Data Igloo tasks occur during a maintenance period. You must configure the settings in the [Maintenance Period](#) for the tasks to be updated as per the settings in the maintenance period.

Data Igloo Service provides the Data Igloo Status Report with detailed logs. For more information, see [Data Igloo](#).



Folder Redirection Tab

The Folder Redirection Tab allows you to move and map a folder to any volume or partition on the hard drive.

Complete the following steps to move a folder:

1. Specify the Source folder. For example, C:\files.
2. Specify the Destination folder. For example, D:\data.
3. Select the *Create folder if it does not exist* checkbox to create the Source or Destination if it does not exist.
4. Click *Add Redirection*.

Based on the above steps, the folder C:\files are mapped to D:\data.



Folder redirection will occur during a maintenance period. You must configure the settings in the [Maintenance Period](#) for the task to be updated as per the settings in the maintenance period.

Deep Freeze users: Ensure the Destination drive or folder is Thawed.

User Profile Redirection Tab

The User Profile Redirection Tab allows you to move a user profile to any volume or partition on the hard drive.

Complete the following steps move user profiles:

1. Select *Enable user Profile Redirection*.
2. Select *Redirect all User Profiles* and select the Destination. For example D:\ or D:\Users. Ensure that the Destination is always Thawed if you are using the Deep Freeze Cloud Service.
3. Alternatively, select *Allocate space for all User Profiles* and select the allocation size (between 15 MB to 1024 GB).



User profile redirection will occur during a maintenance period. You must configure the settings in the [Maintenance Period](#) for the task to be updated as per the settings in the maintenance period.

Deep Freeze users: Ensure the Destination drive or folder is Thawed.

Registry Key Redirection Tab

The Registry Key Redirection Tab allows you to move selected registry keys to any volume or partition on the hard drive.

Complete the following steps to move selected registry keys:

1. Select *Redirect registry key changes to*:
2. Specify the Destination. For example, D:\Registry Keys.



3. Specify the registry key and click *Add Registry Key*. Repeat this step for each registry key to be redirected.



Registry key redirection will occur during a maintenance period. You must configure the settings in the [Maintenance Period](#) for the task to be updated as per the settings in the maintenance period.

Deep Freeze users: Ensure the Destination drive or folder is Thawed.



Software Updater Service (Windows)

Software Updater Service automatically downloads and updates selected software applications on managed computers.

To add Software Updater to the Policy, go to *Add Policy > Deep Freeze Windows > Software Updater* > select *Enable (install and inherit settings from Faronics Default policy)* or *Enable (Install and use below settings)*. Selecting this option installs Software Updater on all computers using this Policy.



Selecting *Enable (install and inherit settings from Faronics Default policy)* or *Enable (Install and use below settings)* installs Software Updater on the computers whenever the computers check-in. The computers check-in based on the heartbeat specified in [Cloud Agent Settings](#).

- *Enable (install and inherit settings from Faronics Default policy)* – installs the service and inherits settings from the Faronics Default policy. Selecting this option saves time in configuring all the policy settings. Selecting this option makes the settings for the current policy read-only.
- *Enable (Install and use below settings)* – installs the service and uses custom settings. Selecting this option will allow you to customize the settings for this service in the current policy.
- *Disable* will not install the service or will uninstall the service from the computers whenever the computers check-in.

You can configure settings for the Software Updater through various tabs. The configuration settings for Software Updater through various tabs are explained further in this chapter.

- [Application Tab](#)
- [Software Deployment Tab \(for Usage Stats Ultimate Only\)](#)
- [Windows Update Tab \(for Ultimate only\)](#)
- [Advanced Options Tab](#)
- [Windows Update Dashboard](#)



The software updates occur during a maintenance period. After configuring the settings in the Application Tab and Advanced Options Tab, you must configure the settings in the [Maintenance Period](#) Tab. The selected applications will be installed and updated as per the settings in the [Maintenance Period](#) Tab.



Application Tab

Configure the following settings:

1. Select the products that you would like to install or upgrade on your managed computers. The following types of products are available:
 - > Web Browsers
 - > Messaging
 - > Media
 - > Runtimes
 - > Imaging
 - > Documents
 - > Utilities
 - > Compression
 - > Developer Tools
 - > Online Storage
 - > Other
 - > Web Conferencing
 - > Security
 - > Older Versions
 - > Custom Apps (Ultimate)
2. Click *Schedule Maintenance Period*. You will be taken to the [Maintenance Period](#) tab. Schedule a Maintenance Period to specify when the selected products will be downloaded and installed.
3. Optionally, configure settings in the [Advanced Options Tab](#).

Software Deployment Tab (for Usage Stats Ultimate Only)

The Software Deployment tab allows administrators to deploy software packages across all computers managed by Software Updater Service.

The Usage Stats Ultimate Service must be installed on at least one computer that contains the software package that is to be deployed.

The Usage Stats Service scans and sends the list of software packages once per hour.

If two packages with different versions are selected to be deployed, the higher version that is appropriate for the operating system on the target computer will be deployed.

Deploying the software package consists of the following steps:

1. Install Usage Stats service on at least one computer. The software package to be deployed must be installed on this computer.
2. Go to *Usage Stats > Manage Software Assets*.
3. Create a Package.



4. Go to *Software Updater* > *Software Deployment* tab and select the package to be deployed.

For the deployment, make sure to schedule a Maintenance Period by selecting the *Enable Maintenance Period* checkbox and select *Perform Software Updater* tasks.

Add Packages

For deploying packages from the Software Updater Service, you must complete the following steps:

1. Enable *Usage Stats Service*.
2. Apply the policy containing the Usage Stats Service on at least one managed computer. Usage Stats Service scans all the software applications installed on the managed computers and lists them in Managed Software Assets page.
3. Go to *Usage Stats* > *Managed Software Assets*.
4. Click the Software Name and click the *Package Details* tab.
5. Click *Add New*. Specify the values for the following parameters:
 - > Package Name – specify the name of the package.
 - > Software Version – select the software version.
 - > Install File Location – specify a UNC, HTTP or FTP location to download and install the files.
 - > Include Entire Directory – select the checkbox if you want the package to include the entire directory of the installer.
 - > Install if not found installed – this setting will install the software if it is not found installed on the target computer.
 - > Upgrade older versions – select the checkbox to upgrade from older versions. Select the version from the drop-down to the version to be upgraded.
 - > Architecture Support – select if it is 32-bit, 64-bit or 32 and 64-bit.
 - > OS Support – Specify the Minimum and Maximum Windows OS version supported by the package.
 - > MSI Options – select the behavior for Operation (Install, Uninstall). Select the behavior for Restart (Always, Not Set).
 - > Command Line – select the Custom checkbox and specify the command line for the installation.
 - > Install Timeout – select the timeout in Minutes. Software Updater Service will stop trying to install after the specified duration.
 - > Stop Deployment if Higher Version is Available – select this checkbox if you want to stop installation of the package if a higher version is detected.
6. Click *Save*.
7. Go to the Software Updater Service.



8. Click the *Software Deployment* tab.
9. Select the newly created package.

Software Updater Service will deploy the selected packages as per the specified maintenance period.

Windows Update Tab (for Ultimate only)

The Windows Update tab allows administrators to manage Windows updates and patch scans across all computers managed by Software Updater Service.



Windows Update can only be enabled for Policies without Deep Freeze enabled. In Policies without Deep Freeze enabled, the Software Updater will perform patch scan and Windows Update patch installation.

For Policies with Deep Freeze enabled, all Windows updates must be scheduled using the Windows Update Workstation Task in the Deep Freeze policy. Only Windows Update patch reporting will be available through the Software Updater.

The following policy configuration options are available:

- Perform Windows Updates – Select whether to *Always install* or *Install if approved*.
 - > Always install – Select this option to install category patches without approval required from Admin. Patches will be installed in the next maintenance period unless there is a deferred setting enabled in the policy.



Declined patches will not be installed even if they are set to *Always install*.

- > Install if approved – Select this option to require Admin approval prior to installation of the patch category.

Select the categories of updates to install:

- > Critical Update – A widely released fix for a specific problem that addresses a critical, non-security-related bug.
- > Security Update – A widely released fix for a product-specific, security-related vulnerability. Security vulnerabilities are rated by their severity as critical, important, moderate, or low.
- > Definition Update – A widely released and frequent software update that contains additions to a product's definition database often used to detect objects that have specific attributes such as malicious code, phishing websites, or junk mail.
- > Update Rollup – A tested, cumulative set of hotfixes, security updates, critical updates, and updates packaged together for easy deployment. A rollup generally targets a specific area (such as security), or a component of a product (such as Internet Information Services (IIS)).
- > Service pack – A tested, cumulative set of all hotfixes, security updates, critical updates, and updates. Additionally, service packs may contain additional fixes for



problems that are found internally since the release of the product. Service packs may also contain a limited number of customer-requested design changes or features.

- > Tool – A utility or feature that helps complete a task or set of tasks.
- > Feature pack – New product functionality that is first distributed outside the context of a product release and that is typically included in the next full product release.
- > Update – A widely released fix for a specific problem that addresses a non-critical, non-security-related bug.
- > Drivers – Software that controls the lower level input and output of a device.
- > Microsoft – Updates for Microsoft applications.
- > Upgrades – Feature updates to Windows Operating Systems.



By default, *Critical Updates* and *Security Updates* are set to *Always install*.

- Defer updates marked as 'Always install' by X days from release – Select this option to delay updates that are set to Always install until up to 30 days from the date of the release of the update.
- Patch scan frequency – Select from the drop-down list to schedule how frequently to perform patch scans.
 - > Once every 24 hours
 - > Once every 12 hours
 - > Once every 6 hours



Patch scans are triggered once every X hours from the last time it was performed, based on the selected frequency.

By default, patch scans are scheduled *Once every 24 hours*.

- Force auto-reboot prior to installation if user is logged on – Select this option to force auto-reboot a computer when the machine goes into maintenance if a user is logged on. When selected, the user will receive a notification that the computer is scheduled for maintenance.
- Download Windows updates prior to the scheduled maintenance period – Select this option to enable downloading Windows updates once on every reboot.
- Restart option after updates:
 - > Always restart – Select this option to reboot the computer after all Windows updates are installed.
 - > Reboot if required – Select this option to reboot the computer only if the Windows update requires a reboot. This is the default setting.

Prior to a restart, a warning message will be displayed to the user.



Starting from Windows 10

Starting from Windows 10, configure when feature updates or quality updates are to be installed and the targeted channel for which to install the updates.

- Semi-Annual Channel (Targeted) – Select this option to install the updates on select devices to evaluate the major release prior to deployment for the whole organization.
- Semi-Annual Channel – Select this option install the updates for all devices.

Feature updates include new capabilities and improvements. This update can be deferred until up to 365 days.

Quality updates include security improvements. This update can be deferred until up to 30 days.

These Windows update settings will override the corresponding Windows Update local policies on the target workstation.

For the Windows Updates, click *Schedule Maintenance Period* and select *Enable Maintenance Period*. Under *Actions*, select *Perform Software Updater tasks*.

After Windows Update is configured, apply the policy to the computers.

Advanced Options Tab

Configure the following settings:

- Update Only (Do not install, if not installed) – Select this option to avoid installing if the application is not installed. However, if the application is already installed, selecting this option will update it.
- Disable Shortcuts – Select this option to avoid installing shortcuts on the Desktop of the managed computers.
- Disable Auto Updates – Select this option to disable the auto-updates for the selected programs.
- Log Off Users (recommended if Windows auto log on is enabled) – Select this option if you are using Windows auto log on. Deep Freeze Cloud will log off the users from the computer before performing updates to the software. This is to ensure that the applications being updated are not locked by the users.



If you select *Log Off Users (recommended if Windows auto log on is enabled)* option, users may lose unsaved data due when the logoff occurs.

- Uninstall older versions of Java Runtime (Oracle and AdoptOpenJDK) – Select this option to uninstall older versions of Java Runtime. If you do not select this option, newer versions of Java Runtime will be installed with the existing version.

Click *Latest Updates* to view a full list of the software that can be updated, including version numbers.

Software Updater Cache Server

- Use Software Updater Cache Server – Select the checkbox if you have set up an Software Updater Cache Server on your network that downloads and distributes virus definitions to all computers. For more information, refer to [Software Updater Cache Server](#).



- Server IP – Specify the IP address of the Software Updater Cache Server.
- Server Name – Specify the name of the Software Updater Cache Server.
- Port – Specify the port of the Software Updater Cache Server.
- Connect to Web Server if there is no communication with the Software Updater Cache Server in the last x hours – Select this option if the managed computers must connect to the Faronics Web Server through the Internet if the Software Updater Cache Server is not accessible for some reason.

Windows Updater Cache Server

- Use Windows Updater Cache Server – Select the checkbox if you have set up a Windows Updates Cache Server on your network that downloads and distributes patches to computers requiring the patches.
- Server IP – Specify the IP address of the Windows Updater Cache Server.
- Server Name – Specify the name of the Windows Updater Cache Server.
- Port – Specify the port of the Windows Updater Cache Server.

Windows Update Dashboard

The Windows Update Dashboard provides a general view of Windows Update activity across all computers.

To access the dashboard, go to *Home > Windows Update Dashboard*.

Alerts

The dashboard alerts displays Windows Updates alerts about Vulnerable computers, outdated patch scans, and Critical and Security updates requiring approval.

Status Summary Tab

The Status Summary tab highlights the number of computers that are flagged as *Vulnerable*, and the number of patches currently missing in the environment.

The Status Summary tab provides the following key functionality:

- Interconnected widgets: All the widgets are interconnected and selecting the values in one widget automatically changes all widgets and the values in the Computers grid. For example, if you select Security Patch Status as Highly Vulnerable, the Computers grid will show the computers that are missing 2 or more security or critical patches.
- Multiple selections: You can select values in multiple widgets to filter the output. For example, you can select Security Patch Status as Highly Vulnerable and select a Tag. The result in the Computers grid will reflect all computers that are Highly Vulnerable with the specific tag. Click the *Clear Filter* icon to clear multiple selections.

The Status Summary tab is a visual representation of the following parameters:

- Security Patch Status – Shows the breakdown on current Security status of computers:
 - > Up to date – When a computer has no Security and Critical category patch missing and has a patch scan status reported not older than 7 days.



- > Vulnerable – If a computer has at least 1 Security or Critical category patch missing or has an outdated patch scan status (older than 7 days).
- > Highly vulnerable – A computer has 2 or more Security or Critical category patches missing.
- Patch Scan Status – Shows the breakdown of current patch status:
 - > Outdated – If a patch scan is older than 7 days
 - > Failed – If patch scan process has failed
 - > Initiated – If patch scan is in progress
 - > Successful – When the patch scan successfully completes on the device and is not older than 7 days
- Missing Patches – Shows the breakdown of total patches (Approved, Not approved, Declined) missing across all computers.
 - > Critical Update
 - > Security Update
 - > Definition Update
 - > Update Rollup
 - > Service pack
 - > Tool
 - > Feature pack
 - > Update
 - > Drivers
 - > Microsoft
 - > Upgrades
- Patches Pending Approval – Shows the breakdown of patches that are pending approval.
- Group – Shows the number of computers assigned to each group.
- Policy – Shows the number of computers assigned to each policy.
- Tags – Select or clear the tags to filter the widgets and Computers grid accordingly.
- Computers grid: Shows all the computers that match the widget selection on the dashboard. Click on the computer name to show the detailed view. You can select one or more computers in the grid and *Initiate Patch Scan* or *Install Missing Patches*.
 - > Initiate Patch Scan – This action will run a patch scan on the machine and update the current patch status of the computer to DF cloud.
 - > Install Missing Patches – This will force the machine to perform a *Run Maintenance Period task* where all patches that fulfill the installation criteria will be installed.



To successfully install missing patches:

1. *Maintenance Period* must be enabled under *General Settings*.
2. The *Perform Software Updater tasks* option must be enabled under the *Maintenance Period*.

Install missing patches will run maintenance during which it will only perform Windows Updates and not any other actions configured within the Maintenance Period.



You can export information to a PDF, image, or spreadsheet format by clicking the *Export To* icon at the top right of each widget.

Vulnerable Computers Tab

The Vulnerable Computers tab shows a list of computers with Security Patch Status flagged as Vulnerable or Highly Vulnerable.

You can arrange the list for each column in ascending or descending order by clicking on the column name. Enter a parameter in the Search field to search a particular column. You can also filter by clicking the filter icon.

Vulnerable Computers

This page shows the list of computers that are flagged as Vulnerable.

The following information is displayed:

- Computer Name
- Updates Managed by
- Policy
- Group
- OS Type
- Last Patch Scan
- Last Scan Status
- Missing Patches
- Failed Install
- Security Patch Status
- Next Maintenance Period

Click on the computer name to show the detailed view. Select one or more computers to *Initiate Patch Scan* or *Install Missing Patches*.

All Computers

This page shows the list of all computers that have Windows Update enabled.

The following information is displayed:

- Computer Name
- Updates Managed by
- Policy
- Group
- OS Type
- Last Patch Scan
- Last Scan Status
- Missing Patches
- Failed Install
- Installed Patches

Select one or more computers to *Initiate Patch Scan* or *Install Missing Patches*.



Detailed View

This page shows detailed information for each computer managed by Software Updater or Deep Freeze. Click on the Computer Name field and type the computer name or select the computer from the drop-down list.

The following information is displayed for each selected computer:

- Computer Name
- Security Status
- Managed by
- Policy
- Group
- OS Type
- Last Patch Scan
- Last Scan Status

The table shows information for the patches available for each computer:

- Patch Name
- Patch Type
- Approval Status (Not applicable to computers managed by Deep Freeze)
- Release Date
- Install Status:
 - > Installed – The patch is currently installed on the computer.
 - > Not Installed – This patch has not been marked for install, either by patch approval or setting patch category to 'Always install'.
 - > Install Failed – Installation was attempted but failed.
 - > Install Pending (for computers managed by Software Updater) – Marked for installation and will install in the next maintenance period.
 - > Install Deferred (for computers managed by Software Updater) – Patch install is deferred as defined in the policy. The deferred period is counted from the day of release of the patch and not from the time that the patch becomes applicable on the computer.
 - > Install Declined (for computers managed by Software Updater) – If patch approval status is set to Decline, this patch will have a declined install status for all computers.
- Install Date

Missing Patches Tab

The Missing Patches tab shows a list of missing and all patches.

You can arrange the list for each column in ascending or descending order by clicking on the column name. Enter a parameter in the Search field to search a particular column. You can also filter by clicking the filter icon.

Missing Patches

This page lists all category/type patches currently missing across all computers.

The following information is displayed:

- Patch Name



- Patch Type
- Approval Status
- Approved By
- Approved On
- Missing Computers
- Failed Computers
- Release Date
- Restart Required

Click on the patch name to show the detailed view. Select one or more patches and click *Approve* or *Decline*.

- **Approve** – Select this option to approve the selected patches for installation on the online computers in the next scheduled Maintenance Period.
- **Approve and Install Now** – Select this option to execute the assigned Maintenance Period on the online computers. Approved patches as well as missing patches that meet the installation criteria specified in the policy will be installed.



To successfully install missing patches:

1. *Maintenance Period* must be enabled under *General Settings*.
2. The *Perform Software Updater tasks* option must be enabled under the *Maintenance Period*.

Install missing patches will run maintenance during which it will only perform Windows Updates and not any other actions configured within the Maintenance Period.

- **Decline** – Select this option to decline patches.

All Patches

This page shows a list of all patches that have been installed, missing, or failed on 1 or more computers.

The following information is displayed:

- Patch Name
- Patch Type
- Restart Required
- Approval Status
- Approved By
- Approved On
- Missing Computers
- Failed Computers
- Installed Computers
- Release Date

Click on the patch name to show the detailed view. Select one or more patches and click *Approve* or *Decline*.



Detailed View

This page shows detailed information for each patch. Click on the Patch Name field and select the patch from the drop-down list.

The following information is displayed for each patch:

- Patch Name
- Patch Type
- Release Date
- Approval Status

Click on the pencil icon to change the approval status for each patch. Click on the disk icon to save the changes made.

You can select to install approved patches by clicking the *Install Now* button at the end of the *Patch Name* field. This will execute the assigned Maintenance period on the online computers. Approved patches as well as missing patches that meet the installation criteria specified in the policy will be Installed.

You can select to approve and install declined patches or patches that are not approved by clicking the *Approve and Install Now* button at the end of the Patch Name field. This will execute the assigned Maintenance period on the online computers. Approved patches as well as missing patches that meet the installation criteria specified in the policy will be Installed.

The table shows a list of computers for where the patch is missing:

- Computer Name
- Updates Managed by
- Policy
- Group
- OS Type
- Install Status
- Install Date



Anti-Executable Service

Anti-Executable Service ensures total endpoint productivity by only allowing approved applications to run on a computer or server. Any other program – whether they are unwanted, or simply unnecessary – are blocked from ever executing.



To enable communication between the computer and Deep Freeze Cloud Services through the firewall, ensure that outbound traffic is permitted on specified ports, and access is allowed on certain domains and IP addresses on both the console and client computer. Refer to [Authorized Domains and Ports](#).

To add Anti-Executable to the Policy, go to *Add Policy > Deep Freeze Windows > Anti-Executable > select Enable (install and inherit settings from Faronics Default policy) or Enable (Install and use below settings)*. Selecting this option installs Anti-Executable on all computers using this Policy.



Selecting *Enable (install and inherit settings from Faronics Default policy)* or *Enable (Install and use below settings)* installs Anti-Executable on the computers whenever the computers check-in. The computers check-in based on the heartbeat specified in [Cloud Agent Settings](#).

- *Enable (install and inherit settings from Faronics Default policy)* – installs the service and inherits settings from the Faronics Default policy. Selecting this option saves time in configuring all the policy settings. Selecting this option makes the settings for the current policy read-only.
- *Enable (Install and use below settings)* – installs the service and uses custom settings. Selecting this option will allow you to customize the settings for this service in the current policy.
- *Disable* will not install the service or will uninstall the service from the computers whenever the computers check-in.

You can configure settings for Anti-Executable through various tabs. The configuration settings for Anti-Executable through various tabs are explained further in this chapter.

- [Anti-Executable Terms](#)
- [How to use Anti-Executable](#)
- [Deployment Options](#)
- [Protection Settings](#)
- [Policy Control List](#)
- [Ransomware Prevention](#)
- [User Settings](#)
- [Central List](#)
- [Anti-Executable Dashboard](#)



Anti-Executable Terms

The following Anti-Executable terms are important:

- Allow – a file can be launched.
- Block – a file is prevented from being launched.
- Publisher – creator of a program. For example, Microsoft is the Publisher of Microsoft Word.
- Central List – a list of the files on your network. Files can be added to the Central List manually.
- Policy Control List – a list of all the files or Publishers for the particular policy. The files or Publishers are added to the Policy Control List from the Central List or the Anti-Executable Dashboard. Allow or Block files in a Policy Control List.
- Local Control List – a list of all the files or Publishers for the particular computer.
- Execution Control List – a combination list consisting of settings from the Local Control List and Policy Control List enforced on the computer. In case of a conflict in settings for a particular file or publisher, the Block settings always takes precedence.
- Anti-Executable Dashboard – The Anti-Executable Dashboard provides a dynamic view of the Anti-Executable activity across all computers. Anti-Executable actions can be performed directly from the dashboard.

How to use Anti-Executable

To make the most of Anti-Executable, follow these steps:

1. Identify – identify the files that users are installed or executing on the computers. Review the [Deployment Options](#) for more information.
2. Determine – determine the files that are authorized to run through the [Anti-Executable Dashboard](#).
3. Monitor – monitor the files from the [Anti-Executable Dashboard](#).

Deployment Options

Anti-Executable Service provides the following deployment options based on your requirement:



Deployment Option	When to use	Configuration Options
Staged Deployment	<p>When you are not aware about the files used by the users across your network.</p> <p>Anti-Executable Service collects information about the files launched by the users on their computers.</p>	<p>Stage 1 – Audit only: Logs which files are launched by the users or the system. It is recommended to leave stage 1 for 7-30 days to collect information about all the files used on the computers. Go to the Anti-Executable Dashboard to define which files are to be Allowed or Blocked in the Policy Control List. All files are allowed to run in this stage.</p> <p>Stage 2 – Partial Protection: The Policy Control List is enforced. All files not specified in the Policy Control List (Unknown Files) are allowed and reported as violations in the Anti-Executable Dashboard.</p> <p>Final Stage – Full Protection: The Policy Control List is enforced. All files not specified in the Policy Control List (Unknown Files) are blocked and reported as violations in the Anti-Executable Dashboard.</p>
Deploy on newly installed or imaged computer environment	<p>When it is a clean computer with known programs and all files can be <i>Allowed</i>.</p> <p>This will create a Local Control List of all files present on a computer.</p>	<p>To globally block files on computers, add those files as Blocked in Policy Control List.</p> <p>Unknown files are Blocked and violations are reported in the Anti-Executable Dashboard.</p>
Custom Deployment	Create your own custom configuration.	<p>You can create custom configuration for the following:</p> <ul style="list-style-type: none"> Files in the Policy Files on the computer Unknown files on the computer

Protection Settings

Configure the following settings:

Protection Status

Enable Protection – select this option to launch only the approved applications.

Disable Protection – select this option to launch all applications.

Settings

Deployment options

Choose one of the following deployment options:



Option 1: Staged Deployment

Staged Deployment on computers with unauthorized software. Select this option and click *Next*. The staged deployment has 3 steps:

- Stage 1 – Audit only (build a Policy Control List): In this stage, Anti-Executable runs in logging mode to collect information about the files and executables launched on the computers. All files are allowed to run on client computers and file executions are logged. Unknown files are allowed to launch and violations are logged in the [Anti-Executable Dashboard](#).
 - > Allow All Windows OS files – add all Windows OS files to the Local Control List as *Allowed*.



To keep the Local Control List updated with all Windows OS files after installation, run Windows Updates during Maintenance Mode.

- Stage 2 – Partial Protection (enforce Policy Control List and Allow Unknown files): In this Stage, files specified in the Policy Control List are Allowed or Blocked as defined. All files not specified in the Policy Control List (unknown files) are allowed to execute and reported as violations in the [Anti-Executable Dashboard](#).
 - > Allow All Windows OS files – add all Windows OS files to the Local Control List as *Allowed*.
- Final Stage – Full Protection (Enforce Policy Control List and Block Unknown files): In this stage, the Policy Control List is enforced and all Unknown files are blocked. Files specified in the Policy Control List are Allowed or Blocked as defined. All files not specified in the Policy Control List (Unknown Files) are Blocked and reported as violations in the [Anti-Executable Dashboard](#).
 - > Allow All Windows OS files – add all Windows OS files to the Local Control List as *Allowed*.

Option 2: Deploy on newly Installed or Imaged computer environment

This option authorizes everything that's pre-installed on the computer for execution and creates a Local Control List. All executables installed on the computer are allowed to run unless it is explicitly blocked in the [Anti-Executable Dashboard](#).

In this option, the Policy Control List is enforced. Unknown Files are blocked and violations logged in the [Anti-Executable Dashboard](#).



To globally block files on client computers, add those files as *Blocked* in Policy Control List.

File and folder authorization set in Policy Control List, overrides authorization set in Local Control List.

Option 3: Custom Deployment

The custom deployment is based on your unique requirement which can be configured in the policy. Configure the following settings:



Authorization Settings:

- Policy Control List – A Policy Control List contains a list of files and executables for the particular policy with the information if the file is *Allowed* or *Blocked*. Select one of the following options:
 - > Enforce. Log Violations – enforce the Policy Control List and log the violations in the [Anti-Executable Dashboard](#). The files will be Allowed or Blocked as specified in the Policy Control List.
 - > Do Not Enforce. Log Violations – do not enforce the Policy Control List and log the violations in the [Anti-Executable Dashboard](#).
- Unknown Files – Unknown Files are the files that are not in the Local Control List or Policy Control List. Select one of the following options:
 - > Allow and Log Violations – allow the files to run and log the violations in the [Anti-Executable Dashboard](#).
 - > Block and Log Violations – block the files and log the violations in the [Anti-Executable Dashboard](#).
- Scan all files and create a Local Control List during installation – scan the computer and create a Local Control List of all files present on the computer when the Anti-Executable Client is installed.
- Allow All Windows OS files – add all Windows OS files to the Local Control List as *Allowed*.



To keep the Local Control List updated with all Windows OS files after installation, run Windows Updates during Maintenance Mode.

Policy Control List

File Authorization

Add, Remove, Allow, or Block files from the File Authorization pane:

- Add – click *Add* to add the files to the Policy Control List. In the *Add files* screen, select *Add files from the Central List* or *Add files from computer*. Select one or more files and select Allow or Block in the *Add as* drop-down.
- Remove – select the files and click *Remove*.
- Allow – select the files and click *Allow*.
- Block – select the files and click *Block*.

Folder Authorization

Add, Remove, Allow, or Block folders from the Folder Authorization pane:

- Add – specify Folder Path, select Allow or Block, and click *Add*. You can optionally add a comment.
- Allow – select a folder and click *Allow*. You can also allow multiple folders.
- Block – select a folder and click *Block*. You can also block multiple folders.



Publisher Authorization

- Add – click *Add* to add Publishers to the Policy Control List. In the *Add Publishers* screen, select *Add publishers from Central Control List* or *Add publishers from computer*. Select one or more publishers and click *Update*.

Advanced Control

- Monitor DLL Execution – select this option to monitor DLLs. If this checkbox is not selected, the DLLs will not be monitored even if they have been added to the Central List.



The Monitor DLL Execution option is only available for *Deploy on newly Installed or Imaged computer environment*.

- Monitor JAR Execution – select this option to monitor JAR files. If this checkbox is not selected, the JAR files will not be monitored even if they have been added to the Control List.
- Monitor VBScript Execution – select this option to monitor VBScript files. If this checkbox is not selected, the VBScript files will not be monitored even if they have been added to the Control List.
- Monitor PowerShell Script Execution – select this option to monitor PowerShell Script files. If this checkbox is not selected, the PowerShell files will not be monitored even if they have been added to the Control List.

Ransomware Prevention

Configure the following settings to protect the computers from ransomware:

- Enable Ransomware Prevention – select this option to protect your computers from Ransomware using Anti-Executable. If this option is not selected, Anti-Executable will not protect your computers from Ransomware.
- Prevention Level – Select *Standard* to allow Anti-Executable to manage the settings for Ransomware protection. Alternatively, select *Custom* to select the required options:
 - > Block known Ransomware file extensions – blocks the know Ransomware file extensions. Click *View* to see the list of file extensions that will be blocked. Faronics will keep updating the list to keep it current.
 - > Disable Remote Access (RDP) on Client Computers – disables remote access on client computers using the Remote Desktop Protocol.
 - > Disable Macros And ActiveX in MS Office – disables macros and ActiveX in Microsoft Office files.
 - > Enable "Hide extensions for known file types" windows – disables the option that allows users or malicious programs to hide extensions.
 - > Disable Windows Scripting Host (WSH). Disable running of all kind of scripts like (VB Script and JScript) that depend on WSH – disables know scripts from running on the computers that can be used maliciously by Ransomware.



- > Disable Admin \$ shares on Windows – disables are hidden network shares created by Windows operating systems that allow system administrators to have remote access to every disk volume on a network-connected system.
- > Turn off Autoplay for all media and devices in Windows – disables auto-play for all kinds of media and devices to prevent Ransomware from automatically running when it is disguised as a media file.

User Settings

Configure the following settings:

Trusted Users

Trusted users are the Windows User accounts or Groups that are authorized to manage the Local Control List, change protection mode and allow execution for unknown files.

- Object Type – select whether a *User* or a *Group*.
- User Name – specify the user name and click *Add*.
- Enable Anti-Executable Password (Optional) – this will force the above authorized Anti-Executable users to also enter a password.
 - > AE Administrator User Password – specify the password. Click *Show Password* to make the password visible. The Administrator User can manage Local Control List, Users, and Setup and can uninstall Anti-Executable.
 - > AE Trusted User Password – Can configure Anti-Executable, and set the Local Control List. specify the password. Click *Show Password* to make the password visible. They are prohibited from uninstalling Anti-Executable and cannot manage Users or Setup.

User Alerts

- Execution Control List violation message – enter a message or use the default message. This message is displayed to the user when there is a violation.
- Blocked notification message – enter a message or use the default message. This message is displayed to the user when an executable is blocked from running.

Stealth Mode

Stealth Mode is a group of options that control visual indication of Anti-Executable's presence on a system. Stealth functionality has the following options:

- Hide Notification – prevents the Alert from being displayed.
- Hide icon on system tray – hides the Anti-Executable icon in the system tray.



Logging

- Log to file – select the checkbox to create log files.
- Number of log files – specify the number of log files (up to a maximum of 10). The logging information is stored in the files serially. For example, if there are 3 files A, B and C, Anti-Executable first writes the error logs to file A. Once file A is full, it starts writing to file B and finally file C. Once file C is full, the data in file A is erased and new logging data is written to it.
- File size – Select the size of each file in MB. There can be a maximum of 10 log files of up to 10 MB each i.e. total 100 MB.

Central List

A Central List is a repository of files and Publishers. You can populate the Central List by adding the files and Publishers by using the [Anti-Executable Data Import Utility](#).

The following actions are available:

- Add – click *Add* to add files and Publishers to the Central List.
- Remove – select one or more files or Publishers and click *Remove*.
- Files View/Publishers View – toggle between files or Publishers.

Anti-Executable Dashboard

The Anti-Executable Dashboard provides a dynamic view of the Anti-Executable activity across all computers. Anti-Executable actions can be performed directly from the dashboard.

Go to *Home > Anti-Executable Dashboard* to launch the Anti-Executable dashboard.

Overview

The following dynamic widgets are available:

- Protection Status – shows the number and % of computers where Anti-Executable is Enabled vs Disabled.
- Violations – shows the breakdown of violations count based on different violation types.
- Violations by Policies – shows the number and % of violations by policy name.
- Violations by Groups – shows the number and % of violations by group name.
- Violations History – shows the detailed violation history with the Date, File Name, Computer, Policy, Group, Violation Type, Status, and Violations.
- Daily Violation – shows a graph of number of violations by date.
- Violations Trend – Weekdays – shows a graph of number of violations by weekday.
- Most Blocked Programs – shows a graph of the most blocked program with the number of violations.
- Computers with Most Violations – shows a graph of computers with the most number of violations.
- Computers – shows a list of computers with the AE Status, AE version, Policy, Group, and Violation Report, and where you can select on which computers to perform *Live*



Actions (Enable Protection, Disable Protection, Enable Maintenance Mode, Initiate a Local Control Scan).

File Events

File Events pane captures and summarizes Anti-Executable events in the context of a file. Files that need to be reviewed by the administrator are in bold.

Actions: *Allow* and *Block* actions have the following options:

- In All Policy Control List – This option Allows or Blocks the file in all Policy Control Lists in all policies where this file exists.
- In Reported Policy Control List – This option Allows or Blocks the file in Policy Control Lists where the file has been reported as a violation.

The table has the following fields:

- Event Type – The following Event types are shown:
 - > Unknown File Allowed – a file that is not defined in Policy Control List or Local Control List, but is allowed to execute in Audit mode or Unknown File is set to Allow in Policy Settings.
 - > Unknown File Blocked – a file that is not defined in Policy Control List or Local Control List, or Unknown File is set to Block in Policy Settings.
 - > Block Override – a file that is defined as Blocked in Policy Control List but is allowed to run since Anti-Executable is running in Audit mode with Policy Control List settings not enforced.
 - > Control List Blocked – this event is logged when a file that is specified as Blocked in Policy Control List or Local Control List tries to execute and is blocked by Anti-Executable.
 - > Add – Maintenance Mode – this event is logged when a new file is added on a computer and it is not defined or present in Local Control List or Policy Control List.
- Add – AE Admin – An unknown file that gets blocked but an AE Admin chooses to add it to local client side file exceptions.
- Name
- Details
- Product Name
- Count
- On Computers
- In Policy
- Groups
- Actions
- Action Taken

Computer Events

Computer Events summarizes Anti-Executable events keeping a specific computer in context. Computers that need to be reviewed by the administrator are in bold.

Actions: Select one or more events and click *Enable Protection*.

The table has the following fields:



- Event Type – The following Event Types are shown:
 - > Anti-Executable protection disabled over 12 hours
 - > Anti-Executable protection disabled over 6 hrs but less than 12
 - > Anti-Executable computer in maintenance mode for over 6 hours
 - > Anti-Executable computer in maintenance mode for over 3 hrs but less than 6
 - > Computers with violations (highest count will show up first in the grid)
 - > Computers with new files added in Maintenance (highest count files show up first)
- Computer Name
- Count
- Last Reported
- In Policy
- Tags
- Groups
- Action
- Action Taken

AE Policy Stats

AE Policy Stats shows the status of each Anti-Executable policy. It clearly shows the deployment type for the Anti-Executable policy and other policy related information. The edit option allows administrators to change the Deployment type or change the Stage in the 3 stage deployment.

Actions: Hover your mouse on any of the Policies and click *Edit* to change the Deployment Type if required.

The table has the following fields:

- Policy Name
- Deployment Type
- Computers
- Unknown Files
- Files in Control List
- Unknown Files Violations in the Last 14 Days
- Policy Deployment Completion

Client Event Logs

Client Event Logs shows events occurring on the Anti-Executable client and reported to Deep Freeze Cloud by all computers where it is installed. This log will be a combination of all Anti-Executable events reported and displayed in order of the time the event occurred on the computer.

Actions: Select one or more entries and click *Allow* or *Block*. *Allow* and *Block* actions have the following options:

- In All Policy Control List – This option Allows or Blocks the file in all Policy Control Lists in all policies where this file exists.
- In Reported Policy Control List – This option Allows or Blocks the file in Policy Control Lists where the file has been reported as a violation.



- In Reported Computer's Local Control List – This option Allows or Blocks the file in Policy Control Lists where the file has been reported as a violation.

The table has the following fields:

- Computer Name
- File Name
- Event Description – The following Event types are shown:
 - > Unknown File Allowed
 - > Unknown File Blocked
 - > File Added in Local Control List in AE Maintenance Mode
 - > File Added to Local Control List by AE User
 - > File Blocked - Defined block in Control list
- Time Stamp
- User
- Tags
- Group
- Policy
- Set Authorization
- Action Taken

Client Side File Exception

Client Side File Exception is a collection of all file exceptions added across all Anti-Executable computers that include the following situations:

- Local Control List in maintenance mode
- Files Added to Local Control List by Anti-Executable Administrator
- Files added to only Local Control List

Actions: Select one or more entries and click *Allow* or *Block*. *Allow* and *Block* actions have the following options:

- In All Policy Control List – This option Allows or Blocks the file in all Policy Control Lists in all policies where this file exists.
- In Reported Policy Control List – This option Allows or Blocks the file in Policy Control Lists where the file has been reported as a violation.
- In Reported Computer's Local Control List – This option Allows or Blocks the file in Policy Control Lists where the file has been reported as a violation.

The table has the following fields:

- Computer Name
- File Name
- File Version
- Local Authorization
 - > Allowed - AE Maintenance
 - > Allowed - AE User Local
 - > Blocked - AE User Local



- Group
- Policy
- Set Authorization
- Publisher
- Product Name
- Comment
- Time Stamp
- Added By

Local Control List

Local Control List provides a dynamic table showing the Local Control List with all files for each computer managed by Anti-Executable. Select or search for the computer in the *View Local Control List of Computer* field. Select a computer to retrieve its Local Control List. A task is initiated and the Local Control List will be retrieved within 10 minutes.

Actions: Select one or more entries and click *Allow* or *Block*. *Allow* and *Block* actions have the following options:

- In All Policy Control List – This option Allows or Blocks the file in all Policy Control Lists in all policies where this file exists.
- In Policy Control List – This option Allows or Blocks the file in Policy Control List selected from the list.

The table has the following fields:

- File Name
- File path
- File Version
- Set Authorization
- Publisher
- File Hash
- Product Name
- Comment
- Time Added
- Added By

Central List

Central List tab provides a dynamic table which is an aggregation of all files reported across all Local Control Lists. Actions can be performed directly from the Central List tab.

Actions: Select one or more entries and click *Allow* or *Block*. *Allow* and *Block* actions have the following options:

- In All Policy Control List – This option Allows or Blocks the file in all Policy Control Lists in all policies where this file exists.
- In Policy Control List – This option Allows or Blocks the file in Policy Control List selected from the list.

The table has the following fields:

- File Name



- File Version
- Publisher Name
- Hash
- Product Name
- Comment
- Date



WINSelect Service

WINSelect Service empowers administrators with full control over its abilities. Windows operating system features, Start menu functionality, Internet Explorer capabilities, and Windows Explorer options can all be heavily customized to suit organizational needs.



To enable communication between the computer and Deep Freeze Cloud Services through the firewall, ensure that outbound traffic is permitted on specified ports, and access is allowed on certain domains and IP addresses on both the console and client computer. Refer to [Authorized Domains and Ports](#).

Program Requirements

Supported programs:

- Microsoft Office 2003, 2007, 2010 and 2013
- Internet Explorer 10 and above
- Mozilla Firefox (up to version 62.0)

To add WINSelect to the Policy, go to *Add Policy > Deep Freeze Windows > WINSelect > select Enable (install and inherit settings from Faronics Default policy) or Enable (Install and use below settings)*. Selecting this option installs WINSelect on all computers using this Policy.



Selecting *Enable (install and inherit settings from Faronics Default policy)* or *Enable (Install and use below settings)* installs WINSelect on the computers whenever the computers check-in. The computers check-in based on the heartbeat specified in [Cloud Agent Settings](#).

- *Enable (install and inherit settings from Faronics Default policy)* – installs the service and inherits settings from the Faronics Default policy. Selecting this option saves time in configuring all the policy settings. Selecting this option makes the settings for the current policy read-only.
- *Enable (Install and use below settings)* – installs the service and uses custom settings. Selecting this option will allow you to customize the settings for this service in the current policy.
- *Disable* will not install the service or will uninstall the service from the computers whenever the computers check-in.

You can configure settings for WINSelect through various tabs. The configuration settings for WINSelect through various tabs are explained further in this chapter.

- [Kiosk Tab](#)
- [System Tab](#)
- [Application Tab](#)
- [Printers Tab](#)
- [Acceptable Use Policy Tab](#)



- [Administrator Tab](#)

Kiosk Tab

Configure the following settings:

Enable/Disable

- Enable Protection – select this option to enable WINSelect protection on the computers. Clear the checkbox to disable protection on the computers.
- Disable WINSelect for Administrators – select this option to disable WINSelect on the computers when an administrator logs in.

Kiosk Mode

This setting allows administrators to create a kiosk type computer where only specified executables can be run.

- Enable – select this option to enable Kiosk Mode.
- Disable Tablet Mode (Windows 10 only) – select this option to disable the tablet mode for Windows 10.

Configuration

Configure the orientation, grid layout, and background of the kiosk.

- Orientation – Choose between landscape or portrait.
- Grid layout – Select this option to customize the layout of the icons in the preferred orientation.
 - > Landscape – 5x3, 4x2, 3x2, 6x3
For example: a 5x3 layout displays five icons per row, over three rows.
 - > Portrait – 3x5, 3x4, 2x3
For example: a 3x5 layout displays three icons per row, over five rows.
- Background – Click the pencil icon to edit the wallpaper for the background. Choose the background from the Wallpaper Gallery or upload a custom wallpaper. To upload a wallpaper:
 - A. Click *Add a Custom Wallpaper*.
 - B. Select the image to upload as the wallpaper.
 - C. Click *OK*.



Image dimensions should be between 1024 x 768 and 1920 x 1080 pixels. Only image files are allowed (jpeg, jpg, png), and must not exceed 2 MB.



Header and Footer

Place up to three elements on the left, right, and center in the header and footer sections. You can also customize the text font, text alignment, text size, and text color for certain elements.

- Click *Add* on the top right.
- Choose the element to add.
 - > Text – Enter up to a maximum of 100 characters.
You can enter text in any of the supported languages. The text in the assigned language will be displayed when that language is selected as the default language for the kiosk.
 - > Logo – Choose the logo from the Logo Gallery or upload a custom logo.



Image dimensions should be under 300 x 150 pixels. Only image files are allowed (jpeg, jpg, png), and must not exceed 300 KB.

- > Date and Time – Select the date format, time format, and a single-line or two-line display format.
- > Power Control – Select to display the *Logoff*, *Shutdown*, or *Restart* power options.
You can customize the icon color, placement, text font, text alignment, text size, and text color.
- > Language Picker – Choose the displayed language for the kiosk.

Elements for the Header and Footer sections can be selected multiple times except for the Language Picker. You can only select the Language Picker once and display it in either the Header or Footer section.

Body

Place up to a total of 50 applications and/or weblinks in the kiosk. You can adjust the placement of the applications and weblinks by dragging and dropping the element rows (not the icons).

- Click *Add* on the top right.
- Choose *Application* or *Weblink*.
- Under *Configuration*:
 - > Application
Configure the application name, application path, command line parameters, and tooltip description. Set the application to Auto Launch with the option to always maintain full screen or as Hidden application running in the background.
Select the *Allow Other Applications to Run in This Folder* to allow other applications to run from the folder designated in the Application Path.
You can set the application name and tooltip description to any of the supported languages.



- > Weblink
Enter the URL, caption, and tooltip description.
You can set the weblink caption and tooltip description to any of the supported languages.
- > Under *Design*, configure the text font, text size, text color, tile color, and icon title. Choose an icon from the Icon Gallery or add a custom icon.



Only image files are allowed (jpeg, jpg, png), and must not exceed 300 KB.

System Tab

System

The System page allows you to configure the system-wide options:

Task Manager

- Disable Task Manager (Ctrl+Alt+Del) – select this option to disable the Task Manager. This prevents the user from accessing the Task Manager and ensures currently running tasks and processes can only be ended by an authorized user.

Windows Explorer

- Disable right-click – select this option to prevent users from accessing commands such as View, Paste, Copy, and Properties in Windows Explorer.
- Disable UNC paths – select this option to prevent users from accessing shared network resources.
- Disable folder manipulation – select this option to prevent users from manipulate the folders on the system.
- Disable drag and drop – select this option to prohibit users from moving files and folders to different locations. This option also disables selecting text and images by dragging the mouse pointer in all applications.
- Disable RunAs – select this option to enable or disable the RunAs option when Kiosk is enabled. This option is enabled by default.

Control Panel

The Control Panel page provides options for restricting the display of Windows Control Panel applets. Windows Control Panel can be accessed by the user but the icons may be selectively hidden.

- Show applets – select this option to display each applet found in the Control Panel.
- Hide All applets – select this option to prevent access to every Control Panel applet.
- Hide Selected applet – select the particular applet to hide it.
- Specify applet – specify the name of the applet and click *Add*.



Desktop & Windows Taskbar

The Desktop & Windows Taskbar page provides options for restricting the use of the computer desktop and Windows Taskbar.

Desktop

- Disable right-click on Desktop – select this option to disable right-click on the Desktop. The user will not be able to access the right-click menu and commands such as New and Properties.
- Disable right-click on Desktop icons – select this option to disable right-click on the Desktop icons. Users will not be able to access commands such as Open. The user will also not be able to delete shortcuts or rename them.
- Hide all icons – select this option to hide all the icons on the Desktop.
- Hide selected icons – select the icon that must be hidden.
- Add Desktop icon – specify the Desktop icon and add it to the list.

Taskbar

- Disable right-click on Taskbar and Start button – select this option to disable right-click on Taskbar and the Start button.
- Hide Taskbar icons – select this option to hide the icons in the Taskbar.
- Disable Action Center – select this option to disable the Action Center.

Drives and File Extensions

The Drives and File Extensions page provides options for restricting access to drives and specified file extensions for each application installed on the computer:

- Disable Selected Drives – select the available drives and file extensions to be disabled by selecting the checkbox next to each one. Use the Select All option if required. Files and directory structures are not visible once this feature is enabled. For example, if all drives are selected, exploring the directories contained within is not permitted.
- Disable Removable Drives – select this option to disable removable drives. This feature prevents the user from seeing any removable drives connected.
- Disable access to user directory – select this option to disable access to the user directory. The users will not be able to browse their own user directory.



The *Disable access to user directory* option will take effect only if the system drive is disabled.

Disable Selected File Extensions

- Disable – select the extensions that must be disabled. If a file extension is selected, then the file extension will be disabled across all drives.
- Add File Extensions – specify the file extension and click *Add* to add a new file extension to the list.



Start Menu

Customize access to the Start menu by selecting one or more options:

- Enable Start Menu – select this option to allow access to the Start Menu.
- Disable all Start Menu items – select this option to disable Start Menu completely.
- Disable selected Start Menu items – select this option to disable the selected Start Menu items. Select the checkbox for the specific items/operating system version you want to disable. Following is a list of the Start Menu items that can be disabled:
 - > Administrative Tools
 - > Control Panel, Printers and Network Connections...
 - > Cortana
 - > Devices Charm
 - > Documents (Classic Menu Only)
 - > Downloads
 - > Favorites
 - > File Explorer
 - > Games
 - > Help and Support
 - > Homegroup
 - > Lock Screen / Lock
 - > Log Off/ Sign out
 - > Most Frequently Used Programs / Most Used
 - > My Computer / Computer
 - > My Documents / Documents
 - > My Music / Music
 - > My Network / Network
 - > My Pictures / Pictures
 - > Pinned Programs List
 - > Programs / All Programs / All apps
 - > Recent Documents/Recent Items
 - > Recorded TV
 - > Run...
 - > Search
 - > Search Charm
 - > Set Program Access and Defaults/Defaults Program...
 - > Settings Charm
 - > Share Charm
 - > Shut Down
 - > Start Button Context Menu
 - > Start Charm
 - > Task Switching Bar



- > Taskbar and Start Menu
- > User Specific Folders
- > User's Folder
- > Videos
- > Windows Store
- Disable right-click Start Menu item – select this option to disable right-click for the Start Menu and prevent the user from accessing the secondary menu. This option is not available for Windows 8.1.
- Enable Classic Style Start Menu – select this option to enable the Classic Style Start Menu.

Windows 8.1/Windows 10 and above

Select the following options if Windows 8.1 is installed on the managed computers:

- Always boot to Desktop (Windows 8.1 Only) – select this option if you want the computers to always boot into Desktop mode. If you do not select this option, the computers running Windows 8.1 will boot into the Start Screen by default.
- Hide Task View (Windows 10 and above) – select the checkbox to disable Task View on Windows 10 and above. The Task View allows you to switch between programs currently running on the computer.
- Disable uninstall of apps – select this option to disable uninstalling Windows 8.1 apps by the user.
- Disable pinning of apps to taskbar – select this option to disable pinning the Windows 8.1 apps to the taskbar by the user.
- Disable right-click on tiles and customization of start screen – select this option to disable the ability to right-click tiles on the start screen and also disable the customization of the start screen by the user.
- Disable Xbox Game Bar (Windows 10 and above) – select this option to disable Xbox Game Bar.

Network Restrictions

Network Restrictions allow you to restrict access to specific URL or IP range.

- Enable – select this option to enable Network Restrictions.
- Specify the URL – specify the URL and click *Add*.
- Specify IP address (or range) – specify a single IP or a range of IP address and click *Add*.
- Allow selected – select this option to allow the selected IP addresses.
- Disallow selected – select this option to block the selected IP addresses.

Hot Keys

The Hot Keys node provides options for restricting the use of specified hot keys at the system level. Key combinations that work in multiple applications can be disabled regardless which application is enabled on the computer.

- Select hot keys to disable – select the hot keys that must be disabled.
- Specify Hot key – specify the hot key and click *Add* to add a hot key to the list.



Application Tab

Configure the following settings:

Application

This feature allows customizing of applications. This feature is unavailable when Kiosk mode is enabled. If administrators want to create a Windows environment featuring only specific applications, but do not wish to create a WINSelect Kiosk, they can specify the applications on this page:

- Allow only selected desktop applications – select this option to allow only the selected applications to run.
- Disallow selected desktop and modern applications – select this option to block the selected applications.
- List all programs – click the *List all programs* button to list all the programs available on Deep Freeze Cloud Console.
- Application Name – enter the application name and click *Add* to all programs to the list.

Microsoft Office

Select the menu items to be disabled from Microsoft Office:

- Disable Macro
- Disable VB editor
- Disable Templates and add-ins
- Disable execution of Visual Basic application
- Disable Web
- Disable detect and repair

Internet Browser

This feature provides options for restricting access to Internet browser functions and menus. Enable these features when users are required to access the Internet, but are not permitted to save locations, print pages, access the favorites menu, etc.

- Disable right-click – select this option to disable right-click from the browser.
- Prevent opening of files or folders from address bar – select this option to prevent users to navigate to files or folders from the address bar.
- Remove Address Bar (Internet Explorer 9.0 and higher only) – select this option to remove the address bar and prevent Internet browsing.
- Home Page – specify the URL that will always be displayed as the home page when the user launches the browser.
- Menus – select the browser and the menus that must be disabled.
- Disable Favorites menu of Internet Explorer – select this option to disable the Favorites menu.



Printers Tab

The Printers node provides options for restricting access to any available printers connected to the computer. Use this feature to restrict printers entirely, or to permit users to print a specific amount of material on one or more selected printers. Access to offline printers can also be restricted (since offline printers can still receive printing jobs).

- Enable Printer Quota – select this option to specify the maximum number of pages that can be printed from the computer.
- Disable all – select this option to disable all printers.
- Disable Selected – select the printers that must be disabled.
- Printer Name – specify the name of a printer and click *Add* to add the printer to the list.
- Print Quota in pages per session (0 means no limit)– specify the maximum number of pages that can be printed in a session.

Acceptable Use Policy Tab

This feature allows the administrator to specify the conditions of use each time a user logs into a computer. The user must accept this policy before using the computer.

- Display AUP at start up – select this option to display the AUP when the computer starts up. Enter the AUP.

Administrator Tab

Administrator

- Enable client password – select this option to specify a password for the WINSelect client.

User Session

This feature provides the option to create user sessions that are limited in duration. This allows the administrator to specify the amount of time a user can spend logged into a computer.

- Enable – select this option to enable a user session at the computer.
- Duration of User Session in minutes – select a value ranging from 5 minutes to 1440 minutes.
- Number of codes to generate – select a value ranging from 1-1000.
- Log off Windows User if no session code is entered in X minutes – select this option to disable the session timer up to a maximum of 120 minutes. When disabled, user sessions are not limited in duration and remains logged into the computer.
- Show Warning message x minutes before session expires – select this option to show a warning message. Specify the value.
- Reboot computer after user session finishes – select this option to reboot the computer after the session ends.
- Generate Code – click *Generate Code* to generate the codes based on the configured settings.
- Export All Codes – click *Export All Codes* to export the codes in .csv format.
- Print All Codes – click *Print All Codes* to print the generated codes.



Cloud Sync

Cloud Sync allows users to access and save documents from Google Drive, OneDrive, or Dropbox without having to sync them onto the local system. On clicking a file, Cloud Sync downloads the files from the specified cloud account to the local system and uploads it back to the cloud during the user session.

To add Cloud Sync to the Policy, go to *Add Policy > Deep Freeze Windows > Cloud Sync > select Enable (install and inherit settings from Faronics Default policy) or Enable (Install and use below settings)*. Selecting this option installs Cloud Sync on all computers using this Policy.



Selecting *Enable (install and inherit settings from Faronics Default policy)* or *Enable (Install and use below settings)* installs Cloud Sync on the computers whenever the computers check-in. The computers check-in based on the heartbeat specified in [Cloud Agent Settings](#).

- *Enable (install and inherit settings from Faronics Default policy)* – installs the service and inherits settings from the Faronics Default policy. Selecting this option saves time in configuring all the policy settings. Selecting this option makes the settings for the current policy read-only.
- *Enable (Install and use below settings)* – installs the service and uses custom settings. Selecting this option will allow you to customize the settings for this service in the current policy.
- *Disable* will not install the service or will uninstall the service from the computers whenever the computers check-in.

Configuring Cloud Sync

The following configuration options are available:

Login Settings

Select the following settings:

- User must provide an email address with the following domain(s) – specify the domains separated by a comma. For example, you can specify @yourcompany.com where [yourcompany.com] is the domain for your organization.
- Preferred cloud drives – select one of the following cloud drive service providers:
 - > Google Drive
 - > Dropbox
 - > Microsoft OneDrive

Drive Settings

- Folder Name – select one of the following options:
 - > User Email – the email of the user will be the name of the folder.
 - > Custom – specify a custom name. For example, you can specify *Cloud Sync*.



- Reserve Drive Size – specify the cache size for temporarily saved files. Select from 1 to 50 GB.



Cloud Sync will appear as [Cloud Sync Name] or [user]@[domain.com] under Favorites (for Windows 7 or higher).

Users can drag and drop files from any location on the computer to *Favorites > [Cloud Sync Name]*.

Status of Files on Cloud Sync

The following icons represent the status of files on Cloud Sync:

When a file is shown on Google Drive or Dropbox, the following icon is displayed:



When a file is modified, but not synced to the cloud (Google Drive or Dropbox), the following icon is displayed:



When a file is synced to the cloud (Google Drive or Dropbox), the following icon is displayed:





Usage Stats Service

Manages software assets and reports on license compliance, application usage and computer usage.

To add Usage Stats to the Policy, go to *Add Policy > Deep Freeze Windows > Usage Stats* > select *Enable (Install)*. Selecting this option installs Usage Stats on all computers using this Policy.



Selecting *Enable (Install)* installs the Usage Stats service on the computers whenever the computers check-in. The computers check-in based on the heartbeat specified in [Cloud Agent Settings](#).

Selecting *Disable* uninstalls Usage Stats service from the computers whenever the computers check-in or goes into Maintenance mode.

Multiple reports are available for Usage Stats. For more information on the reports, go to [Usage Stats](#).



Incident Reporting Service

Incident Reporting Service allows students to anonymously report bullying incidents on computers managed with Deep Freeze Cloud.

To add Incident Reporting to the Policy, go to *Add Policy > Deep Freeze Windows > Incident Reporting > select Enable (install and inherit settings from Faronics Default policy) or Enable (Install and use below settings)*. Selecting this option installs Incident Reporting on all computers using this Policy.



Selecting *Enable (install and inherit settings from Faronics Default policy)* or *Enable (Install and use below settings)* installs Incident Reporting on the computers whenever the computers check-in. The computers check-in based on the heartbeat specified in [Cloud Agent Settings](#).

- *Enable (install and inherit settings from Faronics Default policy)* – installs the service and inherits settings from the Faronics Default policy. Selecting this option saves time in configuring all the policy settings. Selecting this option makes the settings for the current policy read-only.
- *Enable (Install and use below settings)* – installs the service and uses custom settings. Selecting this option will allow you to customize the settings for this service in the current policy.
- *Disable* will not install the service or will uninstall the service from the computers whenever the computers check-in.

Configuring Incident Reporting

The following configuration options are available:

- **Anonymous Reporting** – select this option to ensure all Incident Reporting reports are anonymous. User name or computer name will not be collected.
- **Non-anonymous Reporting (Collects User Name and Computer Name along with the incident)** – select this option to collect the user name and computer name.
 - > **Also allow anonymous reporting** – select this option to optionally allow anonymous reporting.

Display Incident Reporting Form

The Incident Reporting Form can be displayed in the following three ways:

- **Open the form as user logs in** – select this option to display the form immediately when the user logs in.
- **Display the form x minutes after the user logs in** – specify the value for x. The maximum value is 60 minutes.

The user at the computers can still launch the Incident Reporting pop-up from the system tray.

Incident Reporting Form Content

- **Add Content** – add a description that will pop-up on the computer.



- Add Help Text – add additional description like a help text or a warning.

Notification Settings

- Email submitted forms to – specify the email address for the user who will receive Incident Reporting reports. You can specify multiple email addresses by adding a comma between the addresses.

To view the Incidents Summary for Incident Reporting Service, go to [Incident Reporting](#).



Ticketing Service

Ticketing Service helps efficiently manage interactions on a support or service case.

To add Ticketing to the Policy, go to *Add Policy > Deep Freeze Windows > Ticketing > select Enable (install and inherit settings from Faronics Default policy) or Enable (Install and use below settings)*. Selecting this option installs Ticketing on all computers using this Policy.



Selecting *Enable (install and inherit settings from Faronics Default policy)* or *Enable (Install and use below settings)* installs Ticketing on the computers whenever the computers check-in. The computers check-in based on the heartbeat specified in [Cloud Agent Settings](#).

- *Enable (install and inherit settings from Faronics Default policy)* – installs the service and inherits settings from the Faronics Default policy. Selecting this option saves time in configuring all the policy settings. Selecting this option makes the settings for the current policy read-only.
- *Enable (Install and use below settings)* – installs the service and uses custom settings. Selecting this option will allow you to customize the settings for this service in the current policy.
- *Disable* will not install the service or will uninstall the service from the computers whenever the computers check-in.

Ticketing Form Content

Complete the following to customize the template of the Ticket Form:

- **Title** – Assign a title to the ticket.
- **Content** – Use this space to create a message encouraging your audience to provide details of the issues they are dealing with if preferred.

If not customizing a message, the default message will be *Please provide details about the problem you're facing with your computer below*.

- **Help Text** – Use this space to provide more information to your users. As an example, you can inform the users the process involved after they have submitted a ticket, how long it will take to respond (if possible), and other details as needed.

If not customizing a message, the default message will be *This will be sent to your IT Admin. You will also receive a confirmation email with a ticket ID once the ticket has been submitted successfully*.

Click *Preview* to do a quick review of your ticket form template.

To view the submitted tickets, go to [Tickets](#).



Power Save Service

Power Save Service provides non-disruptive PC power management by analyzing CPU, disk, keyboard, mouse, and network activity, as well as application status, before taking computer power management actions.

To add Power Save to the Policy, go to *Add Policy > Deep Freeze Windows > Power Save > select Enable (install and inherit settings from Faronics Default policy) or Enable (Install and use below settings)*. Selecting this option installs Power Save on all computers using this Policy.



Selecting *Enable (install and inherit settings from Faronics Default policy)* or *Enable (Install and use below settings)* installs Power Save on the computers whenever the computers check-in. The computers check-in based on the heartbeat specified in [Cloud Agent Settings](#).

- *Enable (install and inherit settings from Faronics Default policy)* – installs the service and inherits settings from the Faronics Default policy. Selecting this option saves time in configuring all the policy settings. Selecting this option makes the settings for the current policy read-only.
- *Enable (Install and use below settings)* – installs the service and uses custom settings. Selecting this option will allow you to customize the settings for this service in the current policy.
- *Disable* will not install the service or will uninstall the service from the computers whenever the computers check-in.

You can configure settings for Power Save through various tabs. The configuration settings for Power Save through various tabs are explained further in this chapter.

- [Audit Mode](#)
- [Power Schedule Tab](#)
- [Critical Apps Tab](#)
- [Windows Options Tab](#)
- [Hardware Settings Tab](#)
- [User Experience Tab](#)
- [Administration Settings Tab](#)
- [Energy Cost Tab](#)



Audit Mode

Run in Audit Mode only – select this option to run Power Save in Audit Only Mode. In the Audit Only Mode, the Power Save actions are disabled. However, Power Save will record the events on the computer. The events recorded are startup time, shutdown time, monitor on time, monitor standby time, computer standby time, computer hibernate time, and computer sleep time. The recorded events can be analyzed using Power Save reports.

Power Schedule Tab

Power Schedule and Power Events are two main components that are used to define how Power Save manages power on the computer.

Power Schedule

A Power Schedule can consist of one or more Power Events.

Power Event

A Power Event consists of:

- Inactivity Timeout Actions – defines whether Power Save must turn off monitors, hard disks and shut down the computer after a pre-defined interval.
- Inactivity Definitions – defines whether Power Save must manage power on the computer when the hard disk, CPU or network activities are below the specified levels.

Complete the following steps to add a Power Event:

1. Click *Add*.
2. Specify a name for the *Power Event*.
3. Specify the values for the following fields:
 - > Start Time – select the time when the selected Power Policy has to be applied.
 - > Days – select the days to apply the Power Policy.
 - > Wake up client for this policy to take effect – select the checkbox if you want Power Save to wake up the client to apply the power policy. This will ensure that Power Save wakes up the computers on Standby or Hibernate mode before applying the new Power Policy. If this option is not selected, the new Power Policy will not be applied on computers that are on Standby or Hibernate mode.
4. Select the action to be taken by Power Save:
 - > Shutdown – Power Save shuts down the computer.
 - > Dynamic Configuration – select the configuration from the slider. You can either set the configuration towards Increased Power Savings or Low User Disruption.



- > Advanced Settings – select if you want to begin power management On Computer Startup or After first keyboard/mouse activity. Configure the steps for Advanced Settings in the next steps.

5. Advanced Settings: Select the required options for the following fields:

Option	Description	When plugged in	Description	When running on Batteries	Description
Turn off monitor after	Select the checkbox to turn off the monitor after the specified time interval.	x minutes/seconds	Select the numeric value and specify if it is minutes or seconds when plugged in.	x minutes/seconds	Select the numeric value and specify if it is minutes or seconds when the computer is running on batteries.
Turn off hard disk after	Select the checkbox to turn off the hard disk after the specified time interval.	x minutes/seconds	Select the numeric value and specify if it is minutes or seconds when plugged in.	x minutes/seconds	Select the numeric value and specify if it is minutes or seconds when the computer is running on batteries.
Shutdown/Standby/Hibernate PC after	Select the checkbox to Shutdown/Standby/Hibernate the computer after the specified time interval.	x minutes/seconds	Select the numeric value and specify if it is minutes or seconds when plugged in.	x minutes/seconds	Select the numeric value and specify if it is minutes or seconds when the computer is running on batteries.
Shutdown if action is not supported	Select the checkbox to shutdown the computer if Standby or Hibernate actions are not supported.				
Manage power only after first keyboard/mouse activity	Select the checkbox to manage power only after the first keyboard or mouse activity.				

6. Additional Inactivity Definitions: Select the required options for the following fields for the Additional Inactivity Definitions pane:



Option	Description	When plugged in	Description	When running on Batteries	Description	Sample every
Disk activity is less than	Select the checkbox to manage power when the disk activity is less than the specified value.	x percent	Select the value in percent.	x percentage	Select the value in percent.	Select the duration for sampling the activity to check if it is less than the selected value.
For example, if the % is set to 50 and sample every is set to 10 seconds, the program will check for disk utilization every 10 seconds to determine if the utilization is below 50%.						
CPU activity is less than	Select the checkbox to manage power when the CPU activity is less than the specified value.	x percent	Select the value in percent.	x percentage	Select the value in percent.	Select the duration for sampling the activity to check if it is less than the selected value.
For example, if the % is set to 25 and sample every is set to 10 seconds, the program will check for CPU activity every 10 seconds to determine if the utilization is below 25%.						
Network activity is less than	Select the checkbox to manage power when the network activity is less than the specified value.	x percent	Select the value in percent.	x percentage	Select the value in percent.	Select the duration for sampling the activity to check if it is less than the selected value.
For example, if the % is set to 25 and sample every is set to 10 seconds, the program will check for Network activity every 10 seconds to determine if the utilization is below 25%.						
Do not manage power if the following applications are running	Select the checkbox to stop managing power when the selected applications are running.					



Option	Description	When plugged in	Description	When running on Batteries	Description	Sample every
Continue to manage power only for monitors.	Select the checkbox to continue to manage power for monitors even if selected applications above are running.					

7. Click OK. The Power Event is added to the Power Schedule.

Critical Apps Tab

The administrator can now define the behavior of the Power Save service when critical applications are running on the computer.

Complete the following steps to set the behavior of Power Save when critical applications are running:

1. Select the *Do not manage power if the following applications are running* checkbox.
2. Click the *Add* button to select the application. Browse to select the application.
3. Click OK.

If the selected application is running, Power Save will not manage power on the computer.

Complete the following steps to set the behavior of Power Save when non-critical applications are running:

1. Select the *Ignore all activity contributed by the following checked applications* checkbox.
2. Click the *Add* button to select the application. Browse to select the application.
3. Click OK.

Power Save will ignore all activity contributed by the selected application.

Windows Options Tab

- **Override Windows Power Options** – select this option to turn off power management options in Windows. This allows Power Save to take action on the computer without interference by the operating system's power saving options.
- **Resume From Standby Password Challenge** – select this option to require users to enter their Windows password when the computer resumes from standby or hibernate.
- **Log off Before Powering Down Computer** – select this option to logoff the user before placing the computer in standby and hibernate mode.



Hardware Settings Tab

Configure the following settings:

Wake by Device

Select the devices that are allowed to wake the computer.

- Keyboard
- Mouse
- Network Interface Card (NIC)



At least one device must be enabled to ensure the computer can be woken up.

Configure the following optional settings:

- Do not manage power if the computer is on a wireless network connection – select this option if the computer is on a wireless connection.

User Experience Tab

Configure the following settings:

User Notification

Complete the following steps to set the User Notification:

1. Select the *Notify user of Power Save actions* checkbox. Select the *seconds in advance* from the spin box.
2. Enter a message in the *Notification Message* field.



The duration of the User Notification setting must always be set lower than the lowest Inactivity setting across all Power Policies.

Stealth Mode

Stealth mode hides Power Save on the computer. Select one or more options to enable Stealth Mode:

- Hide icon in system tray – hides Power Save icon in the system tray.

User Input

- Allow users to temporarily defer computer power management for x hours – select this option and select the hours. Power Save will not save power on the computer for x hours.



- Allow users to schedule a local wake up and defer power management to for up to x hours – select this option and select the number of hours from the drop-down for the value of x. The Local Wake up feature enables users to schedule a wake up on their computers locally when it is in *Standby* or *Hibernate* mode. A network connection is not required for the Local Wake up to take effect.

Administration Settings Tab

Configure the following settings:

Password Protection

Enable client password – set a password to avoid uninstalling of the Power Save service.

Save Open Documents

The Save Open Documents feature ensures that Power Save saves any open document to a pre-defined location on the computer. The following types of files can be saved:

- Word documents
- Excel spreadsheets
- Power Point presentations
- Outlook and Lotus Notes – E-Mail drafts, to-do list, meeting planner and calendar
- Notepad files
- WordPad files

Complete the following options to configure the settings:

1. Select *Save a copy of any open document(s) in the following location* checkbox. The default location is *My Documents\Files Saved by Power Save* for the particular user profile logged on.
2. Change the path as required. (You can click *Restore Default* to restore it later if required.)
3. Select *Notify user if a copy of the document was saved* checkbox to notify the user.



Ensure that the currently logged in user has rights to the folder where Power Save saves open documents.

Energy Cost Tab

Define the Energy Cost to calculate savings by Power Save. Complete the following steps to Configure Energy Cost:

1. Click *Add*.
2. Configure the following:
 - > Cost per kWh – specify the cost of energy per kilowatt hour.



- > Start Time – select the time when the energy savings will be calculated.
 - > Days – select the day when the energy cost will be calculated.
3. Click *OK*.



Imaging Service

Create images of computers and deploy the images across multiple computers in the network.

To enable *Imaging Policy*, go to *Add New Windows Policy > Deep Freeze Windows > Imaging > select Enable*.

Selecting this option enables the Imaging function on all computers using this Policy.



Selecting *Enable* installs the Imaging service on the computers whenever the computers check-in.

Selecting *Disable* uninstalls the Imaging service from the computers whenever the computers check-in or goes into Maintenance mode.



Remote Connect Service

Access connected computers across dispersed networks via Deep Freeze Cloud.

To add Remote Connect to the Policy, go to *Add Policy > Deep Freeze Windows > Remote Connect > select Enable (install and inherit settings from Faronics Default policy) or Enable (Install and use below settings)*.

Selecting this option enables the Remote Connect function on all computers using this Policy.



To enable communication between the computer and Deep Freeze Cloud Services through the firewall, ensure that outbound traffic is permitted on specified ports, and access is allowed on certain domains and IP addresses on both the console and client computer. Refer to [Authorized Domains and Ports](#).



Selecting *Enable (install and inherit settings from Faronics Default policy)* or *Enable (Install and use below settings)* installs Remote Connect on the computers whenever the computers check-in. The computers check-in based on the heartbeat specified in [Cloud Agent Settings](#).

- *Enable (install and inherit settings from Faronics Default policy)* – installs the service and inherits settings from the Faronics Default policy. Selecting this option saves time in configuring all the policy settings. Selecting this option makes the settings for the current policy read-only.
- *Enable (Install and use below settings)* – installs the service and uses custom settings. Selecting this option will allow you to customize the settings for this service in the current policy.
- *Disable* will not install the service or will uninstall the service from the computers whenever the computers check-in.

When the Remote Connect policy is enabled, the *Ask for User Permission to Remotely Access Computer* option will be enabled by default. One option (RDP or VNC) must be selected to be able to save the policy.

Once the Remote Connect service is installed, navigate to the Computers page and select a computer to remotely connect.

RDP

Select the *Enable RDP Connection* checkbox to allow remote access to the computer (including apps, files, network resources). The *Ask for User Permission to Remotely Access Computer* option will be enabled by default. This option will notify the users whenever an IT Admin tries to remote into the user's computer.



Active user session will be locked out once a remote connection is established.



VNC

VNC allows you to remotely access computers and assist end users using VNC over Internet.

Select the *Enable VNC Connection* checkbox to allow remote access to the computer, and assign a VNC password.

The *Ask for User Permission to Remotely Access Computer* option will be enabled by default. This option will notify the users whenever an IT Admin tries to remote into the user's computer.



Requesting user permission is recommended to avoid disrupting active users.

Enabling VNC connection will install UltraVNC on the computer once the policy is applied to a new computer.

If UltraVNC has been previously installed or already enabled in the Software Updater policy, it will be uninstalled and replaced with the password-protected version as per policy.

For Policies with Deep Freeze and/or Anti-Executable enabled and Remote Connect already installed, enabling VNC in the Remote Connect Policy or applying a new policy on a computer with VNC disabled requires running a maintenance period to install the VNC client.



Disabling VNC will not uninstall VNC from the computer.



User permission will be requested during remote connection if someone is logged into the computer.



Anti-Virus Service

Anti-Virus Service provides protection from security threats without slowing down computers due to slow scan times and large footprints. Anti-Virus Service gives you powerful anti-virus, anti-rootkit, firewall and anti-spyware software in-one that protects you against today's highly complex malware threats.



To enable communication between the computer and Deep Freeze Cloud Services through the firewall, ensure that outbound traffic is permitted on specified ports, and access is allowed on certain domains and IP addresses on both the console and client computer. Refer to [Authorized Domains and Ports](#).

To add Anti-Virus to the Policy, go to *Add Policy > Deep Freeze Windows > Anti-Virus > select Enable (install and inherit settings from Faronics Default policy) or Enable (Install and use below settings)*. Selecting this option installs Anti-Virus on all computers using this Policy.



Selecting *Enable (install and inherit settings from Faronics Default policy)* or *Enable (Install and use below settings)* installs Anti-Virus on the computers whenever the computers check-in. The computers check-in based on the heartbeat specified in [Cloud Agent Settings](#).

- **Enable (install and inherit settings from Faronics Default policy)** – installs the service and inherits settings from the Faronics Default policy. Selecting this option saves time in configuring all the policy settings. Selecting this option makes the settings for the current policy read-only.
- **Enable (Install and use below settings)** – installs the service and uses custom settings. Selecting this option will allow you to customize the settings for this service in the current policy.
- **Disable** will not install the service or will uninstall the service from the computers whenever the computers check-in.

Configuring Anti-Virus

You can configure settings for Anti-Virus through various tabs. The configuration settings for Anti-Virus through various tabs are explained further in this chapter.

- [Security Options Tab](#)
- [Computer Settings Tab](#)
- [Scan Settings Tab](#)
- [Firewall Protection Tab](#)



Security Options Tab

Configure the following settings:

- Enable Active Protection – select this option to enable real-time protection. Active Protection is the real-time scanning by Faronics Anti-Virus in the background without any impact on system performance. If there is a risk of real-time virus infection from the Internet, select this option.
- Allow users to switch off Active Protection – select this option to allow users to switch off Active Protection. If users install or use software that might be mistaken from a virus (for example, running advanced Macros in Microsoft Office or complex batch files), select this option.
- Show Active Protection alert – select this option to display an alert if a threat is detected during Active Protection. Do not select this checkbox if you do not want an alert to be displayed.
- Enable Firewall Protection – select the checkbox to enable Firewall Protection. Configure additional options in the [Firewall Protection Tab](#).

Computer Settings Tab

Configure the following settings:

User Actions

- Show taskbar icon – select the checkbox to display Faronics Anti-Virus icon on the taskbar at the computer(s). If this checkbox is not selected, Faronics Anti-Virus will be hidden to the user.
- Allow manual scanning – select the checkbox to allow users to manually initiate Faronics Anti-Virus scanning at the computer(s).
- Allow user to take action on scan results – select the checkbox to allow the computer user to take action on the scan results.
- Allow user to abort a scan initiated locally- select the checkbox to allow users to abort the scan initiated locally at the computer.

Windows Security Center

- Integrate into Windows Security Center – select the checkbox to integrate Faronics Anti-Virus into the Windows Security Center. Windows Security Center will notify you via the System Tray if Faronics Anti-Virus is active or inactive.

Anti-Virus Cache Server

- Use Anti-Virus Cache Server – select the checkbox if you have set up an Anti-Virus Cache Server on your network that downloads and distributes virus definitions to all computers. For more information, refer to [Anti-Virus Cache Server](#).
- Server IP – specify the IP address of the Anti-Virus Cache Server.
- Server Name – specify the name of the Anti-Virus Cache Server.
- Port – specify the port of the Anti-Virus Cache Server.
- Connect to Web Server if there is no communication with the Anti-Virus Cache Server in the last x hours – select this option if the managed computers must connect to the



Faronics Web Server through the Internet if the Anti-Virus Cache Server is not accessible for some reason.

Log Actions

- Log Level- select the logging level. Select *None* for no logging. Select *Error* to log the error message. Select *Trace* for trace. Select *Verbose* for detailed logging.
- Number of rolling log files – specify the number of logging files. The logging information is stored in the files serially. For example, if there are 3 files A,B and C, Faronics Anti-Virus first writes the error logs to file A. Once file A is full, it starts writing to file B and finally file C. Once file C is full, the data in file A is erased and new logging data is written to it.
- File size up to- Select the size of each file in MB.

Scan Settings Tab

Configure the following settings:

Cleanup Actions

Select the default actions for infected files:

- Clean/Quarantine – when a threat is detected, attempt to disinfect the file and quarantine if unsuccessful. If the file could not be disinfecting, it will be quarantined and will not be deleted.
- Clean/Delete – when a threat is detected, attempt to disinfect the file and delete if unsuccessful. If the file could not be disinfecting, it will be deleted from the computer.
- Delete items from quarantine that are older than – specify the number of days to retain items in quarantine. The default is 3 days.

Scan Schedule

- Quick Scan – Click the *Edit* icon for Quick Scan. Configure the following options and click *Update*.
 - > Enable Quick Scan – select the checkbox to enable Quick Scan.
 - > Start – specify the start time.
 - > Stop – specify the end time. The maximum duration between the Start time and Stop time is 23.59 hours. The scan ends if all the files are scanned before the Stop time. If the scan is not complete before the Stop time, it is aborted at the Stop time. Alternatively, select *When scan is complete* to ensure that scan is completed.
 - > Days – select the days when the scheduled Quick Scan will take place.
- Deep Scan – Click the *Edit* icon for Deep Scan. Configure the following options and click *Update*.
 - > Enable Deep scan – select the checkbox to enable Deep Scan.
 - > Start – specify the start time.
 - > Stop – specify the end time. The maximum duration between the Start time and Stop time is 23.59 hours. The scan ends if all the files are scanned before the Stop time. If the scan is not complete before the Stop time, it is aborted at the Stop time. Alternatively, select *When scan is complete* to ensure that scan is completed.
 - > Days – select the days when the scheduled Deep Scan will take place.



Scan Options

- Randomize scheduled scan start times by x minutes – specify the number of minutes. The scheduled scan start time is randomized to reduce the impact on network traffic. This might impact the network traffic if the scan for multiple systems start at the same time.

Missed scan options at start-up: Select one of the following options on how a scan will be performed if the computer was not *ON* during a scheduled scan:

- Do not perform quick scan – select this option if you do not want to perform quick scan on startup.
- Perform quick scan approximately x minutes after start-up – specify the number of minutes after start-up when Faronics Anti-Virus must perform a quick scan.
- Prompt user to perform quick scan – select the option to prompt user to perform a quick scan.

Scan Exceptions

Folders or files that are known to be safe and free of infections can be added to the Scan Exceptions. Files added to the Scan Exceptions will always be scanned by Faronics Anti-Virus. However, Faronics Anti-Virus will never report the files as malicious or infected. This feature is useful since files and folders that are known to be safe by the Administrator will not be reported as malicious.

1. Click *Add Exception*.
2. In the *Add* dialog, select *File by full path*, or *Entire folder*. Click *Browse* to select the file or folder and click *OK*.
3. The *File by full path* is added to the Scan Exceptions.

Advanced Options

For each type of scan, select the following options (some options may be grayed out depending on the type of scan):

- Enable rootkit detection – detects if the computer is infected with a rootkit.
- Scan inside of archives – scans the contents of a zip file. Select for the scan to include archive files, such as .RAR and .ZIP files. When a .RAR/.ZIP file is found to contain an infected file, the .RAR/.ZIP file will be quarantined. Specify the *File Size Limit*.
- Exclude removable drives (e.g USB) – excludes the removable drives from the scan process. Any external hard disks, USB drives etc will not be scanned.
- Scan Registry – scans the registry for threats.
- Scan Running Processes – scans all running processes on the computers.
- Restore Defaults – click *Restore Defaults* if you want to restore all the default settings for the Advanced Options.

USB Devices

- Scan USB drives upon insertion – select this option to scan USB drives upon insertion and select one of the following options:
- Interrupt active scan for USB scan – select this option to interrupt an active scan to scan the USB drive when it is inserted. Once the active scan is interrupted, it will not resume automatically and must be restarted manually.



- Do not perform USB scan if another scan is already in progress – select this option to ensure that an active scan is not interrupted when a USB drive is inserted. The USB drive must be manually scanned once the active scan is complete.
- Suppress USB scan in progress dialogue – select this option to hide indications that Anti-Virus is scanning USB drives when they are inserted; no Anti-Virus interface will open, and the system tray icon will not display tooltips indicating a scan in progress. Users will be notified at the end of a scan if a virus was found, but if no viruses were detected there will be no notification that the scan occurred.

Note that if the *Scan USB drives upon insertion* option is not selected, this option is ignored.

Firewall Protection Tab

Configure the following settings:

Firewall Protection Settings

- Enable Firewall Protection – select the checkbox to enable Firewall Protection. Firewall Protection prevents hackers or malicious software from gaining access to your computer through the Internet or the network.
- Allow users to disable firewall – select this option to allow users to disable the firewall at the computer.
- Enable Firewall Logging – select this option to log all actions related to the Firewall.

Firewall Rules

Configure settings for Program Rules, Network Rules, Advanced Rule, Intrusion Rules, and Trusted Zones.

Program Rules

Program Rules define the action taken by the firewall on the network activity to and from an application. Program Rules have priority over the default rules. Default rules can be edited but cannot be deleted.

Click *Add* to add a new Program Rule. Specify or select the options and click *OK*. The following parameters are displayed:

- Name – name of the rule.
- Program – name of the program, including full path and extension.
- Trusted Zone Inbound – the action to be taken for inbound communication to the program in a Trusted Zone (Allow, Block or Prompt).
- Trusted Zone Outbound – the action to be taken for outbound communication from the program in a Trusted Zone (Allow or Block).
- Untrusted Zone Inbound – the action to be taken for inbound communication to the program in an Untrusted Zone (Allow or Block).
- Untrusted Zone Outbound – the action to be taken for inbound communication from the program in an Untrusted Zone (Allow or Block).

Click the *Edit* icon to modify or click the *Delete* icon to delete.



Network Rules

Network Rules define the action taken by the firewall on the network activity. Network Rules can be edited but cannot be deleted. Select the Network Rules for the following:

Name	Description	Trusted Zone Inbound	Trusted Zone Outbound	Untrusted Zone Inbound	Untrusted Zone Outbound
IGMP	Internet Group Management Protocol	Select Allow or Block	Select Allow or Block	Select Allow or Block	Select Allow or Block
Ping	Ping and Tracert	Select Allow or Block	Select Allow or Block	Select Allow or Block	Select Allow or Block
OtherIcmp	Other ICMP packets	Select Allow or Block	Select Allow or Block	Select Allow or Block	Select Allow or Block
DHCP	Dynamic Host Configuration Protocol	Select Allow or Block	Select Allow or Block	Select Allow or Block	Select Allow or Block
DNS	Domain Name System	Select Allow or Block	Select Allow or Block	Select Allow or Block	Select Allow or Block
VPN	Virtual Private Network	Select Allow or Block	Select Allow or Block	Select Allow or Block	Select Allow or Block
LDAP	Lightweight Directory Access Protocol	Select Allow or Block	Select Allow or Block	Select Allow or Block	Select Allow or Block
Kerberos	Kerberos Protocols	Select Allow or Block	Select Allow or Block	Select Allow or Block	Select Allow or Block
NETBIOS	Microsoft File and Printer Sharing	Select Allow or Block	Select Allow or Block	Select Allow or Block	Select Allow or Block

Advanced Rules

Advanced Rules define the action taken by the firewall for the specified application, port or protocol. This may include a single or a combination of protocol, local or remote ports, and direction of traffic. You can add, edit or delete an advanced rule.

Advanced Rules are processed in the order in which they are listed. Any user-defined advanced rules will take precedence over the pre-defined Advanced Rules.



Click *Add* to add a new Advanced Rule. Specify or select the options and click *OK*. The following parameters are displayed in the Advanced Rules pane:

- Name – name of the rule.
- Program – name of the program and path.
- Action – the action taken by the Firewall for communication from the specified application, port or protocol (Allow, Block or Prompt).
- Direction – the direction of communication (Both, In or Out).
- Protocol – the name of the protocol.
- Local Port – details of the local port.
- Remote Port – details of the remote port.

Click the *Edit* icon to modify or click the *Delete* icon to delete.

Trusted Zones

Trusted Zones specify computers, networks and IP addresses that are trusted. Network traffic from and to the Trusted Zones are not blocked. Trusted Zones and Internet (Non-Trusted) Zones can be treated differently by Program and Network Rules.

Click *Add* to add a new Trusted Zone. Specify or select the options and click *OK*. The following parameters are displayed:

- Name – name of the Trusted Zone.
- Description – description of the Trusted Zone.
- Type – type of the Trusted Zone (IP Address or Network).

Click the *Edit* icon to modify or click the *Delete* icon to delete.

Advanced Firewall Protection Settings

- Enable Process protection – select this option to enable process protection. This feature is used to set the action for unknown code injectors and to add your own allowed code injectors based on the settings in the *Process Protection* pane.
- Enable boot time protection – select this option to enable boot time protection. Boot time protection protects your computer when it starts, blocking traffic from occurring before Windows has a chance to open.



Deep Freeze Mac Service

Deep Freeze Mac Service can only be installed on macOS computers. Once Deep Freeze is installed on a computer, any changes made to the computer—regardless of whether they are accidental or malicious—are never permanent.



Only the Deep Freeze Mac Service can be installed on Mac computers. All other services cannot be installed on Mac computers.

To add Deep Freeze Mac to the Policy, go to *Add Policy > Deep Freeze Mac > select Enable (install and inherit settings from Faronics Default policy) or Enable (Install and use below settings)*. Selecting this option installs Deep Freeze Mac on all computers using this Policy.



Selecting *Enable (install and inherit settings from Faronics Default policy) or Enable (Install and use below settings)* installs Deep Freeze Mac on the computers whenever the computers check-in. The computers check-in based on the heartbeat specified in [Cloud Agent Settings](#).

- *Enable (install and inherit settings from Faronics Default policy)* – installs the service and inherits settings from the Faronics Default policy. Selecting this option saves time in configuring all the policy settings. Selecting this option makes the settings for the current policy read-only.
- *Enable (Install and use below settings)* – installs the service and uses custom settings. Selecting this option will allow you to customize the settings for this service in the current policy.
- *Disable* will not install the service or will uninstall the service from the computers whenever the computers check-in.

Deep Freeze Mac (HFS+)

Deep Freeze Mac (HFS+) is compatible with versions of macOS starting from OS X Mavericks 10.9 up to macOS High Sierra 10.13 with HFS+ formatted drive.

You can configure settings for Deep Freeze through various tabs. The configuration settings for Deep Freeze through various tabs are explained further in this chapter.



- [User & Drives Tab](#)
- [Maintenance Tab](#)
- [Advanced Options Tab](#)



Deep Freeze protects the computers that are set to boot from the hard drive. Deep Freeze cannot protect the computers that are set to boot from an external drive (USB, FireWire or Thunderbolt) or from a hard drive where Deep Freeze is not installed.

User & Drives Tab

The User & Drives tab is used to provides the following options:

User

Create a user account to manage Deep Freeze locally on your Mac. Only the users added below are authorized to make changes locally.

- User name – enter the user name.
- Password – enter the password.
- Add User – click the *Add User* button after entering the user name and password.
- Allow users to change Local Policy – select this option to allow users to modify the settings locally on the computer. If this option is not selected, users cannot modify settings locally and Deep Freeze Mac will be managed only from Deep Freeze Cloud.



If you do not select the option *Allow users to change Local Policy*, you will not be able to manage Deep Freeze locally on the Mac computers. In such a scenario, if you lose connectivity to the network or the Internet, you can Freeze or Thaw Mac computers using the following command line options:

```
DFXPSWD=password deepfreeze -u username -p bootThawed  
--force
```

```
DFXPSWD=password deepfreeze -u username -p bootFrozen  
--force
```

Drives

- Specify the drives to be Thawed on your Mac. Enter the name of the drive and click *Add Drive*.

Maintenance Tab

The Maintenance tab is used to schedule a Maintenance Period when the computer will be automatically Thawed to allow Apple Software Updates to be permanently applied. The computer must be Frozen for the Maintenance schedule to start.

To create multiple individually named Maintenance Schedules, complete the following steps:

1. On the Maintenance Tab, click *Add*.
2. The Add Schedule dialog is displayed. Specify or select the following:
 - > Name – the default is Schedule 1. You can modify the name or leave it as it is.



- > Days – select one or more days by clicking Mon to Sun.
- > Start – select the start time.
- > End – select the end time.
- > Select *Install Apple Software Updates* to install any available *Apple Software Updates*.
- > Run script – select this option and specify the name of the script.



Scripts must be present at */Library/Application Support/Faronics/Deep Freeze/Scripts* on all computers. You can copy the script files manually or use a remote access tool to copy the scripts to all computers.

- > Select *Lock Out User* to prevent a user from accessing the computer during the Maintenance Period.
- > Select *Shutdown After Maintenance* to shut the computer down after the Maintenance Period is complete.
- > Select *Show message x minutes before maintenance starts* to provide a message to users warning them that the computer will be taken over at a specified time, and enter the warning time in the field provided. Use the text box to enter a custom message for the user, explaining that the Maintenance Schedule will take place at a specified time; by inserting %d as a variable into the message, Deep Freeze will automatically display the number of minutes until the Maintenance Period begins. (Again, %d is a variable corresponding to the number of minutes between the current time and the time that scheduled Maintenance will begin.)



The minimum time allowed for a Maintenance Period is 10 minutes. There is a minimum 10-minute interval required between schedules. Ensure sufficient time for the maintenance activity to complete. Insufficient time will lead to the failure of the update.

3. To save any changes made, click *OK*.

Advanced Options Tab

The following configuration options are available:

User Experience

- To hide the Frozen icon, select the *Hide Frozen Icon* in menu bar checkbox.
- To hide the Thawed icon, select the *Hide Thawed Icon* in menu bar checkbox.
- To display Frozen partitions without a Deep Freeze icon, select the *Don't badge Frozen partitions* checkbox.
- To set the computers to restart when a user logs out, select the *Restart instead of Log Out* checkbox. (This option does not work if Fast User Switching is enabled.)



Apple Remote Desktop

- To display the computer status (Frozen or Thawed) remotely in Apple Remote Desktop, select the *Show Status in Apple Remote Desktop* checkbox and select the desired Information Field. The computer will now write Frozen or Thawed to the selected Information Field during boot time.
- To view this status information in Apple Remote Desktop, select *Edit > View Options* and select the matching Computer Info Field (1–4). Computers will now show their current status, and groups of computers can be sorted by this status column.

Existing Deep Freeze Mac Customers

- Convert Deep Freeze Mac On-Premise to Subscription licensing to manage from Cloud – select this option to manage the Deep Freeze Mac computers from Deep Freeze Cloud. This option will convert Deep Freeze Mac On-Premise license to a subscription license.



This option is only applicable to existing Deep Freeze Mac users who are on a Perpetual license. Once this option is selected, the Perpetual licenses are converted to Subscription licenses. Reverting to a perpetual license will require uninstalling Deep Freeze Mac Service (with subscription license) and re-installing Deep Freeze Mac (with perpetual license).

Deep Freeze Mac (APFS)

Deep Freeze Mac (APFS) is compatible with versions of macOS starting from macOS High Sierra 10.13.5 with APFS formatted drive.

You can configure settings for Deep Freeze through the following tabs:

- [Volumes Tab](#)
- [ThawSpace Tab](#)
- [Passwords Tab](#)
- [Maintenance Tab](#)
- [Advanced Options Tab](#)

Volumes Tab

The Volumes tab is used to specify the volumes to be Thawed on your Mac. Enter the name of the volume and click *Add*.

Installing Configuration Profiles

Starting with macOS Big Sur, Deep Freeze can no longer install the configuration profiles to disable automatic software updates or prevent Standard users from performing software updates.

Click *Download Required Configuration Profiles* to download the two configuration profiles:

- *Disable Notification.mobileconfig* – This file will disable software update notifications.
- *Disable Auto Update.mobileconfig* – This file will disable automatic software update installations, as well as allow software update installations to be performed only by admin users.



You can install these profiles using the following methods:

- Manually
- Apple Remote Desktop
- Mobile Device Management

Installing the Configuration Profiles Manually

1. Open *Disable Notification.mobileconfig* file by double-clicking it.
2. On macOS Monterey and earlier systems: Open *System Preferences* and click on the *Profiles*.
3. On macOS Ventura: Open *System Settings* > *Privacy & Security* > *Profiles*.
4. On the Profiles pane, click on the *Install...* button to install the configuration profile.
5. On the confirmation dialog, click *Install* button
6. Enter the administrator password to authenticate.

Repeat the steps for the other configuration profile.

Installing the Configuration Profiles Using Apple Remote Desktop

1. Copy the two configuration profiles to the target computers.
2. For each of the target computer:
 - > Select the computer from the All Computers list and control the computer.
 - > Navigate to the folder where the configuration profiles are copied to.
 - > Perform steps 1 to 5 of installing the configuration profiles manually.

Installing the Configuration Profiles Through Mobile Device Management

If you are using MDM to manage the computers, you can push the configuration profiles to the computers running macOS Big Sur.

ThawSpace Tab

The ThawSpace tab is used to allocate ThawSpaces where data is retained persistently on Frozen computers. Administrators can create a User ThawSpace for each User, or a Global ThawSpace that all users can share. The ThawSpace tab displays only the users that have ThawSpace.



Global and User ThawSpace names should not be modified. If a ThawSpace is renamed, Deep Freeze can no longer associate the ThawSpace to the volume.



It is strongly recommended not to delete Global and User ThawSpace volumes using a third-party tool. If a ThawSpace volume that has been deleted through a third-party tool is recreated even with the same name, Deep Freeze can no longer associate the ThawSpace to the volume.



Creating ThawSpaces

To add a Global ThawSpace, select *Global ThawSpace* in the ThawSpace Type and click *Add*.

To add a User ThawSpace, select *User ThawSpace* in the ThawSpace Type, specify the User name, and click *Add*.

Deleting ThawSpaces

To delete ThawSpaces, click the (X) icon at the end of the Global or User ThawSpace. Check the *I understand by enabling this option, everything within the existing ThawSpaces will be permanently deleted. There is no going back.* Click *OK*.



Deleting ThawSpaces will remove all existing data within the ThawSpace.

Passwords Tab

The Passwords tab allows administrators to manage the Deep Freeze passwords. There are a maximum of four passwords permitted.

Select the *Enable Deep Freeze Password* to enable users to log in to Deep Freeze using a Deep Freeze password.

To add a password, specify the *Description* and *Password*, then click *Add*.

To delete a password, click the (X) icon at the end of each password. Click *Yes* when prompted to confirm that you want to delete the password.

Select the *Allow users to change local policy* to allow users to modify the settings locally on the computer. If this option is not selected, users cannot modify settings locally and Deep Freeze Mac will be managed only from Deep Freeze Cloud.

Maintenance Tab

The Maintenance tab is used to schedule a Maintenance Period for computers.

Administrators can create, edit, delete, enable, and disable Maintenance Schedules through the Maintenance Tab.

To create multiple individually named Maintenance Schedules, complete the following steps:

1. On the Maintenance Tab, click *Add*.
2. The Add Schedule dialog is displayed. Specify or select the following:
 - > Name – the default is Schedule 1. You can modify the name or leave it as it is. The schedule name has to be unique.
 - > Days – select one or more days by clicking Mon to Sun.
 - > Start – select the start time.
 - > End – select the end time.



- > Select *Install Apple Software Updates* to install any available *Apple Software Updates*.



The *Install Apple Software Updates* option is disabled on Macs with Apple Silicon architecture. The updates can be performed using *System Preferences > Software Update*.

Maintenance schedules upgraded from Deep Freeze Mac 7.3 with this option enabled will be automatically disabled when run/executed.

- > Run script – select this option and specify the name of the script.



Scripts must have already been added through Deep Freeze Mac or the command line.

- > Select *Lock Out User* to prevent a user from accessing the computer during the Maintenance Period.
- > Select *Shutdown After Maintenance* to shut the computer down after the Maintenance Period is complete.
- > Select *Show message x minutes before maintenance starts* to provide a message to users warning them that the computer will be taken over at a specified time, and enter the warning time in the field provided. Use the text box to enter a custom message for the user, explaining that the Maintenance Schedule will take place at a specified time; by inserting %d as a variable into the message, Deep Freeze will automatically display the number of minutes until the Maintenance Period begins. (Again, %d is a variable corresponding to the number of minutes between the current time and the time that scheduled Maintenance will begin.)



The minimum time allowed for a Maintenance Period is 10 minutes. There is a minimum 10-minute interval required between schedules. Ensure sufficient time for the maintenance activity to complete. Insufficient time will lead to the failure of the update.

3. To save any changes made, click *OK*.

Advanced Options Tab

The following configuration options are available:

User Experience

- To hide the Frozen icon, select the *Hide Frozen Icon in menu bar* checkbox.
- To hide the Thawed icon, select the *Hide Thawed Icon in menu bar* checkbox.
- To set the computers to restart when a user logs out, select the *Restart instead of Log Out* checkbox. (This option does not work if Fast User Switching is enabled.)



Apple Remote Desktop

- To display the computer status (Frozen or Thawed) remotely in Apple Remote Desktop, select the *Show Status in Apple Remote Desktop* checkbox and select the desired Information Field. The computer will now write Frozen or Thawed to the selected Information Field during boot time.
- To view this status information in Apple Remote Desktop, select *Edit > View Options* and select the matching Computer Info Field (1–4). computers will now show their current status, and groups of computers can be sorted by this status column.

Existing Deep Freeze Mac Customers

- Convert Deep Freeze Mac On-Premise to Subscription licensing to manage from Cloud – select this option to manage the Deep Freeze Mac computers from Deep Freeze Cloud. This option will convert Deep Freeze Mac On-Premise license to a subscription license.



This option is only applicable to existing Deep Freeze Mac users who are on a Perpetual license. Once this option is selected, the Perpetual licenses are converted to Subscription licenses. Reverting to a perpetual license will require uninstalling Deep Freeze Mac Service (with subscription license) and re-installing Deep Freeze Mac (with perpetual license).



Software Updater Service (Mac)



This feature is only available for organizations using WebSocket.

To add Software Updater to the Policy, go to *Add Policy > Deep Freeze Mac > Software Updater > select Enable (Install)*.

Selecting this option installs Software Updater on all computers using this Policy.



Selecting *Enable (Install)* installs the Software Updater service on the computers whenever the computers check-in.

Selecting *Disable* uninstalls the Software Updater service from the computers whenever the computers check-in or goes into Maintenance mode.



Starting from macOS Ventura, Full Disk Access should be enabled for Software Updater to be able to install, uninstall, and update applications.

Complete the following steps to enable Full Disk Access:

1. Open *System Settings*, click *Privacy & Security*, then click *Full Disk Access*.
2. On *Finder*, navigate to [Macintosh HD]/Library/PrivilegedHelperTools.

Note that *Macintosh HD* is the default name of the startup volume on the computer after unpacking from the box. Replace *Macintosh HD* with the volume name on the computer.

3. Drag and drop *com.faronics.softwareupdaterd* into the *Full Disk Access* pane.
4. Enter the administrator password to authenticate.

Once authenticated, you should see *com.faronics* added to the list of applications with Full Disk Access.

After Software Updater Service has been enabled, supported applications can be installed, updated or uninstalled from the [Applications](#) page.



Anti-Virus Service (Mac)



This feature is only available for organizations using WebSocket.



Anti-Virus Service (Mac) is supported on macOS Big Sur and later versions.

To add Anti-Virus to the Policy, go to *Add Policy > Deep Freeze Mac > Anti-Virus > select Enable (Install)*.

Selecting this option installs Anti-Virus on all computers using this Policy.



Selecting *Enable (Install)* installs the Anti-Virus service on the computers whenever the computers check-in.

Selecting *Disable* uninstalls the Anti-Virus service from the computers whenever the computers check-in or goes into Maintenance mode.

Configuring Anti-Virus

You can configure settings for Anti-Virus through various tabs. The configuration settings for Anti-Virus through various tabs are explained further in this chapter.

- [Security Options Tab](#)
- [Computer Settings Tab](#)
- [Scan Settings Tab](#)

Security Options Tab

Configure the following settings:

- **Enable Active Protection** – select this option to enable real-time protection. Active Protection is the real-time scanning by Faronics Anti-Virus in the background without any impact on system performance. If there is a risk of real-time virus infection from the Internet, select this option.
- **Allow users to switch off Active Protection** – select this option to allow users to switch off Active Protection. If users install or use software that might be mistaken from a virus (for example, running advanced Macros in Microsoft Office or complex batch files), select this option.



- Show Active Protection alert – select this option to display an alert if a threat is detected during Active Protection. Do not select this checkbox if you do not want an alert to be displayed.

Computer Settings Tab

Configure the following settings:

User Actions

- Show taskbar icon – select the checkbox to display Faronics Anti-Virus icon on the taskbar at the computer(s). If this checkbox is not selected, Faronics Anti-Virus will be hidden to the user.
- Allow manual scanning – select the checkbox to allow users to manually initiate Faronics Anti-Virus scanning at the computer(s).
- Allow user to take action on scan results – select the checkbox to allow the computer user to take action on the scan results.
- Allow user to abort a scan initiated locally- select the checkbox to allow users to abort the scan initiated locally at the computer.

Scan Settings Tab

Configure the following settings:

Cleanup Actions

Select the default actions for infected files:

- Clean/Quarantine – when a threat is detected, attempt to disinfect the file and quarantine if unsuccessful. If the file could not be disinfecting, it will be quarantined and will not be deleted.
- Clean/Delete – when a threat is detected, attempt to disinfect the file and delete if unsuccessful. If the file could not be disinfecting, it will be deleted from the computer.
- Delete items from quarantine that are older than – specify the number of days to retain items in quarantine. The default is 3 days.

Scan Schedule

- Quick Scan – Click the *Edit* icon for Quick Scan. Configure the following options and click *Update*.
 - > Enable Quick Scan – select the checkbox to enable Quick Scan.
 - > Start – specify the start time.
 - > Stop – specify the end time. The maximum duration between the Start time and Stop time is 23.59 hours. The scan ends if all the files are scanned before the Stop time. If the scan is not complete before the Stop time, it is aborted at the Stop time. Alternatively, select *When scan is complete* to ensure that scan is completed.
 - > Days – select the days when the scheduled Quick Scan will take place.
- Deep Scan – Click the *Edit* icon for Deep Scan. Configure the following options and click *Update*.



- > Enable Deep scan – select the checkbox to enable Deep Scan.
- > Start – specify the start time.
- > Stop – specify the end time. The maximum duration between the Start time and Stop time is 23.59 hours. The scan ends if all the files are scanned before the Stop time. If the scan is not complete before the Stop time, it is aborted at the Stop time. Alternatively, select *When scan is complete* to ensure that scan is completed.
- > Days – select the days when the scheduled Deep Scan will take place.

Scan Options

- Randomize scheduled scan start times by x minutes – specify the number of minutes. The scheduled scan start time is randomized to reduce the impact on network traffic. This might impact the network traffic if the scan for multiple systems start at the same time.

Missed scan options at start-up: Select one of the following options on how a scan will be performed if the computer was not *ON* during a scheduled scan:

- Do not perform quick scan – select this option if you do not want to perform quick scan on startup.
- Perform quick scan approximately x minutes after start-up – specify the number of minutes after start-up when Faronics Anti-Virus must perform a quick scan.
- Prompt user to perform quick scan – select the option to prompt user to perform a quick scan.

Scan Exceptions

Folders or files that are known to be safe and free of infections can be added to the Scan Exceptions. Files added to the Scan Exceptions will always be scanned by Faronics Anti-Virus. However, Faronics Anti-Virus will never report the files as malicious or infected. This feature is useful since files and folders that are known to be safe by the Administrator will not be reported as malicious.

1. Click *Add Exception*.
2. In the *Add* dialog, select *File by full path*, or *Entire folder*. Click *Browse* to select the file or folder and click *OK*.
3. The *File by full path* is added to the Scan Exceptions.

Advanced Options

For each type of scan, select the following options (some options may be grayed out depending on the type of scan):

- Scan inside archives – scans the contents of a zip file. Select for the scan to include archive files, such as .RAR and .ZIP files. When a .RAR/.ZIP file is found to contain an infected file, the .RAR/.ZIP file will be quarantined. Specify the *File Size Limit*.
- Scan Running Processes – scans all running processes on the computers.



Reports

Generate detailed reports for all available Services across all the computers managed by Deep Freeze Cloud. Export reports to HTML, PDF, and CSV formats.

- [General Report](#)
- [Deep Freeze](#)
- [Data Igloo](#)
- [Anti-Executable](#)
- [Software Updater](#)
- [Usage Stats](#)
- [Incident Reporting](#)
- [Power Save](#)
- [Anti-Virus](#)

General Report

Installed Service Report

Shows the list of services installed on all computers with the following information:

- Computer Name
- Tags
- Policy
- Group
- Last Reported
- IP Address
- Services

Task Summary Report

Shows the list of tasks on the computers with the following information:

- Computer Name
- Tags
- Groups
- Task Name
- Status
- Last Updated
- Failure Reason



Maintenance Period Status

Shows the list of Maintenance Period tasks running on computers with their status. The following information is shown in the report:

- Computer Name
- Tags
- Policy
- Date
- Start Time
- End Time
- Status

Deep Freeze

Workstation Status

Shows the status of the computers whether Frozen or Thawed with the following information:

- Computer Name
- Tags
- Group
- Policy
- IP Address
- MAC Address
- Last Reported
- Version
- Status



If you are using Deep Freeze Enterprise, this report will show the computers managed by Deep Freeze Enterprise Console.

Workstation Task Summary

Shows the list of tasks on the computers with the following information:

- Computer Name
- Tags
- Group
- Task Name
- Status
- Last Updated



Data Igloo

Data Igloo Status Report

Shows the action performed by Data Igloo Service along with a log file for actions that have failed.

The following information is displayed:

- Computer Name
- Tags
- Policy
- Type
- Status (Success or Failure*)
- Last Update

* Click *View Log* for the actions that have failed for detailed information.

Anti-Executable

Anti-Executable Activity Report

Shows the activity on all computers managed by Anti-Executable Service.

The following information is displayed:

- Computer Name
- Tags
- User
- Event Description
- Time Stamp

Anti-Executable Blocked Programs Report

Shows the programs blocked by Anti-Executable Service.

The following information is displayed:

- Program Name
- Violations Count
- Last Violation

Anti-Executable Computers with Violations Report

Shows the list of computers with violations when managed by the Anti-Executable Service.

The following information is displayed:

- Computer Name
- Tags
- Violations Count



- Last Violation

Anti-Executable Additions to Local Control List Report

Shows the list of files added to the Local Control List.

The following information is displayed:

- Computer Name
- Tags
- User
- File Name
- AE Action (Allow or Block)
- Path
- Time Stamp

Anti-Executable Additions to Central Control List Report (Files)

Shows the list of files added to the Central Control List.

The following information is displayed:

- User
- File Name
- Time Stamp

Anti-Executable Additions to Central Control List Report (Publishers)

Shows the list of Publishers added to the Central Control List.

The following information is displayed:

- User
- Publisher
- Time Stamp

Software Updater

Application Update Status

Shows the installed version of each application selected within Software Updater and whether the latest version is installed. Even if a particular software is not currently managed or updated by the Software Updater, but is in the list of software that can be managed by Software Updater, this report shows the version of the unmanaged software currently installed on the computer.

The following information is displayed:

- Computer Name
- Tags
- Policy
- Group
- Last Audit (hh:mm:ss)



- Status (click on the status for detailed information)
- Application Name / Version

Click (+) and select the applications to add them to the column.

Activity Logs

Shows the detailed Software Updater activity by computer, logging successful installation status and reasons for failure for each application.

The following information is displayed:

- Computer Name
- Tags
- Policy
- Group Name
- Status (click *View Log* for detailed information like Application Name and Version)
- Last Updated (hh:mm:ss)

Usage Stats

Application Usage Report

Shows a summary of application usage on computers with the number of users using the applications and computers where the applications are installed.

The following information is displayed:

- Application Name
- Total Usage (Day(s) – hh:mm:ss)
- No. of Computers
- No. of User
- No. of Logins

Computer Usage Report

Shows a summary of computer usage with the number of logins by unique users.

The following information is displayed:

- Computer Name
- No. of Logins
- Unique Users
- Total Usage (Day(s) – hh:mm:ss)
- Avg. Duration (Day(s) – hh:mm:ss)

Login Summary Report

Shows a summary of users logging into the computers.

The following information is displayed:



- User Name
- No. of Logins
- Total Usage (Day(s) – hh:mm:ss)
- Avg. Duration (Day(s) – hh:mm:ss)
- First Login
- Last Login

Software License Compliance Report

Shows details of whether managed software is over-deployed or under-utilized.

The following information is displayed:

- Product Name
- Tags
- Latest Version
- Publisher
- Nodes
- Users
- Entitled
- Valid Until
- Compliance

Managed Software Usage Report

Shows the time during which managed software is actively used by users as well as its running time, along with the number of computers where the software is installed.

The following information is displayed:

- Application Name
- Active Usage (Day(s) – hh:mm:ss)
- Running Time (Day(s) – hh:mm:ss)
- No. of Computers
- No. of Users
- No. of Logins

Incident Reporting

Incidents Summary

Shows the bullying incidents reported by the students.

The following information is displayed:

- Date/Time
- Tags
- Description
- Computer Name



- User Name

Power Save

If Windows Power Management settings are enabled or any other third-party power saving measures are being used in the organization, then the actual power saving may be lower than that shown in the report.

Let's say that Power Save and Windows Power Management are configured to put the computer on Standby at 10 pm and 11 pm respectively. Assuming Power Save takes action at 10 pm and puts the computer on Standby, the Power Save Reports take credit for savings from the moment the computer goes on Standby up to when the computer wakes up.

For each of the reports listed, you can select the following two types of report:

- Full Operation Report
 - > Include Windows Power Plan Savings – select this checkbox if you want to include the savings from Windows Power Plan.
- Audit Report

Optionally, select the Group to generate the report for the particular group. The results will include computers that belong only to the selected group.

Saving by Energy Consumption

Shows the savings for each Energy Consumption Profile on the computers. The following information is displayed:

- Energy Consumption Profiles & Savings
 - > Name
 - > Monitor On (watts)
 - > Monitor Standby (watts)
 - > Computer On (watts)
 - > Computer Standby (watts)
 - > Workstation Count
 - > Energy Saved (kWh)
 - > Savings (\$)
- Detailed Power Save Performance Report
 - > Workstation Name
 - > Tags
 - > IP Address
 - > MAC Address
 - > Group
 - > Consumption Profile
 - > Monitor Standby (days)
 - > Computer Standby (days)
 - > Computer Off (days)



- > Energy Saved (kWh)
- > Energy Consumed (kWh)
- > Savings (\$)

Saving by Custom Power Policies

Shows the savings for each Policy on the computers. The following information is displayed:

- Custom Policies & Savings Report
 - > Name
 - > Workstation Count
 - > Average Savings (\$)
 - > Energy Consumed (kWh)
 - > Energy Saved (kWh)
 - > Savings (\$)
- Detailed Power Save Performance Report
 - > Workstation Name
 - > Tags
 - > IP Address
 - > MAC Address
 - > Group
 - > Policy
 - > Monitor Standby (days)
 - > Computer Standby (days)
 - > Computer Off (days)
 - > Energy Saved (kWh)
 - > Energy Consumed (kWh)
 - > Savings (\$)

Top 25 Energy Savers

Shows top 25 computers that save the most energy. The computers ranked from 1 through 25, where 1 is the computer that has the highest dollar savings. The following information is displayed:

- Workstation Name
- Tags
- IP Address
- MAC Address
- Group
- Policy
- Monitor Standby (days)
- Computer Standby (days)
- Computer Off (days)



- Energy Saved (kWh)
- Energy Consumed (kWh)
- Savings (\$)

Bottom 25 Energy Savers

Shows the 25 computers that save the least energy. The computers ranked from 1 through 25, where 1 is the computer that has the lowest dollar savings. The following information is displayed:

- Workstation Name
- Tags
- IP Address
- MAC Address
- Group
- Policy
- Monitor Standby (days)
- Computer Standby (days)
- Computer Off (days)
- Energy Saved (kWh)
- Energy Consumed (kWh)
- Savings (\$)

Policy Configuration Report

Shows the Power Save Schedule settings along with the associated Power Events. The following information is displayed:

- Policy Name
- Power Schedule
- Number of computers where the policy is applied

Select the report for All Power Save policies or a specific policy.

Anti-Virus

Protection Status

Shows the details of Anti-Virus activity on the computer with the following details:

- Computer Name
- Tags
- Status
- Active Protection
- Firewall Protection
- Last Scan



- Definitions Version
- Last Definition Update
- Last Threat Detected
- Version

Anti-Virus Definition Update Status

Shows the details of Anti-Virus definition update activity on the computer with the following details:

- Computer Name
- Tags
- Definition Status
- Definition Version
- Last Definitions Update

Last Scan

Shows the last scan performed on the computers with the following details:

- Computer Name
- Tags
- Date of Last Scan
- Scan Engine Version
- Definitions Version
- Total Found
- Cookies
- Registry
- Files
- Processes
- Deleted
- Quarantined

Scan History

Shows the historical information about past scans with the following details:

- Computer Name
- Tags
- Scan Date
- Scan Engine Version
- Definitions Version
- Trace Type
- Data



Active Protection History

Shows the historical information about threats detected per computer with the following details:

- Computer Name
- Tags
- Event Date
- Event Type
- Monitor Type
- Application

Quarantine

Shows the information about quarantined items on selected computers with the following details:

- Computer Name
- Tags
- Risk Name
- Risk Category
- Event Date
- File Name
- Original Location
- Risk Level
- Age (days)
- Quarantined By

Firewall Daily Network Activity

Show the information for network traffic on allowed and blocked ports with the following details:

- Computer Name
- Tags
- Date
- Policy
- ARP In
- ARP Out
- ICMP In
- ICMP Out
- UDP In
- UDP Out
- TCP In
- TCP Out
- Other In



- Other Out

Top 25 Infected Machines

Shows the historical information about Threats by Number of Detections within a specified period of time with the following details:

- Computer Name
- Tags
- Threat Count
- Status
- Definition Status
- Last Definitions Update
- Last Scan

System Event Messages

Shows the log of events that occurred on the selected computers with the following details:

- Computer Name
- Event Date
- Subsystem
- Description



Utilities

Deep Freeze Cloud Console provides additional utilities for various purposes. The configuration options for Utilities are explained further in this chapter.

- [General Utilities](#)
- [Deep Freeze Utilities](#)
- [Deep Freeze Mac Utilities](#)
- [Anti-Virus Utilities](#)
- [Software Updater Utilities](#)
- [Anti-Executable Utilities](#)

General Utilities

Deployment Utility

The Deployment Utility allows you to deploy the Cloud Agent (including all Services) to computers across your network. The Deployment Utility allows you to select the Policy and all the Services selected in the Policy will be deployed on the selected computers. Once the Cloud Agent is installed, the computers will be visible in Deep Freeze Cloud Console. You can then enable the Services for all computers from the Deep Freeze Cloud Console.

Complete the following steps to deploy the Cloud Agent using the Deployment Utility:

1. Log in to Deep Freeze Cloud Console.
2. Go to the *Utilities* page.
3. Click *Download* for the Deployment Utility.
4. Double-click the Deployment Utility. The Deployment Utility must be run as an administrator.
5. Select the Policy from the drop-down.
6. Select one of the following two options:
 - > Workgroup
 - ~ Select this option and click *Scan*.
 - ~ Select the computers and click *Install*.
 - > Active Directory
 - ~ Select this option and click *Scan*.
 - ~ Specify the Server Name, User, and Password and click *OK*.
 - ~ Select the computers and click *Install*.
7. A ProductInstaller directory is created in the same location where the Deployment Utility is run and the Cloud Agent (including installers for all Services) are downloaded to this directory. The Cloud Agent (including all Services) are installed on the computers.



Once the installation is complete, the computers are visible in the Deep Freeze Cloud Console on the *Computers* page.

Active Directory Import Utility

The Active Directory Import Utility allows you to import groups from your Active Directory Server into the Deep Freeze Cloud Console.

Complete the following steps to import groups from your Active Directory Server:

1. Log in to Deep Freeze Cloud Console.
2. Go to the *Utilities* page.
3. Click *Download* for the Active Directory Import Utility.
4. Double-click the downloaded Active Directory Import Utility.
5. Configure the following:
 - > Server – specify the Active Directory Server.
 - > User – specify the user name for the Active Directory Server.
 - > Password – specify the password for the Active Directory Server.
 - > Use credentials of the logged-in user – select this option if the credentials of the logged-in user are the same as the credentials of the Active Directory Server.
 - > Remember credentials – select this option if you want the Active Directory Import Utility to remember your credentials.
6. Click *Log On*.
7. Click *Import*.

The Active Directory groups are imported into the Deep Freeze Cloud Console. The Active Directory groups are visible in the *Groups* page in the Deep Freeze Cloud Console.

Deep Freeze Utilities

One Time Password Generator

A One Time Password (OTP) Generator is useful when a Deep Freeze password is lost or if a password was not specified in Policy for the Deep Freeze Cloud Service. An OTP Generator can also be used to provide access to a computer for a user performing maintenance duties without requiring to know the permanent Deep Freeze password.

To create an OTP, complete the following steps:

1. Log in to Deep Freeze Cloud Console.
2. Go to the *Utilities* page.
3. Click *Generate* for the One Time Password Generator.
4. Select either *Password valid for one use only* or *Password valid for multiple uses*. All OTPs expire at midnight on the day they were created, regardless of type.
5. Enter the OTP Token from the computer that requires the OTP into the *Token* field.



6. Click *Generate*.



The Deep Freeze Command Line interface does not support the use of One Time Passwords.

MSI Packager

The Deep Freeze MSI Packager allows you to transform the Deep Freeze Workstation Install Program (DFWks.exe) file available with the Deployment Utility into a Windows Installer (.MSI) file format for deployment with Active Directory.

Complete the following steps to convert a Deep Freeze Workstation Install Program into a Windows Installer:

1. Log in to Deep Freeze Cloud Console.
2. Go to the *Utilities* page.
3. Click *Download* for the MSI Packager.
4. Unzip the MSI packager and extract to a location on your computer.
5. Double-click the MSI Packager application in the 32-bit folder (to create a 32-bit MSI file) or in the 64-bit folder (to create a 64-bit MSI file).
6. Configure the following settings:
 - > Package Name – specify a name of the MSI package.
 - > Deep Freeze Installer file – enter the path or browse to select the Deep Freeze Workstation Install Program (DFWks.exe).
 - > Location to Save MSI File – enter the path or browse to select the location to save the MSI file.
7. Select *Accept terms and conditions*.
8. Click *Convert to MSI*.

You can now deploy the MSI file to computers on your network from the Deep Freeze Cloud Console.

On Demand Cloud Relay

The On Demand Cloud Relay allows the Deep Freeze Cloud Console to perform real time actions on your computers.

Complete the following steps to install the On Demand Cloud Relay:

1. Click *Utilities*.
2. Click *Download* for the *On Demand Cloud Relay*.
3. Double-click the *On Demand Cloud Relay*. Click *Next*.
4. Accept the License Agreement. Click *Next*.
5. Specify your email and password used to log on to the Deep Freeze Cloud Console. Click *Install*.



6. Click OK.



Install the On Demand Cloud Relay on any computer on your network. Make sure the computer is on the same subnet as the Deep Freeze Enterprise Console. If you have multiple subnets and they are not configured to communicate with each other, you must install one On Demand Cloud Relay per subnet.

Deep Freeze Mac Utilities

Deep Freeze Mac Command Line (APFS)

The Deep Freeze Mac Command Line gives network administrators increased flexibility in managing Deep Freeze Mac computers. These commands can be run with several different third-party enterprise management tools, such as Apple Remote Desktop, and/or central management solutions; this includes executing commands in Terminal while connected to a remote computer via SSH.

Deep Freeze Mac has the following command line options.

Usage: `deepfreeze <command> <verb> argument [option]`



Specify the Deep Freeze Mac Command Line Utility full path `/usr/local/bin/deepfreeze` when executing the command using third-party management tools.



If Deep Freeze password is enabled, Deep Freeze password can be passed as an environment variable by specifying "`--env`".

Usage:

`DFXPSWD=password /usr/local/bin/deepfreeze <command>
<verb> argument [option] --env`

Command	Description
<code>deepfreeze version</code>	Displays the Deep Freeze Mac version.
<code>deepfreeze status</code>	Displays the current status of Deep Freeze Mac.



Command	Description
<pre>deepfreeze freeze --volume VolumeName --startup --computer deepfreeze thaw --volume VolumeName --startup --computer</pre>	<p>--volume – Freeze or thaw a specific volume</p> <p>--startup – Freeze or thaw the startup volume</p> <p>--computer – Change Global state</p> <p>Volumes will be set to Frozen or Thawed depending on the status of Deep Freeze.</p>
<pre>deepfreeze license [--info]</pre>	<p>[--info] shows detailed information of the license</p> <p>This command displays the full license key if run with root privilege or if Deep Freeze password is enabled.</p>
<pre>deepfreeze password enable deepfreeze password disable</pre>	<p>Enable or disable Deep Freeze password.</p>
<pre>deepfreeze password add --description Description deepfreeze password edit --description Description [--newdescription newDescription] deepfreeze password delete --description Description</pre>	<p>Add, edit or delete Deep Freeze password.</p>
<pre>deepfreeze hideicon frozen [--on --off] deepfreeze hideicon thaw [--on --off]</pre>	<p>Show or hide the Deep Freeze Frozen icon in the menu bar.</p>
<pre>deepfreeze restartinstead [--on --off]</pre>	<p>Restart the computer after user logs out, or the last user logs out if fast user switching is enabled.</p>
<pre>deepfreeze ardinfo [--set N --clear]</pre>	<p>Set or clear ARD info field.</p>



Command	Description
<pre>deepfreeze schedule add --name "ScheduleName" [--enable on off] --day monday[,tuesday,wednesday,thursday,friday,s aturday,sunday] --begin "24-hr-time" --end "24-hr-time" [--onceonly on off] [--installappleupdate on off] [--lockuser on off] [--warnuser off "5-999"] [--message "message string"] [--shutdownafter on off] [--runscript off "script file name"]</pre>	
<pre>deepfreeze schedule edit --name "ScheduleName" [--enable on off] [--day monday[,tuesday,wednesday,thursday,friday,s aturday,sunday]] [--begin "24-hr-time"] [--end "24-hr-time"] [--onceonly on off] [--installappleupdate on off] [--lockuser on off] [--warnuser off "5-999"] [--message "message string"] [--shutdownafter on off] [--runscript off "script file name"]</pre>	Add, edit, remove, enable or disable Maintenance schedules.
<pre>deepfreeze schedule delete --all --name "ScheduleName"</pre>	
<pre>deepfreeze schedule enable --name "ScheduleName"</pre>	
<pre>deepfreeze schedule disable --name "ScheduleName"</pre>	
<pre>deepfreeze schedule scripts --add "ScriptFullpath"</pre>	Add, delete or list scripts.
<pre>deepfreeze schedule scripts --delete "ScriptName"</pre>	This command requires root privilege, even when Deep Freeze password is enabled.
<pre>deepfreeze schedule scripts --list</pre>	

Deep Freeze Tasks for ARD

Select this utility to install Deep Freeze tasks to manage Deep Freeze remotely via ARD. Complete the following steps after downloading the utility.

1. Double-click *Deep Freeze Tasks for ARD*.
2. Select the tasks to install.
3. Click *Continue*.



4. If *Deep Freeze tasks for APFS* is selected, you have the option to use Deep Freeze password if Deep Freeze password is enabled on the console. Select *Use Deep Freeze Password* and enter the password. If *Deep Freeze tasks for HFS+* is selected, specify Deep Freeze user name and password.
5. Click *Continue*.



If you are using Apple Remote Desktop 3.7 or later, you must restart the computer to finalize installing Deep Freeze Tasks. You will be presented with an option to restart the computer at the end of installation. Click *Restart* to restart the computer and finalize the installation.

In ARD, the Deep Freeze-specific tasks are saved in the *Deep Freeze (APFS)* and *Deep Freeze (HFS+)* folder.

The following tasks are available for Deep Freeze (APFS):

Task	Description
DeepFreeze (APFS):addPassword	Add Deep Freeze password.
DeepFreeze (APFS):addSchedule	Add a Maintenance schedule.
DeepFreeze (APFS):addScript	Add scripts.
DeepFreeze (APFS):clearArdInfo	Clear the ARD Info Field
DeepFreeze (APFS):deleteAllSchedules	Delete all Maintenance schedules.
DeepFreeze (APFS):deletePassword	Delete Deep Freeze password.
DeepFreeze (APFS):deleteSchedule	Delete a Maintenance schedule.
DeepFreeze (APFS):deleteScript	Delete one scripts at a time.
DeepFreeze (APFS):disablePassword	Disable Deep Freeze password.
DeepFreeze (APFS):disableSchedule	Disable a Maintenance schedule.
DeepFreeze (APFS):editPassword	Edit Deep Freeze password.
DeepFreeze (APFS):editSchedule	Edit a Maintenance schedule.
DeepFreeze (APFS):enablePassword	Enable Deep Freeze password.
DeepFreeze (APFS):enableSchedule	Enable a Maintenance schedule.
DeepFreeze (APFS):freezeComputer	Change Global state to Frozen.
DeepFreeze (APFS):freezeStartup	Freeze the startup volume.
DeepFreeze (APFS):freezeVolume	Freeze a specific volume.
DeepFreeze (APFS):hideFrozenIcon	Show or hide the Deep Freeze Frozen icon in the menu bar.



Task	Description
DeepFreeze (APFS):hideThawedIcon	Show or hide the Deep Freeze Thawed icon in the menu bar.
DeepFreeze (APFS):licenseInfo	Displays the License information.
DeepFreeze (APFS):listScripts	List all the script files.
DeepFreeze (APFS):restartInstead	Restart the computer when the user logs out (if fast user switching is enabled, restart the computer when the last user logs out)
DeepFreeze (APFS):setArdInfo	Set the specific ARD Info Field to show Deep Freeze status.
DeepFreeze (APFS):status	Displays the current status of Deep Freeze Mac.
DeepFreeze (APFS):thawComputer	Change Global state to Thawed.
DeepFreeze (APFS):thawStartup	Thaw the startup volume.
DeepFreeze (APFS):thawVolume	Thaw a specific volume.
DeepFreeze (APFS):version	Displays the Deep Freeze Mac version.

The following commands and arguments are available for Deep Freeze (HFS+):



If Deep Freeze is to be upgraded from the previous installation on the target computer, the existing Deep Freeze Administrator user name and password must be entered during this step. A new Deep Freeze Administrator cannot be created during this step if a Deep Freeze Administrator already exists.



Each task can be configured in Deep Freeze, except for *requestStatus*.

Command	Argument	Description
activateSchedule	Schedule name	Activates the scheduled updates on target computer(s); name of the schedule must be included in the command as a parameter.



Command	Argument	Description
addSchedule	schedule_name [-a "on" "off"] [-d monday[,tuesday,wednesday,thursday,friday,saturday,sunday]] [-b "24-hr-time"] [-e "24-hr-time"] [-o "on" "off"] [-i "on" "off"] [-l "on" "off"] [-w "off" 5-999] [-m "message string"] [-s "on" "off"] [-r "off" "script name"]	<p>Adds a schedule.</p> <p>24-hr-time is in the form of HH:MM.</p> <p>Multiple days is only for repeating schedules.</p> <p>When specifying multiple schedules, there should be no space between the days specified.</p>
addUser	New user name	Adds user to list.
badgeFrozenPartitions	on off	Shows/Hides Deep Freeze icon on Frozen partitions.
bootFrozen		Sets target computer(s) to restart in a Frozen state.
bootThawed		Sets target computer(s) to restart in a Thawed state.
bootThawedFor	Times	Sets target computer(s) to restart in a Thawed state for the next x restarts; this number can be customized in the Times argument.
deactivateSchedule	Schedule name	Deactivates the scheduled updates on target computer(s); name of the schedule must be included in the command as an argument.
deleteAllScripts		Deletes all scripts.
deleteScript	Script Name	Deletes a specific script.
deleteUser	User name	Deletes user from list.
editSchedule	schedule_name [--newname "new_schedule_name "] [--activate "on" "off"] [--day monday[,tuesday,wednesday,thursday,friday,saturday,sunday]] [--begin "24-hr-time"] [--end "24-hr-time"] [--onceonly "on" "off"] [--installappleupdate "on" "off"] [--lockuser "on" "off"] [--warnuser "off" 5-999] [--message "message string"] [--shutdownafter "on" "off"] [--runscript "off" "script name"]	Edits a schedule.
editUser	User name	Allows administrators to edit the name and password of a user.



Command	Argument	Description
freezePartition	Partition name	Designates a partition on target computer(s) to be Frozen.
getARDInfoField		Specifies which Apple Remote Desktop's information field is used to display the computer status.
getLicenseInfo		Displays the License information.
help		This will print all the options and parameters available in the "deepfreeze" command line tool.
mapAllUsers	(Argument 1) admin standard mobile (Argument 2) Partition name userthawspace	Maps all users to a specified ThawSpace: name of user type and location of ThawSpace must be included as a parameter; e.g. admin Panther maps all admin users to the partition named Panther.**
rebootInsteadOfLogoff	on off	Restarts target computer(s) instead of logging off when the on argument is used. This feature is turned off when the off argument is used.
removeAllSchedules		Removes all schedules.
removeAllThawSpace		Removes all ThawSpaces present.
removeSchedule	schedule_name	Removes a schedule.
removeThawSpace	userthawspace_name global	Removes a single ThawSpace***
resizeThawSpace	"global" userthawspace_name nnnn	Resizes a ThawSpace. global is entered as it is, representing global ThawSpace. nnnn is the new size in MB.
setARDInfoField	ARD Info Field	This parameter is used to specify which Remote Desktop's Information Field is used to display the computer status. The parameter value is 0 to 4, 0 is to unset the Information Field.
showFrozenIcon	on off	Configures target computer(s) to show/hide the Deep Freeze Frozen icon in the menu bar.
showThawedIcon	on off	Configures target computer(s) to show/hide the Deep Freeze Thawed icon in the menu bar.



Command	Argument	Description
status	[-x]	Requests target computer(s) to display the status of various Deep Freeze settings. x specifies that the result is in XML format.
thawPartition	Partition name	Designates a partition on target computer(s) to be Thawed.
uninstall	[keepThawSpace]	Uninstalls Deep Freeze from target computer(s). The target computer(s) must be restarted in the Boot Thawed state before the uninstall task can be run. [keepThawSpace] uninstalls Deep Freeze from target computer(s) but retains ThawSpace.
version	[-x]	Displays Deep Freeze version number. x specifies that the result is in XML format.

* = This only occurs during the first Deep Freeze installation using the settings provided by the custom installer created by Deep Freeze Assistant.

**= The mapAllUsers command also includes the parameters: "admin", "standard", "mobile", "userthawspace" and, partition name such as "Macintosh HD" or "Panther".

***= The single ThawSpace "name" must be specified as well as "global" for a Global ThawSpace.

Adding a script file via Apple Remote Desktop

Complete the following steps to add a script file via Apple Remote Desktop:

1. Select the target computer(s) from the computer list.
2. From the menu, select Manage > Copy Items...
3. Add the script files to the *Items to copy* list.
4. In the *Place items in;* select *Specify full path...* and enter */Library/Application Support/Faronics/Deep Freeze/Scripts*. Click *OK*.
5. In the *Set ownership to;* select *Inherit from destination folder*.
6. Other settings can be set as required.
7. Click *Copy*.

Adding Targeted Computers to the Task List

In order to run a task, there must be computers targeted to run the task. To add one or more computers to be targeted to run the task, complete the following steps:

1. In the left column, double-click the task to be targeted to the specified computers.



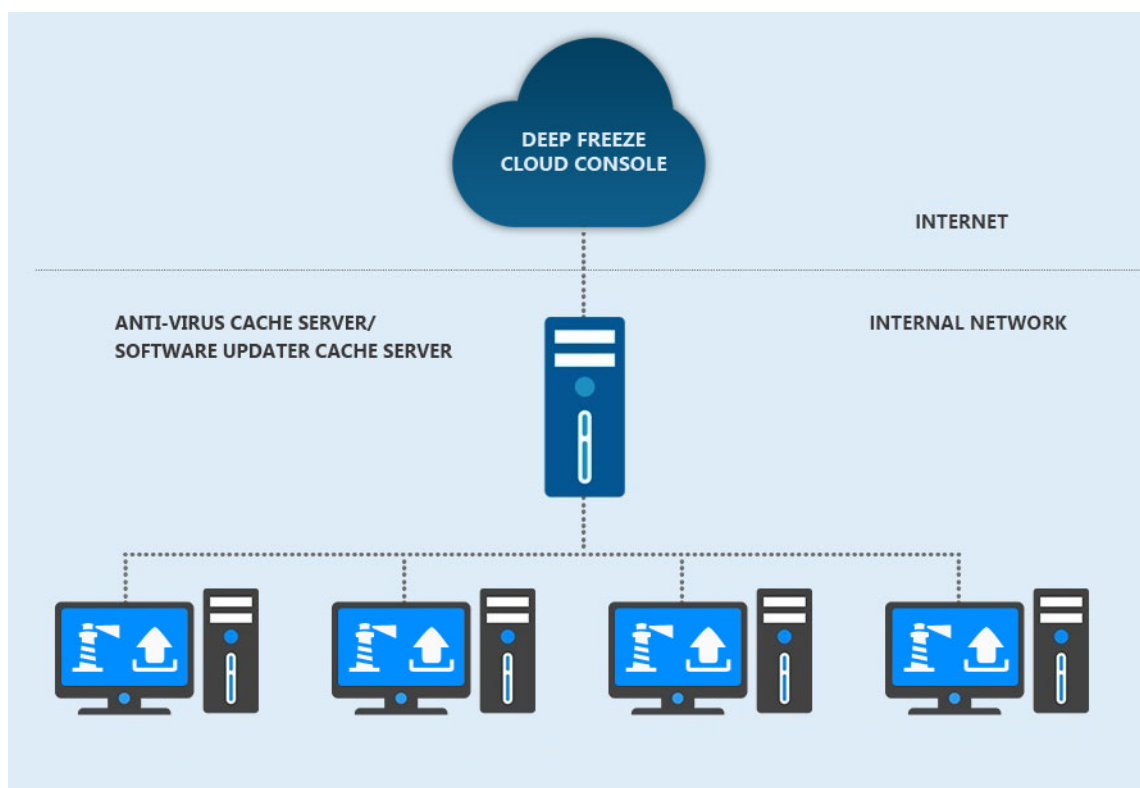
2. The *Task Edit* window appears. At the bottom of the window is a dialog listing the designated computers assigned to the task. Before a computer is added to the list, it reads *No Computers*.
3. Drag and drop the preferred computer or group of computers into the dialog from the computers in the *All Computers* list. The number of computers assigned to a specific task appears at the bottom of the window.
4. Click *Save*.

Anti-Virus Utilities

Anti-Virus Cache Server

The Anti-Virus Cache Server saves internet bandwidth by downloading virus definitions and distributing them to your computers, removing the need for the computers to perform their own individual downloads. It can be installed on any computer on your network, and is configured using the Deep Freeze Cloud Console.

For more information on configuring Anti-Virus Cache Server on Deep Freeze Cloud Console, refer to [Anti-Virus Cache Server](#).



Complete the following steps to install the Anti-Virus Cache Server:

1. Log in to Deep Freeze Cloud Console.
2. Go to the *Utilities* page.
3. Click *Download* for the Anti-Virus Cache Server.
4. Double-click the downloaded Anti-Virus Cache Server. Click *Next*.
5. Accept the *License Agreement*. Click *Next*.



6. Select *Anti-Virus Cache Server*. Click *Next*.
7. Click *Install*.
8. Click *Finish*.

Change Settings

Complete the following steps to change settings for the Cache Server:

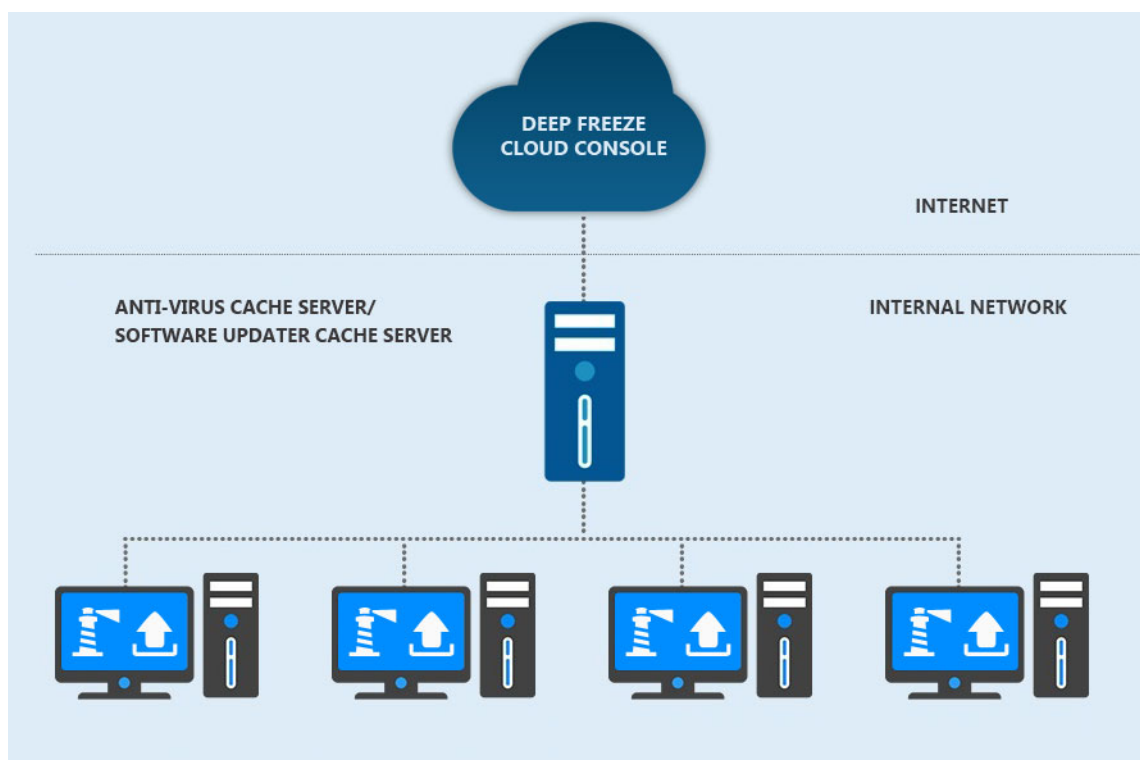
1. Launch the Cache Server from the system tray.
2. Go to the Anti-Virus tab.
3. Select *Enable Anti-Virus Cache Server* checkbox to enable the Cache Server. Clear the *Enable Anti-Virus Cache Server* checkbox to disable the Cache Server.
4. Select *Automatically update in x hours*. Specify the value in hours.
5. Click *Update Now* to update the Anti-Virus definitions. The last update check date/time and the next update check date/time are displayed.
6. Click *OK*.

Software Updater Utilities

Software Updater Cache Server

The Software Updater Cache Server saves internet bandwidth by downloading software updates and distributing them to your computers, removing the need for the computers to perform their own individual downloads. It can be installed on any computer on your network, and is configured using the Deep Freeze Cloud Console.

For more information on configuring Software Updater Cache Server on Deep Freeze Cloud Console, refer to [Software Updater Cache Server](#).



Complete the following steps to install the Software Updater:

1. Log in to Deep Freeze Cloud Console.
2. Go to the *Utilities* page.
3. Click *Download* for the Software Updater Cache Server.
4. Double-click the downloaded Software Updater Cache Server. Click *Next*.
5. Accept the *License Agreement*. Click *Next*.
6. Select *Software Updater Cache Server*. Click *Next*.
7. Click *Install*.
8. Click *Finish*.

Change Settings

Complete the following steps to change settings for the Cache Server:

1. Launch the Cache Server from the system tray.
2. Go to the Software Updater tab.
3. Select *Enable Software Updater Cache Server* checkbox to enable the Cache Server. Clear the *Enable Software Updater Cache Server* checkbox to disable the Cache Server.
4. Select *Automatically update in x hours*. Specify the value in hours.
5. Click *Update Now* to download the software updates. The last update check date/time and the next update check date/time are displayed.
6. Click *OK*.



Anti-Executable Utilities

Anti-Executable Data Import Utility

Run the Anti-Executable Data Import Utility on any computer to automatically add allowed/blocked files and publishers into the Central List.

Complete the following steps to import the data from Anti-Executable:

1. Log in to Deep Freeze Cloud Console.
2. Go to the *Utilities* page.
3. Click *Download* for the Anti-Executable Data Import Utility.
4. Double-click the downloaded Anti-Executable Data Import.
5. Configure the following settings:
 - > Select Action – select Add Files or Add Publishers.
 - > Add as – select Allow or Block.
 - > Select where you want to add from – browse to select the drive, folder or network location. You can also enter a UNC path.
 - > Include Sub-Folders when scanning – select this option if you want to scan all the sub-folders for the selected parent folder.
 - > Include DLL files when scanning – select this option to scan and add DLL files.
 - > Populate the comments field with a custom comment – add a comment for future reference or retain the existing auto-generated comment.
6. Click *Add*.

The files or Publishers are added to the Central List of the Anti-Executable Service.



Alerts

Deep Freeze Cloud administrators can now set alerts for important events on managed computers. The subscribers to the alerts are notified immediately and they can take corrective action if required.

Subscribers to the alerts can receive notifications in the following ways:

- Web console notification
- Email notification
- Deep Freeze Administrator Mobile App notification

You can do the following:

- [Manage Alerts](#)
- [Read and Take Action](#)

Manage Alerts

Complete the following steps to manage alerts:

1. Click the *Alerts* icon on the top right corner of Deep Freeze Cloud.
2. Click *Manage Alerts*.
3. Select Notification, Email or Mobile for the following Alerts:
 - > Anti-Virus
 - ~ Active protection is disabled – Active Protection (AP) is a real-time method for detecting malware. AP sits quietly in the background as you work or browse the internet, constantly monitoring files that are executed (run) without causing noticeable strain to your system.
 - ~ Firewall protection is disabled – Firewall provides bi-directional protection, protecting you from both incoming and outgoing traffic. A firewall protects your network from unauthorized intrusion.
 - ~ Virus definitions are outdated – Definitions (often called threat definitions) are the basis that an anti-virus or anti-spyware tools uses to compare against when protecting you from all sorts of malware, whether by scans, email protection, or real time protection.
 - ~ Virus is detected – The object is a legitimate file infected by a virus. Sometimes the infected file can be disinfected, and the legitimate file can be provided to the end user. However, not all types of infection can be disinfected—for example, the whole Trojan category cannot be disinfected. An important characteristic of a virus is that the virus replicates itself, ensuring its continuous spread. No other threat type replicates itself.



- ~ Spyware is detected – Spyware is a large class of malicious applications with a huge range of malicious activity. This category includes applications which steal password and credit card information, online game account passwords, provide false security alerts giving the impression that the user's machine is in a critical state and demanding money for "fixes", and so on. Usually, spyware gets installed without the user's informed consent.
- ~ Adware is detected – Adware is a class of malicious applications designed to display advertisements on the user's desktop, or in the web browser. Adware is also often used to monitor and report user browsing habits to the advertiser to bring more relevant ads. Some "free" applications available on the Web contain the adware payload, which is usually installed with user consent, while some other adware applications are installed without user consent.
- ~ Dialer is detected – Dialers are applications which use the modem connected to the computer to dial premium-rate numbers. Usually they call either local pay-per-minute numbers or international numbers; per-minute costs have been known to reach several hundreds of dollars. Even if installed with user consent, they usually do not provide information about the real cost of the call.
- ~ Malicious App is detected – The object is an application which is often installed and used for malicious purposes by 3rd parties. While the application itself is not malicious, experience shows that it poses a higher probability (compared to others) to be used for malicious purposes and being installed without user consent. This category includes web or socks proxies, remote administration software and other types of software.
- ~ Severe Level risks are detected – Severe risks are typically installed without user interaction through security exploits, and may allow an attacker to remotely control the infected machine.
- ~ High Level risks are detected – High risks are typically installed without user interaction through security exploits, and can severely compromise system security.
- ~ Moderate risks are detected – Moderate risks are often bundled with functionality unrelated software or installed without adequate notice and consent, and may make unwanted advertising on the user's desktop.
- ~ Elevated Level risks are detected – Elevated risks are typically installed without adequate notice and consent, and may make unwanted changes to your system, such as re-configuring your browser's homepage and search setting.
- ~ Low Level risks are detected – Low risks should not harm your computer or compromise your privacy and security unless they have been installed without your knowledge and consent.



- > Anti-Executable
 - ~ If Anti-Executable protection is disabled for X or more hours – Protection set to disabled, indicates that Anti-Executable is not protecting a computer based on the Policy Control List or Local Control List and any executable can be launched on the computer.
 - ~ If maintenance mode is enabled for X or more hours (Except during scheduled maintenance) – In Maintenance Mode, new executable files added or modified are automatically added to the Local Control List of Anti-Executable. Typically AE Maintenance should automatically end once scheduled maintenance is over. Computer which remains in maintenance mode for an extended time can be a security concern needing Admin attention.
 - ~ If a protected computer has X or more Violations in a day – A protected machine can have violations when a user tries to execute a file outside its Allowed list of files as authorized in its Policy Control List or Local Control List. A high number of violation can indicate as unauthorized file trying to execute itself needing Admin attention.
 - ~ If a protected computer has X or more Blocked File Violations in a day – A protected computer blocks files that are explicitly defined as Blocked in the Policy Control List or Local Control list. A "Control List Blocked" violation is logged. Admin attention may be needed if a specific computer is reporting high number of this violation type.
 - ~ If a specific file is causing Violations on X or more computers – If more than a specified number of computers report a violation or blocked event for the same file, this could be a case of a network virus attack across computers that can be actively reported by AE.
- > Deep Freeze Alerts
 - ~ If the computer is in Thawed state for more than X hours – An alert will be sent if a computer remains Thawed for longer than the configurable threshold.
Enable the *Except during scheduled maintenance* option to suppress alerts generated by computers who exceed the Thawed time threshold during a period of scheduled maintenance.
- > Software Updater Alerts
 - ~ Windows Update security status is marked as Vulnerable – A computer is marked as Vulnerable whenever it has one or more Critical or Security patches missing.
 - ~ Windows Update has a new pending patch waiting approval – An alert is sent when a new security or critical patch is pending approval.
 - ~ Windows Update patch scan status is outdated on a computer – An alert is sent when a computer's patch scan status has not been updated for over 7 days.
- 4. Specify the Computer Tags for which an alert is to be sent or not sent:
 - > If any of the tags match on a particular computer, a notification will be sent to the subscriber.
 - > Alternatively, select *Exclude computers with these Tags* if you do not want to be notified about alerts on the computers with the specified tags.
- 5. Select how you want the subscribers to receive the notification:
 - > Web console notification
 - > Email notification
 - > Deep Freeze Administrator Mobile App notification



6. Click *Save*.



If you add a Tag, the Alert will be generated only for the computers that have (or do not have) the particular Tag. If you want all the computers to be included in the Alert, do not add any Tags.

The Alerts are now configured. When the selected event occurs, the Alerts are sent to the subscriber.



The Alerts are configured for all computers under the particular Site. The Alerts are also specific to the user that created them.

Read and Take Action

Complete the following steps to read and take action on alerts:

1. Click the *Alerts* icon on the top right corner of Deep Freeze Cloud.
2. Click *See All* to see a more detailed view.
3. Click on the Alert to read it.
4. Select the X icon on the Alert that is already reviewed.

The Alert is automatically moved to the *Reviewed* tab upon selection. To completely remove the alert, click *Delete* under the Reviewed tab.



Appendix A Authorized Domains and Ports

Deep Freeze Cloud makes use of a number of ports and URLs for communication between clients and the Cloud Services.

In general, port 443 must be open to outbound traffic to allow for the Deep Freeze Cloud service to function.

Service	Domain/Port
Deep Freeze (For computers to report to the Cloud console)	http://*.deepfreeze.com
Deep Freeze Cloud	<p>To show online/offline status or execute active tasks on computers. Websockets will vary depending on the web server.</p> <ul style="list-style-type: none">• https://www-ws.deepfreeze.com/ or 34.216.139.196• https://www-ws.deepfreeze.com/ or 34.216.139.196• https://www3-ws.deepfreeze.com/ or 54.191.220.116• https://www4-ws.deepfreeze.com/ or 34.216.139.196• https://www5-ws.deepfreeze.com/ or 34.216.139.196• https://www8-ws.deepfreeze.com/ or 34.216.139.196• https://www15-ws.deepfreeze.com/ or 3.134.251.50• https://www2-ws.deepfreeze.com/ or 3.248.47.158• https://www7-ws.deepfreeze.com/ or 3.248.47.158• https://www9-ws.deepfreeze.com/ or 3.248.47.158
Deep Freeze Cloud (S3 Bucket for the installers)	https://s3-us-west-2.amazonaws.com/faronics-dfc-s3-installer-production/Download/
Anti-Virus Definition Server	http://defs.deepfreeze.com/
Anti-Virus Definition Cloud front	d1mrzy9ysz9qq.cloudfront.net
Remote (RDP/VNC) North America	52.88.207.40
Remote (RDP/VNC) International	34.251.160.43
Remote Pro North America: United States (East)	https://useast-rcpcloud.deepfreeze.com:443 or 3.140.73.22 TCP 10000-20000 (WebRTC)
Remote Pro North America: United States (West)	https://uswest-rcpcloud.deepfreeze.com:443 or 54.219.75.81 TCP 10000-20000 (WebRTC)
Remote Pro International: EU (West - Ireland)	https://remote-pro-eu-west-1.deepfreeze.com or 34.248.1.73 TCP 10000-20000 (WebRTC)



Service	Domain/Port
Active Directory Authenticator	https://*.deepfreeze.com
Cloud Relay	https://*.deepfreeze.com
Anti-Executable Cloud Support (Windows OS files information)	https://s3-us-west-2.amazonaws.com/faronics-dfc-s3-installer-production/Download/Utility/AEData/WinOSFiles.xml
Anti-Executable Cloud (Ransomware Extensions list)	https://4ykjtofphl.execute-api.us-west-2.amazonaws.com/production
WINSelect S3 bucket for Kiosk mode for North America	https://s3-us-west-2.amazonaws.com/faronics-dfc-winselect-ui
WINSelect S3 bucket for Kiosk mode for International	https://s3-eu-west-1.amazonaws.com/faronics-eu-winselect-ui



Using Deep Freeze On Demand

This chapter describes using the Deep Freeze On Demand feature.

Topics

[Overview of Deep Freeze On Demand](#)

[Deep Freeze Actions](#)

[Manage Schedules](#)

[Cloud Relay](#)



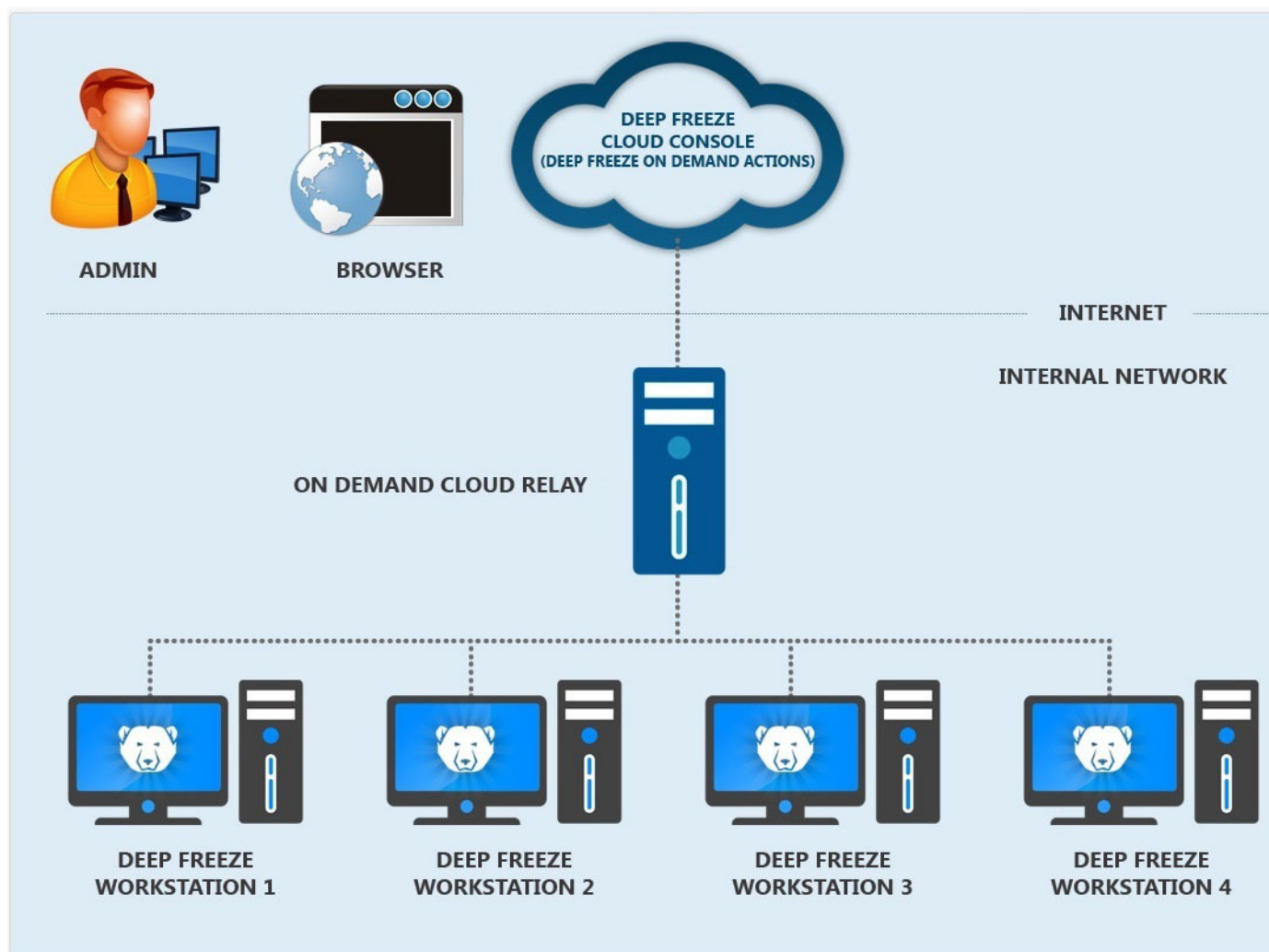
Overview of Deep Freeze On Demand

The Deep Freeze On Demand page allows you to perform real-time Deep Freeze actions on your computers.

Before using Deep Freeze On Demand, you must install the following components:

- On Demand Cloud Relay and the Cloud Agent

For more information about installing the above components, refer to [Deep Freeze Cloud Console Components](#).





Deep Freeze Actions

When the computers are visible on the Deep Freeze On Demand page, you can perform the following actions:

- Wake up managed computers
- Restart managed computers
- Shut down managed computers
- Reboot managed computers to a Frozen state
- Reboot managed computers to a Thawed state
- Reboot managed computers to a Thawed and locked state
- Lock or unlock the keyboard and mouse on managed computers
- Initiate a remote desktop connection
- Format or delete ThawSpaces on managed computers
- End computer tasks on managed computers
- Delete managed computers
- Send push messages to managed computers
- Run Windows Update on managed computers
- Apply Tags to managed computers
- Move managed computers between groups
- Assign schedules to managed computers
- Remotely launch executables on managed computers
- Push an executable to managed computers then remotely launch it



Selecting both Windows and Mac computers shows all the Live Action options. Selecting Windows and Mac computers and applying a Live Action that is not applicable to the particular computer will show the task for that computer as Failed in the task status.

On Demand Actions

Wakeup

Select one or more computers and click *Wakeup*.

Restart

Select one or more computers and click *Restart*.

Shutdown

Select one or more computers and click *Shutdown*.



Reboot Frozen

Select one or more computers and click *Reboot Frozen*.

Reboot Thawed

Reboot Thawed

Select one or more computers and click *Reboot Thawed*.

Reboot Thawed Locked

Select one or more computers and click *Reboot Thawed Locked*. This command reboots the computers in Thawed state and locks the computer so a non-administrator cannot log on.

For both options, you can select the *Thaw Computer(s) for Next X Restarts* and assign the number of restarts.

Selecting this option will reboot the computer in Thawed or Thawed Locked state for the assigned restarts.

For example, when you assign '3' as the number of restarts, the computer will remain in a Thawed or Thawed Locked state after rebooting the next 3 times.

The maximum number of times you can select to reboot the computer in Thawed or Thawed Locked state is 99.

Maintenance

The Maintenance menu has the following options:

Lock Keyboard and Mouse

Select one or more computers and click *Lock Keyboard and Mouse*.

Unlock Keyboard and Mouse

Select one or more computers and click *Unlock Keyboard and Mouse*.

Control with RDC

Select a single computer and select Control with RDC. Double-click to launch the .rdp file to connect to the computer.

Format ThawSpace

Deep Freeze On Demand provides the ability to format all the ThawSpaces remotely on managed computers.

1. Select one or more computers.
2. Click *Maintenance > Format ThawSpace*.
3. A warning *All ThawSpaces will be formatted on the selected computer(s)* is displayed.
4. Select *Would you like to proceed?* to confirm.



5. Click *OK*.



The *Format ThawSpace* command deletes all data on the ThawSpace. The data cannot be recovered once it is deleted. Backup important files before formatting the ThawSpace.

Delete ThawSpace

Deep Freeze on Demand provides the ability to delete a specific ThawSpace or delete all the ThawSpaces on managed computers.

1. Select one or more computers.
2. Select *Maintenance > Delete ThawSpace*.
3. The Delete ThawSpace dialog is shown. Select *All* or select the specific drive to delete.
4. Select *I understand there is no going back and the ThawSpace(s) will be permanently deleted*.
5. Click *OK*.

End Workstation Tasks

Select one or more computers and click *End Workstation Tasks*.

Delete Computer

Select one or more computers and click *Delete Computer*. The selected computers are deleted from the list. You will not be able to perform On Demand actions on the computer.

Send Message

Select one or more computers and click *Send Message*. Define the message text, or select a previously defined message, then click *Send*.

Run Windows Updates

Select one or more computers and click *Run Windows Updates*.

Tag

Select one or more computers and click *Tag*. Specify the tag and click *OK*.

Move to Group

Select one or more computers and click *Move to Group*.

Assign Schedule

Complete the following steps to assign a Schedule:

1. Select one or more computers and select *Assign Schedule*, or click *Manage Schedule* to create a new schedule. Refer to [Manage Schedules](#).
2. Select the schedule you want to assign the computers to.



Cloud Relay needs to be installed to be able to assign schedules. Refer to [Cloud Relay](#) for more information.

Remote Launch

You can remotely launch executable files on managed computers.

Complete the following files to remotely launch files:

1. Select one or more computers.
2. Click *Remote Launch*. The Remote Launch dialog is displayed.
3. Browse to select the file path or specify the file path.
 - > Filename and Path – specify the filename and path where the file is available on the target computer. Alternatively, you can browse to select the executable. File types supported are .exe (executables) and .msi (MSI installers). MSI installers are run in install mode by default. For example, if the executable MyApplication.exe is available at C:\AppFolder, specify C:\AppFolder\MyApplication.
4. Specify the Command Line Parameters with environment variables (optional):
 - > Arguments – enter the arguments that you want to apply with this executable, or select a set of parameters used recently in the past. For example, if the executable is run from the command prompt with the command C:\AppFolder\MyApplication -o logFile.log, specify -o logFile.log for arguments. For .msi files, specify the arguments that you would normally specify when launching a .msi file with MSIEEXEC. If you do not specify any argument for a .msi file, Deep Freeze will automatically append "/i" (install). Deep Freeze also replaces any display options with /qn, (quiet, no UI).
5. Click OK.

The file is remotely launched on the selected computers.

Push and Launch

You can push and launch files on managed computers.

1. Select one or more computers.
2. Click *Push and Launch*. The Push and Launch dialog is displayed.
3. Browse to select the file path or specify the file path.
 - > Filename and Path – specify the filename and path where the file is available on the console computer. Alternatively, you can browse to select the executable. File types supported are .exe (executables) and .msi (MSI installers). MSI files are run in install mode by default. For example, if the executable MyApplication.exe is available at C:\AppFolder, specify C:\AppFolder\MyApplication.
4. Specify the Command Line Parameters with environment variables (optional):
 - > Arguments – enter the arguments that you want to apply with this executable, or select a set of parameters used recently in the past. For example, if the executable is run from the command prompt with the command C:\AppFolder\MyApplication -o logFile.log, specify -o logFile.log for arguments. For .msi files, specify the arguments that you would normally specify when launching a .msi file with MSIEEXEC. If you do not specify any argument for a .msi file, Deep Freeze will automatically append "/i" (install). Deep Freeze also replaces any display options with /qn, (quiet, no UI).
5. Click OK.

The file is pushed to the selected computers and remotely launched.



Manage Schedules

A schedule is a task or group of tasks that is performed at a set time in the future, and can be configured to be performed on a recurring basis. Once a schedule is defined, you can assign it to computers—those computers then perform the tasks at the times you defined.

A schedule can consist of the following:

- Any single task from the list below:
 - > Restart
 - > Shutdown
 - > Wake-on-LAN
 - > Reboot Frozen
 - > Reboot Thawed
 - > Reboot Thawed Locked
 - > Send Message
 - > Run Window Update
 - > Format ThawSpace
 - > Remote Launch
 - > Push & Launch
- A Combination Task, which is a combination of up to 5 tasks from the list below. The start times for all the tasks within a Combination Tasks must be within the same 20-hour period.

Regardless if your schedule includes one or multiple tasks, you define the time of day when each task starts, and how frequently the schedule is to be executed.

Creating a New Schedule

1. Go to *Deep Freeze On Demand > Assign Schedule > Manage Schedules*.
2. Click *Add Schedule*. The Add Schedule window opens.
3. Define a Schedule Name. This is purely an identifier and will not be seen by users, but it must be unique.
4. Define what task(s) will be executed as part of the schedule:
 - > Task Type – use this field to select what task will be executed by the schedule. Your options are the following:
 - ~ Combination Task – select this option to run multiple tasks within the same schedule. Additional controls will appear; see step 5 for further instructions.
 - ~ Restart – reboots scheduled computers.
 - ~ Shutdown – shuts down scheduled computers.
 - ~ Wake-on-LAN – sends wake-up command to scheduled computers.
 - ~ Reboot Frozen – reboots scheduled computers into Frozen state.
 - ~ Reboot Thawed – reboots scheduled computers into Thawed state.



- ~ Reboot Thawed Locked – reboots scheduled computers into Thawed state, but locks out the keyboard and mouse. In this state, files can be modified remotely but not locally.
- ~ Send Message – sends a push message to scheduled computers. If you select this option, an empty field appears below; use this field to define the message text.
- ~ Run Windows Update – run Windows Update on scheduled computers.
- ~ Format ThawSpace – reformat one or more ThawSpaces on scheduled computers. If you select this option, use the *Select Drive* field that appears to select which ThawSpace(s) require formatting, and confirm that you are aware that existing data will be erased using the checkbox below.





Note that using the Format ThawSpace command will irrevocably erase all existing data within affected ThawSpaces!

- ~ Remote Launch – remotely launch an executable on scheduled computers. If you select this option, *File Path or URL* and *Command Line Parameters* fields appear. Use these fields to enter the location of the file on the scheduled computers to be executed, and define any command line parameters that should be incorporated into the launch command.
 - ~ Push & Launch – push a locally available executable to scheduled computers and remotely launch it. If you select this option, *File Path or URL* and *Command Line Parameters* fields appear. Use these fields to enter the location of the file on your local computer or network to be executed, and define any command line parameters that should be incorporated into the launch command. Note that the file will be automatically removed from the scheduled computers after.
5. If you selected Combination Task as your Task Type, additional controls appear below to enable you to select up to five tasks to be part of the schedule.
 - > Use the *Select Task* field that appears to define the first task to be executed. The options are the same as for the *Task Type* field described above (except that Combination Task is not available), and note that additional fields may appear depending on what task is selected.
 - > To add another task to the schedule, click the + icon to add a new *Select Task* field. The schedule can include up to five tasks. Tasks will be executed in the order that they are listed.
 - > To remove a task, click the associated x icon.
 6. Define when the tasks will occur by defining the following properties:
 - > Start Time – use this field to define when the task will start.
If you are creating a schedule with multiple tasks, each task will have its own Start Time. Define the time for each task normally, but note that all tasks must be started within a 20-hour window. For example, if the first task starts at 6:00am, the last task could start no later than 2:00am, 20 hours later.



- > Frequency – use this field to define how frequently the schedule should be executed. Depending on what option you select, additional fields and controls appear that enable you to refine your choice.
Your options are as follows:
 - ~ Daily – the schedule should be executed every day or every few days. For example, you could configure the schedule to run every day, or every fifth day.
 - ~ Weekly – the schedule should be executed on certain days of the week, or on certain days every few weeks. For example, you could configure the schedule to run every day except Wednesday, or on every third Saturday and Monday.
 - ~ Monthly – the schedule should be executed on a certain day of certain months. For example, you could configure the schedule to run on the 12th day of every month, or the second Tuesday of February and July.
 - ~ One Time Only – when the current time reaches the Start Time, the schedule will be executed once. Note that the Start Time must be greater than the current time to use this option.
 - > Start Date – use this field to define the earliest date the schedule should take effect.
7. Click *Add*.

Editing or Deleting an Existing Schedule

1. Go to *Deep Freeze On Demand > Manage Schedules*.
2. Scroll through the list of schedules and locate the one you want to edit or delete.
3. Edit or delete the schedule as needed:
 - > To open the schedule for editing, click the associated  icon. This will enable you to remove computers from an assigned schedule.
 - > To delete the schedule, click the associated  icon. Click Yes in the confirmation prompt to confirm the deletion.



Cloud Relay

Select the *Enable On Demand Deep Freeze Cloud Relay* to manage computers on your network using the Cloud Relay. If you clear the *Enable On Demand Deep Freeze Cloud Relay* checkbox, the Cloud Relay will be disabled and Deep Freeze Cloud Console will communicate directly with the Cloud Agent.



It is not mandatory to select the *Enable On Demand Deep Freeze Cloud Relay* checkbox. Most of the Deep Freeze actions can be performed through Live Actions. For more information go to [Live Actions](#).

The On Demand Cloud Relay allows the Deep Freeze Cloud Console to perform real time actions on your computers. Install the On Demand Cloud Relay on the same subnet as the computers you want to manage. The Cloud Relays page displays the list of Cloud Relays installed on your network.



If you are using Deep Freeze Enterprise Console, the Cloud Relay is not required to manage computers. Therefore, the Cloud Relay is unavailable to Deep Freeze Enterprise Console users.

Go to *Deep Freeze On Demand > Cloud Relays* to view the list of Cloud Relays. The following fields/actions are displayed:

- Computer Name – name of the computer where the Cloud Relay is installed.
- IP Address – the IP address of the computer where the Cloud Relay is installed.
- Port Number – the port used by the Cloud Relay to communicate with the Deep Freeze Cloud Console.
- Computers – the number of computers managed by the Cloud Relay.
- Version – the version number of the Cloud Relay.
- Status – whether the Cloud Relay is online or offline.
- Last Reported – when the Cloud Relay reported to the Deep Freeze Cloud Console.
- Actions – actions that can be performed on the Cloud Relay:
 - > Click *Download* to download the Cloud Relay.
 - > Click *Refresh* to restart the Cloud Relay.
 - > Click *Delete* to uninstall the Cloud Relay.



Tags

This chapter explains how to assign, add, edit and delete Tags.

Topics

[Tags](#)

[Assign Tags](#)

[Manage Tags](#)



Tags

Tags are keywords added to Computers, Groups, Policies, Reports and Users. Tags are useful in the following ways:

- Provide additional contextual information about Computers, Groups, Policies, Reports, and Users.
- Helps group together multiple items such as Computers, Groups, Policies, Reports, and Users.

You can add general Tags or Location Tags. For example, you may want to Tag the computers as per departments like Accounts, Marketing, or Sales. You can then search for the Tag "Accounts" and all the Computers, Groups, Policies, and Users with the Tag are displayed. Another example is you may also want to Tag computers as per locations like New York, San Francisco or Seattle. You can then search for the Tag "New York" and all the Computers, Groups, Policies, and Users with the Tag are displayed.

You can add Tags in any of the following ways:

- Assign Tags directly to Computers, Groups, Policies, Reports, and Users.
- Add Tags on the Tags page.

To search for Tags, go to the *Search* field and enter the Tag name. The following items containing the Tags are displayed:

- Computers
- Groups
- Policies
- Users
- Managed Software
- Incident Reports



Assign Tags

Tags can be created and assigned to Computers, Groups, Policies or Users.

Complete the following steps to create and assign tags:

1. Go to the Computers, Groups, Policies, Reports or User Management page.
2. Click the *Tags* icon for the Computer, Group, Policy, Reports or User.
3. The *Add Tag* dialog is displayed.
4. Start typing the first few characters of the Tag you want to assign.
5. Select if it is a new Ticket, new general Tag or a Location Tag.
6. Click *OK*.

The selected Tag is assigned to the Computer, Group, Policy, Report or User.

Other ways to add Tags to a new Policy:

- Go to *Policies > Add Policy* and add Tags in the *Tags* section.
- Go to *Computers*. Select a Computer, go to *More Actions > Tag* to add tags to Computers.



Manage Tags

You can Edit or Delete tags that were assigned from the Computers, Groups, Policies, or User Management pages. You can also create new Tags.

Complete the following steps to edit Tickets:

1. Click the *Tags* icon on the top-right corner of the Deep Freeze Cloud Console.
2. Hover over and click the *Edit* sign for the particular ticket under *Tickets*.
3. Edit the Ticket.
4. Press *Enter* on the keyboard or click anywhere on the page.

The Ticket is edited.

Complete the following steps to edit general Tags:

1. Click the *Tags* icon on the top-right corner of the Deep Freeze Cloud Console.
2. Hover over and click the *Edit* sign for the particular Tag under general *Tags*.
3. Edit the Tags.
4. Press *Enter* on the keyboard or click anywhere on the page.

The Tag is edited.

Complete the following steps to edit Location Tags:

1. Click the *Tags* icon on the top-right corner of the Deep Freeze Cloud Console.
2. Hover over and click the *Edit* sign for the particular Tag under *Location Tags*.
3. Edit the Tags.
4. Press *Enter* on the keyboard or click anywhere on the page.

The Tag is edited.

Complete the following steps to delete general Tags:

1. Click the *Tags* icon on the top-right corner of the Deep Freeze Cloud Console.
2. Hover over and click the *Delete* sign for the particular Tag under general *Tags*.
3. A message *Do you want to delete this tag?* is displayed.
4. Click *Yes*.

The Tag is deleted.

Complete the following steps to delete Location Tags:

1. Click the *Tags* icon on the top-right corner of the Deep Freeze Cloud Console.
2. Hover over and click the *Delete* sign for the particular Tag under *Location Tags*.
3. A message *Do you want to delete this tag?* is displayed.
4. Click *Yes*.



The Tag is deleted.

Complete the following steps to add general Tags:

1. Click the *Tags* icon on the top-right corner of the Deep Freeze Cloud Console.
2. Click the + sign for *Tags*.
3. Specify the Tags separated by commas. (Accounts, Marketing, Sales).
4. Click *OK*.

The Tags are added to the list of tags.

Complete the following steps to add Location Tags:

1. Click the *Tags* icon on the top-right corner of the Deep Freeze Cloud Console.
2. Click the + sign for *Location Tags*.
3. Select Geography, Building, Floor, or Room.
4. Specify the Tags separated by commas. (New York, Marketing, Sales).
5. Click *OK*.

The Tags are added to the list of tags.



You can drag and drop the general Tags into the Location Tags section. The first time a Location Tag is created, it is classified as Uncategorized. Drag and drop the newly created Location Tag from the Uncategorized section to the appropriate section.





Deep Freeze Administrator Mobile App

This chapter explains how to use the Deep Freeze Administrator Mobile App to deploy and manage computers.

Topics

[Overview](#)

[Deploy Cloud Agent from the Mobile App](#)

[Manage Computers Locally from the Mobile App](#)

[Manage Computers Remotely from the Mobile App](#)



Overview

Deep Freeze Administrator Mobile App allows you to manage your implementation and perform tasks such as deploying the Cloud Agent, Reboot Thawed, Reboot Frozen, and add Tags.

To get started with Deep Freeze Administrator Mobile App:

1. Go to *Utilities > Mobile App*.
2. Scan the QR code for the iPhone or Android to download the app from the store. Alternatively, click *Send me email invitation* to receive an email with detailed instructions.



Deploy Cloud Agent from the Mobile App

The Deep Freeze Administrator Mobile App allows you to deploy the Cloud Agent on local computers directly from your mobile device.

Complete the following steps:

1. Log on to the Deep Freeze Administrator App.
2. Go to www.deepfreeze.com/connect on the computer you want to manage from Deep Freeze Cloud.
3. Click *Scan* on the Deep Freeze Administrator Mobile App.
4. Point the camera on the mobile device at the QR code on the computer screen.
5. Click one of the following options on the Mobile App:
 - > Install Cloud Agent – this command automatically downloads the Cloud Agent on the scanned computer:
 - ~ Click the downloaded file to open the installation wizard.
 - ~ Follow the steps in the wizard to install the Cloud Agent.
 - > Launch Admin Console – this command launches the Deep Freeze Cloud Console and you are automatically signed-in with the credentials provided on the mobile device.
6. Click *Done* on the Deep Freeze Administrator Mobile App.



Manage Computers Locally from the Mobile App

Once the Cloud Agent is installed, the Deep Freeze Administrator Mobile App allows you to manage your computers by scanning the QR Code.

Complete the following steps:

1. Press CTRL+ALT+SHIFT+F7 on the computer where the Cloud Agent is installed.
2. Click *Scan* on the Deep Freeze Administrator Mobile App.
3. Point the camera on the mobile device at the QR code on the screen.
4. Click one of the following options on the Mobile App:
 - > Reboot Thawed / Reboot Frozen
 - > Tag Computer – add a Normal Tag, Ticket or a Location Tag. Click *OK*.
 - > Refresh Policy – to check-in with Deep Freeze Cloud and apply updates to the Policy.



Manage Computers Remotely from the Mobile App

The Deep Freeze Administrator Mobile App can perform various actions on multiple computers.



You can manage multiple computers remotely using the Deep Freeze Administrator Mobile App only if you are using Deep Freeze On Demand.

View Details

Touch the computer name to view the following details:




- Group
- Policy
- Status
- IP Address
- Operating System
- Lasted Reported
- Tags

Filtering by Status, Policy, or Group

The Deep Freeze Administrator Mobile App features a comprehensive set of filters that can help you determine the status of your computers, and to administer them as a group. Filters can include multiple criteria to narrow the results to exactly the computers of interest.

Note that you can apply status, policy, group, and tag filters at the same time.

Applying a status, policy, or group filter to all computers

1. Launch Deep Freeze Administrator Mobile App.
2. Touch the *All Computers*  icon at the bottom of the screen.
3. Touch the *Filter computers*  icon.
4. By default, the Filter screen contains General criteria, Group criteria, Policy criteria, and criteria for specific services. If desired, you can shorten the list of available criteria by selectively removing services from the list:
 - A. Touch the *Filter*  icon.
 - B. Use the menu to select or remove services.
 - C. Close the menu to apply your changes. Only the selected services will add their service-specific criteria options to the Filter screen.




5. Touch to select the criteria you want to apply. You can select multiple criteria if desired, but you can only select one criteria from each category.
6. Touch *Done* to apply the selected criteria.

The filter is applied to all computers and the results are displayed as a list. Criteria used to build the filter are displayed at the top of the list.

Applying a status, policy, or group filter to computers running a particular service

If you are only interested in computers running a particular service, you can use that as a starting point for further filter criteria.

1. Launch Deep Freeze Administrator Mobile App.
2. Touch the appropriate service-specific icon at the bottom of the screen.
3. Touch the *Filter computers*  icon.
4. Touch to select the criteria you want to apply. You can select multiple criteria if desired, but you can only select one criteria from each category.
5. Touch *Done* to apply the selected criteria.



The filter is applied to computers using the selected service and the results are displayed as a list. Criteria used to build the filter are displayed at the top of the list.

Filtering by Tags

The Deep Freeze Administrator Mobile App filter tools also enables you to filter by tag. If needed, you can filter by multiple tags to narrow the results to exactly the computers of interest.

Note that you can apply status, policy, group, and tag filters at the same time.


Applying a tag filter to all computers

1. Launch Deep Freeze Administrator Mobile App.
2. Touch the *All Computers*  icon at the bottom of the screen.
3. Touch the *Tags*  icon.
4. Touch to select the tags you want to use as filter criteria. You can select multiple tags if desired.
5. Touch *Done* to apply the selected criteria.

The filter is applied to all computers and the results are displayed as a list. Criteria used to build the filter are displayed at the top of the list.

Applying a tag filter to computers running a particular service

If you are only interested in computers running a particular service, you can use that as a starting point for further filter criteria.

1. Launch Deep Freeze Administrator Mobile App.
2. Touch the appropriate service-specific icon at the bottom of the screen.
3. Touch the *Tags*  icon.
4. Touch to select the tags you want to use as filter criteria. You can select multiple tags if desired.



5. Touch *Done* to apply the selected criteria.

The filter is applied to computers using the selected service and the results are displayed as a list. Criteria used to build the filter are displayed at the top of the list.

Removing Active Filters

When the The Deep Freeze Administrator Mobile App has active filters, the filter criteria are displayed at the top of the results list.

To remove the active filter, touch the *Remove filter*  icon to the right of the criteria.

Search

Complete the following steps to search by keywords:

1. Launch Deep Freeze Administrator Mobile App on the smartphone.
2. Click the *Search* field.
3. Enter the keyword.

The keyword search results in the following items which can also be filtered by any one criteria:

- Computers
- Tags – click the *Tag* to show all computers where it is assigned.
- Groups – click the *Group* to show all computers in this group.
- Policies

Perform Actions

Complete the following steps to perform various actions from the Deep Freeze Administrator Mobile App.

1. Launch Deep Freeze Administrator Mobile App on the smartphone.
2. Select one or more computers.
3. Click *Actions*.
4. Select one of the following Actions:
 - > General Actions
 - ~ Restart – the selected computers are restarted.
 - ~ Shutdown – the selected computers are shutdown.
 - ~ Wakeup – the selected computers wakeup.
 - ~ Upgrade Services – upgrades the services on the selected computers to the latest version.
 - ~ Delete Computers – deletes the computers from the database.
 - ~ Send Message – sends a message to the selected computers. Specify a message and click *Send*.
 - ~ Lock Keyboard and Mouse – locks the keyboard and mouse on the selected computers.



- ~ Unlock Keyboard and Mouse – unlocks the keyboard and mouse on the selected computers.
- ~ Send Message – enter the message and click *Send*. The message is sent to the selected computers.
- ~ Run Windows Updates – Windows Updates are downloaded and applied on the selected computers.
- ~ End Workstation Task – Ongoing Workstation Tasks are ended.
- ~ Add Tag – enter the Tags and click *OK*.
- > Deep Freeze – provides the following options:
 - ~ Reboot Thawed – the selected computers are rebooted into a Thawed State.
 - ~ Reboot Frozen – the selected computers are rebooted into a Frozen State.
 - ~ Reboot Thawed Locked – the selected computers are rebooted into a Thawed Locked State.
- > WINSelect – provides the following options:
 - ~ Enable Protection – enables WINSelect protection on the selected computers.
 - ~ Disable Protection – disables WINSelect protection on the selected computers.
- > Anti-Executable – provides the following options:
 - ~ Enable Protection – enables Anti-Executable protection on the selected computers.
 - ~ Disable Protection – disables Anti-Executable protection on the selected computers.
 - ~ Enable Maintenance Mode – enables Maintenance Mode on the selected computers.
- > Anti-Virus – provides the following options:
 - ~ Scan – initiate a Quick Scan, Deep Scan or Abort, Resume and Pause an ongoing scan.
 - ~ Fix Now – downloads the latest virus definition and scans the selected computers.
 - ~ Enable Firewall – enables the firewall on the selected computers.
 - ~ Disable Firewall – disables the firewall on the selected computers.
 - ~ Enable Active Protection – enables the Active Protection.
 - ~ Disable Active Protection – disables the Active Protection.
- > Power Save – provides the following options:
 - ~ Enable Power Management – enables power management on the selected computers.
 - ~ Disable Power Management – disables power management on the selected computers.



- ~ Assign Energy Consumption Profiles – assign pre-defined Energy Consumption Profiles to selected computers.



On iOS, use the *Select* option to select multiple computers. On Android, click and hold to select multiple computers.

Swipe Menu Options

Click the top left corner on the Deep Freeze Administrator Mobile App. This will show the swipe menu with the following options:

- Computers – shows the computers managed by Deep Freeze Administrator.
- Scan QR Code – scans the QR code on the computer.
- Sites – shows the selected site. You can switch between sites.
- Preferences – set the option to *Launch Scanner on Startup* or Logout.
- Feedback – provide your feedback regarding Deep Freeze Administrator Mobile App.





Handout

This chapter explains how to use Handout and handout documents between Teachers and Students.

Topics

[Overview](#)

[Install, Enable and Disable Handout](#)

[Managing a Class](#)

[Handout files to a Class](#)



Overview

Handout allows Teachers to handout documents to Students in a class. Handout integrates with Google Drive to manage handout of documents.

With the Handout feature, you can create a class, add Teachers to the class, add Students to the class and handout files with the entire class.

The Handout feature has the following components:

- Administrator – the Administrator for Deep Freeze Cloud.
- Teacher – the Teacher is the administrator for the Class. The Teacher can handout files using Handout.
- Student – the Students are added by the Administrator.
- Class – a group of students who are part of the Class.



Handout is applicable per Site. If you have multiple Sites, you must enable Handouts for each Site.



Install, Enable and Disable Handout

Install Handout

Only the Deep Freeze Cloud Administrator or Super Administrator can install Handout.

You can install Handout in two ways:

1. Log on to Deep Freeze Cloud.
2. Go to Handout.
3. Select *Enable Handout*. Select one of the following options:
 - > If you know the Google Admin Console Credentials for your Google Apps for Work account, click *Install Now*.
 - ~ Enter the User name, Password, and click *Sign in*.
 - ~ Accept the Terms and Conditions.
 - ~ Click *Accept*.
 - > If you do not have the Google Admin Console Credentials for your Google Apps for Work account, you can send the instructions to your Google Apps for Work administrator by clicking *Email Instructions*. Your administrator can integrate Handouts with Google Apps.

Enable Handout

Only the Deep Freeze Cloud Administrator or Super Administrator can enable Handout.

You can enable Handout in the following way:

1. Log on to Deep Freeze Cloud.
2. Go to Handout.
3. Select *Enable Handout*. Select one of the following options:

Disable Handout

Only the Deep Freeze Cloud Administrator or Super Administrator can disable Handout.

You can disable Handout with the following steps:

1. Log on to Deep Freeze Cloud.
2. Go to Handout.
3. Clear *Enable Handout* checkbox.



Handout is applicable per Site. If you have multiple Sites, you must disable Handouts for each Site.

Remove Handout Completely

For Handouts to be completely disabled, the Google Apps for Work Super Administrator must remove Handouts from Google Marketplace.



Managing a Class

A class consists of Teachers and Students. The first step is to create a class.

For Administrators

Creating a Class

Deep Freeze Administrators can manage Teachers and create a class.

Complete the following steps to create a class:

1. Log on to Deep Freeze Cloud.
2. Go to Handout.
3. Go to *Classroom* > *Create Class*.
4. Specify the *Class Name*.
5. Click *Add Teachers*.
 - > Specify the *First Name*.
 - > Specify the *Last Name*.
 - > Specify the *Email*.
 - > Permission is *Teacher Administrator* by default.
 - > Select the Sites.
 - > The *Handout* action is allowed by default.
 - > Click *OK*. (If you need to add multiple Teachers, click *Add Teachers* and repeat the process.)
6. Select one or more *Teachers*.
7. Enter the email addresses of the students in the *Add Students* field. (The email addresses will appear only if they are part of the Google Contact list.)
8. Click *Create Class*.

The class is created with the Teachers and Students.



A Teacher can also be added by the Deep Freeze Cloud Administrator from User Management page. The Super Administrator must enable Handouts in *Custom Actions* for the Teacher to enable Handouts.

Disabling Teachers from a Class

Complete the following steps to disable a Teacher from a class:

1. Log on to Deep Freeze Cloud as an Administrator or Super Administrator.
2. Go to Handout.
3. Go to *Change Class* > *[Class Name]* > *Edit*.
4. Clear the checkbox for the particular Teacher.



5. Click *OK*.
- The Teacher is disabled.

Deleting a Class

Complete the following steps to delete a class:

1. Go to Handout.
2. Go to *Change Class* > *[Class Name]*
3. Click *Edit Class*.
4. Click *Delete Class*.
5. Click *Yes*.

The class is deleted.

Editing a Class

Complete the following steps to edit a class:

1. Go to Handout.
2. Go to *Change Class* > *[Class Name]*
3. Click *Edit Class*.
4. Edit as required.
5. Click *Save*.

For Teachers

Creating a Class

If you are a Teacher, you can create your own class.

Complete the following steps to create a class:

1. Log on to Deep Freeze Cloud.
2. Go to Handout.
3. Go to *Change Class* > *Create Class*.
4. Specify the *Class Name*.
5. Enter the email addresses of the students in the *Add Students* field. (The email addresses will appear only if they are part of the Google Contact list.)
6. Click *Create Class*.

The class is created with the Students.

Deleting Students from a class

Complete the following steps to delete Students from your own class:

1. Go to Handout.
2. Go to *Change Class* > *[Class Name]*.
3. Select the Students.



4. Click [X].
 5. Click OK.
- The Student is deleted.

Editing a Class

Complete the following steps to edit a class:

1. Go to Handout.
2. Go to *Change Class* > [Class Name]
3. Click *Edit Class*.
4. Edit as required.
5. Click *Save*.

Deleting a Class

Complete the following steps to delete a class:

1. Go to Handout.
2. Go to *Change Class* > [Class Name]
3. Click *Edit Class*.
4. Click *Delete Class*.
5. Click *Yes*.

The class is deleted.



Handout files to a Class

Once a class has been created with Students and Teachers, you can handout files to the entire class.

Complete the following steps to handout files:

1. Log on to Deep Freeze Cloud as a Teacher.
2. Go to Handout.
3. Go to *Change Class* > *[Class Name]*.
4. Select the Students.
5. Click *Handout* icon. You can hand out files in two ways:
 - > Computer: Click *Select files from your computer*. Browse to select the file or drag and drop the file.
 - > Google Drive: Click *Select files from Google Drive*. Select the files and click *Insert*.
6. Select *Send copy to myself* to send a copy of the file to yourself (Teacher).
7. Select *Notify users via email to notify the receivers* and click *Add Message*. Enter a message.
8. Click *Send*.

The files are visible in Google Drive in a folder that is the Teacher's name.



Usage Stats

This chapter describes how to manage software assets using the Usage Stats feature.

Topics

[Usage Stats Overview](#)

[Manage Software Assets](#)

[Pre-defined Products Supported by Usage Stats](#)



Usage Stats Overview

Usage Stats not only allows you to manage software assets in your organization, it also allows you to monitor compliance with software licenses and the usage of computers and applications in your organization.



Select *Enable Usage Stats* in the policy and apply this policy to all computers. Without the Usage Stats service, Deep Freeze Cloud cannot monitor software assets on your network.

Click *Usage Stats* page. The following widgets are displayed:

- Computer Usage – computer usage graph that can be sorted by log in or user.
- Top Utilized Applications – list of the most utilized software. Shows which applications have the highest total usage, in terms of duration (across all computers and users), number of unique users and number of sessions (across all computers and users).
- Top Managed Software – managed software actively used by users and the number of computers where the software is installed.
- Most Over-Utilized Licenses – licenses that are deployed over the allowed numbers. This widget shows a bar graph of the licenses that are over-utilized. The over-utilization percentage is calculated as *(License Utilized minus License Entitled)* divided by the *License Entitled*. The red portion of the bar graph shows the licenses over-utilized.
- Most Under Utilized Licenses – licenses that are under-utilized. Shows the software programs whose under utilization count *(License Entitled minus License Utilized)* is the highest. The blank part of the bar graph shows the licenses unutilized and the green part shows the licenses that are utilized.
- Software License Compliance – % of software programs that are compliant vs. that are not compliant. If the license entitlement is greater than the number of computers where the software is installed, it is compliant. If the license entitlement is less than the number of computers where the software is installed, it is non-compliant. Click the red portion of the widget to show the list of software that is non-compliant. Click the green portion of the widget to show the list of software that is compliant.
- Software License Utilization – shows the *Licenses Utilized / Licenses Entitled*.

The data for the above widgets are displayed based on the settings on the [Manage Software Assets](#) page.



Manage Software Assets

The Manage Software Assets page allows you to selectively manage the software programs installed on your computers.



Usage Stats detects pre-defined products supported by Deep Freeze Cloud, as well as any other software installed on the managed computers. For a list of pre-defined products, go to [Pre-defined Products Supported by Usage Stats](#).

Complete the following steps to configure the details of each software program:

1. Go to *Usage Stats > Manage Software Assets*.
2. Click *Edit Software List*.
3. Select or specify values for the following:
 - > Manage – select the software program to be managed by Usage Stats.
 - > Product Name – the name is not editable.
 - > License Type – select whether the license is by Node, User, Concurrent or Freeware.
 - > License Term – select whether the license is Perpetual or Subscription.
 - > Valid Until – if you select Subscription license term, specify the date when the subscription expires.
 - > Licenses – specify the number of licenses.
 - > License Keys – specify the license keys for the particular program selected.
 - > Description – enter a description of maximum 500 words. The Description is optional.
 - > Tags – add a Tag to the particular software program.
4. Click *Save*.



Usage Stats has the following scan frequency:

- 1st Scan – 5 minutes after Usage Stats Service is installed.
- Ongoing Scans – every 24 hours.
- Re-scan – when the policy is reapplied.



When the title of the *Product Name* column is clicked, the Managed Software is sorted alphabetically first followed by the unmanaged software.



Pre-defined Products Supported by Usage Stats

The following pre-defined products can be tracked by Usage Stats:

- Adobe Acrobat X Pro
- Adobe Acrobat XI Pro
- Adobe Audition CS5.5
- Adobe Audition CS6
- Adobe Creative Suite 6 Master Collection
- Adobe Dreamweaver CS3
- Adobe Dreamweaver CS4
- Adobe Dreamweaver CS5
- Adobe Dreamweaver CS5.5
- Adobe Dreamweaver CS6
- Adobe Photoshop CS2
- Adobe Photoshop CS3
- Adobe Photoshop CS4
- Adobe Photoshop CS5
- Adobe Photoshop CS5.1
- Adobe Photoshop CS6
- Microsoft Office Basic 2007
- Microsoft Office Enterprise 2007
- Microsoft Office Home and Business 2010
- Microsoft Office Home and Business 2013
- Microsoft Office Home and Student 2007
- Microsoft Office Home and Student 2010
- Microsoft Office Home and Student 2013
- Microsoft Office Personal 2013
- Microsoft Office Professional 2007
- Microsoft Office Professional 2010
- Microsoft Office Professional 2013
- Microsoft Office Professional Academic 2013
- Microsoft Office Professional Edition 2003
- Microsoft Office Professional Plus 2007
- Microsoft Office Professional Plus 2010
- Microsoft Office Professional Plus 2013
- Microsoft Office Standard 2007
- Microsoft Office Standard 2010
- Microsoft Office Standard 2013
- Microsoft Office Ultimate 2007



Mobile Device Management

This chapter explains how to setup and use the Mobile Device Management (MDM) feature in Deep Freeze Cloud.

Topics

- [Mobile Device Management \(MDM\) Overview](#)
- [Pre-defining Settings](#)
- [Enrolling and Removing Mobile Devices](#)
- [Managing Apps](#)
- [Managing Groups](#)
- [On-Demand Actions](#)
- [Setting Restrictions](#)
- [Mobile Kiosks](#)
- [Frequently Asked Questions](#)



Mobile Device Management (MDM) Overview

Deep Freeze Mobile Device Management (MDM) enables you manage your iOS, Android, and Chromebook devices using the Deep Freeze Cloud Console web interface. Depending on what types of mobile devices you manage, the MDM can automatically install apps, restrict the device to only use a single app, lock out selected administrative functions, prevent the removal of apps, enforce passcode requirements, track the device's location, update the operating system, lock and unlock the device, prevent the device from accessing social media sites, and more.

What features and operations are available for a given device depend on the device type.

MDM Features for iOS Devices

Deep Freeze MDM can be used to manage iOS devices running iOS 9.0 or higher.

- Apple Device Enrollment Program – The Device Enrollment Program (DEP) helps businesses easily deploy and configure iOS devices. Deep Freeze MDM integrates with DEP. For more information, see [Enrolling iOS DEP Devices](#).
- Apple Volume Purchase Program – The Volume Purchase Program (VPP) makes it simple to find, buy, and distribute apps bulk for your organization. And you can get custom B2B apps for iOS that are built uniquely for you by third-party developers and procured privately through the VPP store. Deep Freeze MDM can deploy apps from VPP store.

For more information on VPP and VPP-managed distribution, visit one of the following websites:

- > Apple Deployment Programs Help
<https://help.apple.com/deployment/business/>
- > Volume Purchase Program for Business
<https://www.apple.com/business/vpp/>
- > Apple School Manager Help
<https://help.apple.com/schoolmanager/>
https://docs.jamf.com/9.9/casper-suite/administrator-guide/User-Based_VPP_Assignments.html
- Install Apps – install apps remotely from Apple App Store across all your mobile devices. For more information, see [Adding iOS apps](#).
- Create Groups – create groups to manage multiple mobile devices to deploy apps, settings and restrictions to all devices within the group. For more information, see [Managing Groups](#).
- Configure settings – configure settings such as wireless access points, proxy, web clip, and wallpapers on the mobile devices remotely. For more information, see [On-Demand Actions](#).
- Set restrictions – set restrictions on the mobile devices defining what the end users is not allowed to do, such as launching the camera. For more information, see [Setting Restrictions](#).



- Send a message – send a message to the mobile device from the Deep Freeze Cloud Console web interface. For more information, see [Sending Messages to Devices](#).
- Wipe mobile devices – retired or lost devices can be wiped remotely to ensure data security. For more information, see [Wiping a Device](#).
- Dynamic widgets – monitor various parameters about the mobile devices with dynamic, interconnected widgets. Log on to Deep Freeze Cloud and go to the MDM page to see the widgets.
- Alerts – set alerts for various security issues on mobile devices to notify administrators immediately.

MDM Features for Android devices

Deep Freeze MDM can be used to manage Android devices running Android 5.0 or higher.

- Google Android for Work (AfW) – This is a feature developed by Google to make Android devices corporate-ready. AfW provides several features and configurations, which secure the device and make the device cater to the needs of an organization. Deep Freeze MDM integrates with Google Android for work. For more information, see [Enrolling an Android Device as a Work-managed Device](#).
- Install Apps – install apps remotely from Google Play Store across all your mobile devices. For more information, see [Adding Apps from the Google Play Store](#).
- Create Groups – create groups to manage multiple mobile devices to deploy apps, settings and restrictions to all devices within the group. For more information, see [Managing Groups](#).
- Configure settings – configure settings such as wireless access points, proxy, web clip, and wallpapers on the mobile devices remotely. For more information, see [On-Demand Actions](#).
- Set restrictions – set restrictions on the mobile devices defining what the end users is not allowed to do, such as launching the camera. For more information, see [Setting Restrictions](#).
- Send a message – send a message to the mobile device from the Deep Freeze Cloud Console web interface. For more information, see [Sending Messages to Devices](#).
- Wipe mobile devices – retired or lost devices can be wiped remotely to ensure data security. For more information, see [Wiping a Device](#).
- Dynamic widgets – monitor various parameters about the mobile devices with dynamic, interconnected widgets. Log on to Deep Freeze Cloud and go to the MDM page to see the widgets.
- Alerts – set alerts for various security issues on mobile devices to notify administrators immediately.

MDM Features for Chromebooks

Deep Freeze MDM can be used to manage Chromebooks in conjunction with G Suite administration tools.

- Disable/re-enable device
- Filter websites using blacklists or whitelists
- Block YouTube content based on category, channel, or URL



- Require devices to use SafeSearch
- Push messaging
- Move devices between organizational groups
- Vary device's active policy based upon weekly schedule and/or device IP address

To manage Chromebooks using the Deep Freeze MDM, you require a G Suite account with a subscription to a Chrome service, and enough subscription licenses to cover the devices you want to manage.



Pre-defining Settings

Before you start adding mobile devices to the system, you may want to take the time to pre-define certain settings so that they can be easily applied and edited when the time comes. Note that these procedures are optional—if you do not pre-define options for a setting, you can still define those settings manually during group creation (except HTTP proxies and Wallpapers)—but they can save you time if you are deploying a large network of mobile devices.

Note that you can edit pre-defined settings at any time. Changes made to a pre-defined setting are propagated to all groups using that setting.

- [Pre-defining Wireless Networks](#) (iOS and Android)
- [Pre-defining Global HTTP Proxies](#) (iOS)
- [Pre-defining Web Clips](#) (iOS and Android)
- [Pre-defining Wallpapers](#) (iOS and Android)
- [Pre-defining Email Settings](#) (iOS)
- [Pre-defining Certificates](#) (iOS)

Pre-defining Wireless Networks

You can pre-define wireless network settings for your enrolled devices, allowing them to connect seamlessly to those networks. Enrolled devices are not limited to connecting only to pre-defined wireless networks, however; they can still connect to other networks, but the user will have to manually select the network and provide authentication (if they have permission to access such settings).

Before you can add wireless networks to groups, you must first configure them. Configured networks are compatible with both iOS and Android, but note that some settings, including all security protocol settings, are only applicable to iOS and will be ignored by Android devices. This means that you can configure iOS devices to connect to a wireless network using a password, but not Android devices.

Adding a new wireless network

1. Go to *MDM > Settings*.
2. Click the *Configurations* tab if it is not already selected.
3. Locate the *Wireless Network* list. Click the *Add* button at the right of the list.
A Wireless Network window opens.
4. Define the wireless network properties:
 - > Name – use this field to define a name for the wireless network. The name is used only within the Deep Freeze Cloud Console for identification and will not be visible to device users.
 - > Wireless network name (SSID) – enter the name (SSID) of the wireless network into this field.
 - > Is the network hidden? – select this option if the wireless network is a hidden network.



- > Private Wi-Fi Address – turn Private Wi-Fi Address on and off. Selecting to turn this option off disables the device from using a unique private network address on each Wi-Fi network it joins. Note that this option is set to On for new connections by default.
- > Proxy Type – Use this field to select a proxy, if required. If you select *Automatic*, you must provide the proxy URL. If you select *Manual*, you must provide a server address and port, and login credentials.

This setting, and any additional fields that appear as a result of your selection, are only applicable to iOS devices.



- > Security Type – Use this field to select the network's security protocol. Depending on what protocol you select, additional fields may appear. For example, if you select *WEP*, a *Password* field appears so you can define a password for authentication.

This setting, and any additional fields that appear as a result of your selection, are only applicable to iOS devices.

5. Click OK.

Editing or deleting an existing wireless network

Any changes or deletions you make to existing wireless networks will propagate to groups and devices using those networks.

1. Go to *MDM > Settings*.
2. Click the *Configurations* tab if it is not already selected.
3. Scroll through the list of wireless networks and locate the one you want to edit or delete.
4. Edit or delete the network as needed:
 - > To edit the network, click the associated  icon in the *Actions* column of the table.
 - > To delete the network, click the associated  icon in the *Actions* column of the table.

Pre-defining Global HTTP Proxies

A Global HTTP Proxy is an optional server that stands as a middleman between the devices and the internet. To use the proxy server, devices must be configured to connect to it. You can pre-configure global HTTP proxy settings and apply them to groups, so that all devices within those groups connect to the same proxy or proxies.

Global HTTP proxy settings can only be applied to iOS devices.

Adding a new Global HTTP proxy

1. Go to *MDM > Settings*.
2. Click the *Configurations* tab if it is not already selected.
3. Locate the *Global HTTP Proxy* list. Click the *Add* button at the right of the list.

A Global HTTP Proxy window opens.

4. Define the proxy properties:
 - > Name – use this field to define a name for this configuration. This is purely an identifier, and will not be visible to users.





- > Proxy Type – use this field to select the nature of the proxy server settings. Select *Manual* to define the proxy server settings manually, *Automatic* to allow devices to detect and adapt proxy settings automatically, or *None* to disable proxy servers.
- > Server – enter the URL of the proxy server into the field.
This field is only relevant if the Proxy Type is set to Manual.
- > Server port- enter the port used to access the proxy server into this field.
This field is only relevant if the Proxy Type is set to Manual.
- > User name – enter the user name required to access the proxy server into this field.
This field is only relevant if the Proxy Type is set to Manual.
- > Password – enter the password required to access the proxy server into this field.
This field is only relevant if the Proxy Type is set to Manual.
- > Proxy PAC URL- enter the location of the proxy auto-configuration file into this field.
This field is only relevant if the Proxy Type is set to Automatic.
- > Allow PAC Fallback- select this option to permit devices to connect directly if the Proxy PAC URL is unreachable.
- > Allow Captive Login- select this option to permit devices to bypass the proxy when connecting to known networks.

5. Click OK.

Editing or deleting an existing global HTTP proxy

Any changes or deletions you make to existing global HTTP proxies will propagate to groups and devices using those proxies.

1. Go to *MDM > Settings*.
2. Click the *Configurations* tab if it is not already selected.
3. Scroll through the list of Global HTTP Proxies and locate the one you want to edit or delete.
4. Edit or delete the proxy settings as needed:
 - > To edit the proxy, click the associated  icon in the *Actions* column of the table.
 - > To delete the proxy, click the associated  icon in the *Actions* column of the table.

Pre-defining Web Clips

Web Clips are optional web links you can add to enrolled devices, appearing as icons on the home screen. When opened, the device's default browser opens to a pre-configured URL.

Before you can add Web Clips to groups, you must first configure them. The configuration procedure depends on whether the clip is meant for iOS or Android devices.

Adding a new iOS Web Clip

1. Go to *MDM > Settings*.
2. Click the *Configurations* tab if it is not already selected.
3. Locate the *Web Clip* list. Click the *Add* button at the right of the list.



A Web Clips window opens.


4. Click the *iOS* icon
5. Define the Web Clip properties:
 - > Label – use this field to define the label for the Web Clip, i.e., the text that appears under the icon. Visible to device users.
 - > URL – use this field to define the destination URL for the Web Clip.
 - > Removable by User – select this option to allow device users to delete the Web Clip from their device.
 - > Icon – the icon image associated with the Web Clip. To define an image, click *Choose Image* to open a file browser, and use it to select an 59 x 60px PNG image file. If no image is defined, devices will display a white square instead.
 - > Full Screen – select this option to have the Web Clip open in full screen mode (i.e., the browser menu bar and toolbars will not be displayed).
6. Click *OK*.

Adding a new Android Web Clip

1. Go to *MDM > Settings*.
2. Click the *Configurations* tab if it is not already selected.
3. Locate the *Web Clip* list. Click the *Add* button at the right of the list.
A Web Clips window opens.
4. Click the *Android* icon
5. Define the Web Clip properties:
 - > Label – use this field to define the label for the Web Clip, i.e., the text that appears under the icon. Visible to device users.
 - > URL – use this field to define the destination URL for the Web Clip.
 - > Removable by User – select this option to allow device users to delete the Web Clip from their device.
 - > Icon – the icon image associated with the Web Clip. To define an image, click *Choose Image* to open a file browser, and use it to select a square PNG image file between 96 x 96 and 192 x 192 pixels in size.
 - > Full Screen – select this option to have the Web Clip open in full screen mode (i.e., the browser menu bar and toolbars will not be displayed).
6. Click *OK*.

Editing or deleting an existing Web Clip

Any changes or deletions you make to existing Web Clips will propagate to groups and devices using those Web Clips.

1. Go to *MDM > Settings*.
2. Click the *Configurations* tab if it is not already selected.
3. Scroll through the list of Web Clips and locate the one you want to edit or delete.
4. Edit or delete the Web Clip as needed:
 - > To edit the Web Clip, click the associated  icon in the *Actions* column of the table.



- > To delete the Web Clip, click the associated ✕ icon in the *Actions* column of the table.

Pre-defining Wallpapers

Wallpapers are sets of background images that can be applied to enrolled devices. Each Wallpaper consists of two images—a home screen background, and a lock screen background—although both images can be the same if desired.

Before you can add Wallpapers to groups, you must first configure them. Wallpapers are available for both iOS and Android devices.

Adding a new Wallpaper

1. Go to *MDM > Settings*.
2. Click the *Configurations* tab if it is not already selected.
3. Locate the *Wallpaper* list. Click the *Add* button at the right of the list.
A Wallpaper window opens.
4. Define the Wallpaper properties:
 - > Name – use this field to define a name for the Wallpaper. The name is used only within the Deep Freeze Cloud Console for identification and will not be visible to device users.
 - > Home Image – the background image for the home screen. To define an image, click *Choose Image* to open a file browser, and use it to select a PNG image file.
 - > Use same image for both – select this option to use the Home Image as the background for both the home screen and lock screen. If selected, the contents of the Lock Image field will be ignored.
 - > Lock Image – the background image for the lock screen. To define an image, click *Choose Image* to open a file browser, and use it to select a PNG image file.

Note that if the *Use same image for both* option is enabled, this field is ignored.
5. Click *OK*.

Editing or deleting an existing Wallpaper

Any changes or deletions you make to existing Wallpapers will propagate to groups and devices using those Wallpapers.

1. Go to *MDM > Settings*.
2. Click the *Configurations* tab if it is not already selected.
3. Scroll through the list of Wallpapers and locate the one you want to edit or delete.
4. Edit or delete the Wallpaper as needed:
 - > To edit the Wallpaper, click the associated ✎ icon in the *Actions* column of the table.
 - > To delete the Wallpaper, click the associated ✕ icon in the *Actions* column of the table.



Pre-defining Email Settings

There are certain applications in which it is desirable for multiple devices to have the same email settings, such that all devices use the same email account. You can pre-define these settings to make the process easier.

Adding a new email configuration



1. Go to *MDM > Settings*.
2. Click the *Configurations* tab if it is not already selected.
3. Locate the *Email Settings* list. Click the *Add* button at the right of the list.
An Email Settings window opens.
4. Click the *Account Info* tab if it is not already selected.
5. Define the general settings for the email account:
 - > Account Description – use this field to define a name or short description for the email settings. The name is used only within the Deep Freeze Cloud Console for identification and will not be visible to device users.
 - > Account Type – use this field to select the type of email account.
 - > User Display Name – use this field to define a display name for the email account, visible to the account user and anybody who receives a message from the account.
 - > Email – enter the account email address into this field.
 - > Allow user to move messages from this account – enable this option to permit users to move messages between different email accounts on the same device.
 - > Allow recent address to be synced – enable this option to permit devices to sync new email addresses from recent messages to iCloud.
 - > Allow mail drop – enable this option to enable Mail Drop, which permits users to send large attachments.
 - > Use only in Mail – normally, the email settings you define here apply to all email clients on the device. Enable this option to apply the email settings only to the iOS Mail app.
6. Click the *Incoming Mail* tab.
7. Define the incoming mail settings:
 - > Mail Server – enter the URL of the incoming mail server into this field.
 - > Port – enter the port used to access the incoming mail server into this field.
 - > User Name- enter the credentials required to access the incoming mail server into this field.
 - > Authentication Type – use this field to select which type of authentication is required to access the mail server.
 - > Password – if the email server requires a password, enter it here.
 - > Use SSL – select this option to enable Secure Socket Layer.
8. Click the *Outgoing Mail* tab.
9. Define the outgoing mail settings:
 - > Mail Server – enter the URL of the outgoing mail server into this field.
 - > Port – enter the port used to access the outgoing mail server into this field.



- > User Name- enter the credentials required to access the outgoing mail server into this field.
- > Authentication Type – use this field to select which type of authentication is required to access the mail server.
- > Password – if the email server requires a password, enter it here.
- > Outgoing password same as incoming – select this option if the password for the outgoing mail server is the same as the incoming mail server, as defined in the Incoming Mail tab.
- > Use SSL – select this option to enable Secure Socket Layer.

10. Click *OK*.

Editing or deleting an existing email configuration

1. Go to *MDM > Settings*.
2. Click the *Configurations* tab if it is not already selected.
3. Scroll through the list of email configurations and locate the one you want to edit or delete.
4. Edit or delete the email configuration as needed:
 - > To edit the email configuration, click the associated  icon in the *Actions* column of the table.
 - > To delete the email configuration, click the associated  icon in the *Actions* column of the table.

Pre-defining Certificates

Devices may require certain certificates to access specific resources on the internet. You can use Deep Freeze Cloud Console to push useful certificate files to your iOS devices, and you can pre-define these certificates to make the process easier to manage.



Adding a new certificate

1. Go to *MDM > Settings*.
2. Click the *Configurations* tab if it is not already selected.
3. Locate the *Certificates* list. Click the *Add* button at the right of the list.
An Upload Certificate window opens.
4. Define the certificate properties:
 - > Name – use this field to define a name for the certificate. The name is used only within the Deep Freeze Cloud Console for identification and will not be visible to device users.
 - > Type – use this field to select the certificate type.
 - > Certificate File – the certificate file. To define a file, click *Choose File* to open a file browser, and use it to select the certificate.
 - > Password – some certificates require a password to use. If a password is necessary, enter it into this field.

Note that this field is only visible if the certificate Type is defined as PKCS12.
5. Click *Upload*.



Editing or deleting an existing certificate

1. Go to *MDM > Settings*.
2. Click the *Configurations* tab if it is not already selected.
3. Scroll through the list of certificates and locate the one you want to edit or delete.
4. Edit or delete the certificate as needed:
 - > To edit the certificate, click the associated  icon in the *Actions* column of the table.
 - > To delete the certificate, click the associated  icon in the *Actions* column of the table.



Enrolling and Removing Mobile Devices

Before a device can be managed by Deep Freeze MDM, it must be enrolled to establish communication between the device and the Deep Freeze Cloud Console. How you enroll a device depends on device type (iOS, Android, or Chromebook), and some device types have multiple enrollment options.

iOS

iOS devices can be enrolled in two ways based on your requirements:

DEP Device

DEP devices are registered in the Apple's Device Enrollment Program (DEP). DEP allows you to make MDM enrollment mandatory and unremovable, and also automatically installs Deep Freeze Cloud MDM during the initial device setup.

BYOD device

A BYOD device allows the user to have complete control over the mobile device. The mobile device user can install or uninstall apps or change settings as required.

Android

Android devices can be enrolled in two ways based on your requirements:

Work-Managed Device

A work-managed device allows the IT administrator to have full control over the device. A work-managed device can be configured to only allow specific apps defined by the administrator to be installed on the device.

User-Owned Device

A user-owned device allows the user to have complete control over the mobile device. The user can install or uninstall apps or change settings as required.

Chromebook

All Chromebooks are added to the system in the same manner: when Deep Freeze Cloud Console is synced to a G Suite account, all Chromebooks in that account are provisioned within the system. Deep Freeze Cloud Console has limited control over Chromebooks, but note that enrolled Chromebooks can still be managed using G Suite administrative tools.

Enrolling iOS Devices

iOS devices can be enrolled as a DEP device or a BYOD device. The following sections provide detailed steps.



Enrolling iOS DEP Devices

DEP devices are registered in the Apple's Device Enrollment Program (DEP). The advantage of a DEP device is the Deep Freeze MDM settings can be directly pushed to the device during initial device setup. Even when the mobile device is reset, the settings are pushed to the device again during setup.

Configuring a DEP device has three stages:

- [Creating an Apple Push Certificate](#) – to connect Deep Freeze MDM with Apple Enterprise Mobile Management.
- [Configuring a DEP MDM Server](#) – to connect Deep Freeze MDM to Apple Enterprise Mobile Management for DEP devices.
- [On Device Setup](#) – to connect the device to Deep Freeze MDM and receive notifications and provide the ability to track the device.

Creating an Apple Push Certificate

The first step to connect the Deep Freeze MDM with Apple Enterprise Mobile Management by creating an Apple Push Certificate and uploading to Deep Freeze MDM.

Complete the following steps:

1. Go to *MDM > Settings > Push Certificate*.
2. Click *Certificate Request* to download the Certificate Request. Save it on your computer.
3. Go to Apple Push Certificate Portal (<https://identity.apple.com/pushcert/>) and sign in with your Apple ID and password.
4. Click *Create a Certificate*. Select *I have read and agree to these terms and conditions* and click *Accept*.
5. Click *Choose File*. Browse to select the *Certificate Request* file (.csr) from Deep Freeze MDM and click *Open*.
6. Click *Upload*. The message *You have successfully created a new push certificate with the following information:* is shown.
7. Click *Download* to download the Apple Push Certificate (.pem) and save it on your computer.
8. Go to *Deep Freeze Cloud > MDM > Settings > Push Certificate*.
9. Click *Choose File*. Browse to select the *Apple Push Certificate* file and click *Open*.
10. Specify the Apple ID.
11. Click *Upload*.

Deep Freeze MDM is now connected to Apple Enterprise Mobile Management.

Configuring a DEP MDM Server

Device Enrollment Program (DEP) is for devices purchased directly from Apple and owned by your organization.

Complete the following steps to configure a DEP Server:

1. Go to *Deep Freeze Cloud > MDM > Settings > DEP*.
2. Click *DEP Public Key* to download the public key.
3. Go to <http://deploy.apple.com/> and sign in to your account.



4. Click *Get Started*.
5. Click *Add MDM Server*.
6. Enter a name for your MDM server (for example Deep Freeze MDM – your company name).
7. Click *Choose File*. Browse to select the DEP Public Key downloaded in step 2. Click *Next*.
8. Download the *DEP Server Token*.
9. Go to *Deep Freeze Cloud > MDM > Settings > DEP*.
10. Click *Choose File*. Browse to select the *DEP Server Token*.
11. Click *Upload*.
12. Go to <http://deploy.apple.com/>.
13. Click *Manage Devices*.
14. Click *Choose by Serial Number*. Specify the serial number of your device.
15. Select *Assign to Server* and *select the MDM Server*.
16. Click *OK*.
17. Go to *Deep Freeze Cloud > MDM > Settings > DEP*.
18. Click *Sync with Apple* to refresh
19. Configure the following settings:
 - > General Configuration
 - ~ Initial device group: select the group that the device will belong to. If no group is selected the device will be part of the Default iOS group.
 - ~ Force Deep Freeze MDM enrollment – select this option if this device will be automatically enrolled in Deep Freeze MDM profile and the Deep Freeze MDM app will be automatically downloaded. Clearing this checkbox gives you an option to either *Apply configuration* or *Skip configuration* during initial setup.
 - ~ Place device in Supervised mode – select this option to place this device in Supervised mode. Supervised mode gives more control to the administrator over the device and additional restrictions can be set. Optionally, select *Allow Deep Freeze MDM* removal by user if you want to give the permission to the user to remove the MDM user profile from *Settings > Device Management > Deep Freeze MDM*.
 - ~ Allow pairing with macOS computers – select this option to make the mobile device visible in macOS computers and pair with them. If this option is not selected, the mobile device will not be visible in the Bluetooth settings in your macOS computers.
 - > Organization Details – This information is presented to the user of the device during the setup process:
 - ~ Support phone number – specify the phone number of the support team.
 - ~ Support email address – specify the email address for your support team.
 - ~ Department name – specify the name of the department to which the mobile device user belongs.
 - > Device Naming Scheme – This option controls how supervised devices are renamed. Select one of the following:
 - ~ Default Name – keep devices' default names when they enroll.



- ~ Add prefix to name – rename each device when it enrolls by adding a prefix to its default name. Define the prefix in the *Prefix* field that appears when this option is selected.
- ~ Name devices based on serial numbers – select this option to define custom names for specific serial numbers. Existing and newly enrolled devices are then assigned the name associated with their serial number. Devices with serial numbers that do not have defined names are not affected (they keep their default/existing name).

To use this option, you must create and upload a table that associates names to serial numbers:

- a. Select the *Name devices based on serial numbers* option.
 - b. Click *Download CSV Template*.
 - c. Edit the downloaded template by defining a name for each serial number you add to the table. Remember that you can enter serial numbers for devices that already enrolled as well as those that will enroll in the future.
 - d. Save and close the .csv file.
 - e. Click *Choose File* and use the file browser to select the .csv file.
- Optional Setup Panes – You can choose to skip any of the setup steps below during initial configuration of the mobile device:
 - > Skip passcode setup
 - > Skip location service
 - > Skip restoring from backup
 - > Remove "Move from Android" from restore options
 - > Skip signing in to Apple ID and iCloud
 - > Skip Terms and Conditions
 - > Skip Touch ID setup
 - > Skip Apple Play setup
 - > Skip zoom setup
 - > Skip Privacy pane (iOS 12+)
 - > Skip iMessage and Face Time (iOS 12+)
 - > Skip ScreenTime (iOS 12+)
 - > Skip Software Update (iOS 12+)
 - > Disable Siri
 - > Disable sending diagnostics info

20. Click *Save*.

21. Set up the mobile device (for a new device) or reset the device.



Once the device setup is completed, go to *Deep Freeze Cloud > MDM > Devices* to view the device.



An Apple device can only be assigned to one Apple MDM Server. The Apple device must be assigned to the Apple MDM Server that is connected to Deep Freeze MDM. If the Apple device is assigned to another Apple MDM Server, you must unassign the iOS device and re-assign to the Apple MDM Server that is connected to Deep Freeze MDM.

Enrolling iOS "BYOD" Devices

A BYOD device allows the user complete control on their mobile device. A user can install or uninstall apps or remove the Deep Freeze MDM profile from the settings.

Configuring a mobile device as a BYOD device has two stages:

- [Creating an Apple Push Certificate](#) – to connect Deep Freeze MDM to Apple Enterprise Mobile Management.
- [On Device Setup](#) – to connect the device to Deep Freeze MDM.

Creating an Apple Push Certificate

The first step to connect the Deep Freeze MDM with Apple Enterprise Mobile Management by creating an Apple Push Certificate and uploading to Deep Freeze MDM.

Complete the following steps:

1. Go to *MDM > Settings > Push Certificate*.
2. Click *Certificate Request* to download the Certificate Request. Save it on your computer.
3. Go to Apple Push Certificate Portal (<https://identity.apple.com/pushcert/>) and sign in with your Apple ID and password.
4. Click *Create a Certificate*. Select *I have read and agree to these terms and conditions* and click *Accept*.
5. Click *Choose File*. Browse to select the *Certificate Request* file (.csr) from Deep Freeze MDM and click *Open*.
6. Click *Upload*. The message *You have successfully created a new push certificate with the following information:* is shown.
7. Click *Download* to download the Apple Push Certificate (.pem) and save it on your computer.
8. Go to *Deep Freeze Cloud > MDM > Settings > Push Certificate*.
9. Click *Choose File*. Browse to select the *Apple Push Certificate* file and click *Open*.
10. Specify the Apple ID.
11. Click *Upload*.

Deep Freeze MDM is now connected to Apple Enterprise Mobile Management.

On Device Setup

Complete the following steps to enroll an iOS device:

1. Go to www.deepfreeze.com/Enroll on the mobile device.
2. Enter the Network ID (XXX-XXX-XXXX).



3. Press *Register*.
4. In the profile that appears, press *Install*.
5. Press *Install* again to confirm.
6. A message *Do you trust this profile's source to enroll your iPhone into remote management?* appears. Press *Trust*.

Go to *Deep Freeze Cloud > MDM > Devices* to view the device.

Configuring a Connection to Android for Work

Before you can enroll Android devices, you must configure Deep Freeze Cloud Console's access to the devices' Android for Work profiles. These work profiles are managed either using G Suite or Google Play; which tool you use not only defines what administrative capabilities you have through Google, but also how you must set up the connection to Deep Freeze Cloud Console. In both cases, you are seeking to obtain permission for Deep Freeze Cloud Console to act as the EMM (Enterprise Mobility Management) provider. This allows Deep Freeze Cloud Console to sync with G Suite/Google Play to obtain device information and manage devices using their work profiles.

Configuring a Connection to Android for Work Managed by Google Play

The following instructions describe how to configure Deep Freeze Cloud Console to link to Google Play. Google Play is Android for Work's lower-cost option: ideal for smaller businesses, but with fewer administration options and no unique domain.

1. Go to *MDM > Settings*.
2. Click the *Android for Work* tab.
3. In the *Enrollment Type* drop down list, select *Managed Play Store Account*.
4. Click *Next*.

The browser opens the Google login screen.

5. Provide your user name and password. Click *Next*.

A Google Play window opens.

6. Click *Get Started*.
7. Enter the name of your company into the *Organization Name* field.
8. Enable the *I have read and agree to the managed Google Play agreement* option.
9. Click *Next*.
10. Click *Complete Registration*.

Deep Freeze Cloud Console is now connected to Android for Work, and you can start enrolling Android devices.

Configuring a Connection to Android for Work Managed by G Suite

The following instructions describe how to configure Deep Freeze Cloud Console to link to G Suite. G Suite is Android for Work's premium management option: higher cost, but with more administration options and a customer-defined domain name.



Configuring the connection between Deep Freeze Cloud Console and G Suite is a three step process: unenroll from your existing EMM provider (if needed), generate a new EMM token in G Suite, then configure Deep Freeze Cloud Console.

Step 1: Unenrolling from your existing G Suite EMM provider

Your G Suite account can only have one EMM provider at a time. If you have an existing software package acting as EMM provider, you must first unenroll your devices from that provider and remove its connection to G Suite before you can configure the connection to Deep Freeze Cloud Console.

How to unenroll from your existing provider varies according to provider.

Step 2: Generating a new G Suite EMM token

In order to obtain permission to act as EMM provider, Deep Freeze Cloud Console must be configured with a valid EMM token—essentially a passcode generated by G Suite. You must use the G Suite administration tools to generate a new token.

1. Use your browser to navigate to G Suite for your domain. Log in as an administrator.
2. Open the *Admin* app.
3. Click the *Security* icon.
4. Expand the *EMM provider for Android* options.
5. Enable the EMM provider option if it is not already enabled.
6. Click *Generate Token*.
7. Copy the resulting alphanumeric code for later use.

Step 3: Configuring Deep Freeze Cloud Console as G Suite EMM provider

1. Go to *MDM > Settings*.
2. Click the *Android for Work* tab.
3. In the *Enrollment Type* drop down list, select *Google Managed Domain (G Suite)*. Additional settings appear.
4. Provide values for the following settings:
 - > Domain – enter your G Suite domain into this field.
 - > Administrator Email – enter the email address you use to log into the administrator account into this field.
 - > EMM Token – enter the EMM token value you generated earlier into this field.
5. Click *Enroll*.

Deep Freeze Cloud Console is now connected to Android for Work, and you can start enrolling Android devices.

Enrolling Android Devices

To manage an device, it must be enrolled.

There are two ways you can enroll Android devices: as a user-owned device, which permits the user to retain ultimate control over the device, or as a work-managed device, where Deep Freeze Cloud Console has control over what apps can be installed and what administrative functions are available.



Note that you must configure a connection to Android for Work before you can enroll Android devices.

Selecting the Default Group

When you enroll an Android device, it is automatically assigned to the default group. The same default group applies to both user-managed and work-managed enrollments, but note that you can move devices to a different group at any time.

1. Go to *MDM > Devices*.
2. Click the *Android* icon.
3. Click *Enroll Device*.
4. Use the *Assign to group* field to select a default group. Newly enrolled devices will be placed in this group.

Enrolling an Android Device as a Work-managed Device

Enrolling a device as a work-managed device gives more control to the Deep Freeze Cloud Console administrator. A work-managed device restricts the user from installing apps other than the ones specified by the administrator; only apps specified by the administrator will be visible in the Google Play Store.

Enrolling an Android device as a work-managed device is a two step process: first, the device must be wiped (assuming it is not a brand new device), then it must be enrolled during the initial device setup. There are three methods for enrolling the device: you can enter an enrollment code, you can scan a QR code, or you can enter an activation code. Note that each of these methods has different prerequisites.

Step 1: Reset the device to factory defaults

Unless the device is brand new, out of the box, it will need to be wiped of all user data before it can be configured as a work-managed device.

How to reset the device depends on the model of device – consult the device instructions.

Step 2 (option 1): Enter the DPC Identifier during device setup

To use this method, the device must run Android 6.0 (Marshmallow) or above.

1. Switch on the device, then wait until it displays the initial language selection screen.
2. Select the language you want to operate in.
3. Touch *Start*.
4. In the Wi-Fi screen, select a wireless network and provide the credentials necessary to connect to it. Once you are connected, touch *Next*.
5. Agree to the Terms and Conditions, then touch *Next*.
6. In the Add your account screen, enter *afw#deepfreeze* into the *Email or phone* field. Touch *Next*.
7. Follow the prompts on the device to continue device configuration. If prompted, download and install the Deep Freeze MDM app.
8. In the Enroll in Deep Freeze MDM screen, do one of the following:



- > Enter the enrollment code displayed by the Deep Freeze Cloud Console at *MDM > Devices > Enrollment > Android* under the *Using DPC Identifier* heading, then touch *Enroll this device*.
 - > Touch the camera icon to activate the camera, then use the camera to scan the QR code displayed by the Deep Freeze Cloud Console at *MDM > Devices > Enrollment > Android*, under the *Using DPC Identifier* heading. Note that this page displays two QR codes; the smaller one is required for this procedure.
9. Follow the prompts on the device to complete device configuration.

Step 2 (option 2): Scan the Deep Freeze QR code during device setup

To use this method, the device must run Android 7.0 (Nougat) or above.

1. Switch on the device, and wait until it displays the initial language selection screen.
2. Select the language you want to operate in.
3. Tap the device screen six times. The device displays the QR code setup screen.
4. Touch *Next* to proceed to the Get connected screen.
5. Select a wireless network and provide the necessary credentials to connect to it.
6. Once the device is connected, it will activate the camera. Use the camera to scan the QR code displayed by the Deep Freeze Cloud Console at *MDM > Devices > Enrollment > Android* under the *Using QR Code* heading. Note that this page displays two QR codes; the larger one is required for this procedure.
7. Follow the prompts on the device to complete device configuration.

Step 2 (option 3): Generate and use an activation code to enroll the device

This method is only available to devices running Android 5.x (Lollipop).

1. Go to *MDM > Devices*.
2. Click the *Android* icon.
3. Click *Enroll Device*.
4. Click the *Work Managed Devices* tab.
5. Enter your G Suite administrator email address into the *Enter your work email address* field.
6. Click *Generate*.

Deep Freeze Cloud Console generates a numerical Activation Code and displays it underneath the email address. Record this code; it will be required when enrolling the device. Note that the same code can be used to enroll multiple devices.
7. Switch on the device, then wait until it displays the initial language selection screen.
8. Select the language you want to operate in.
9. Touch *Start*.
10. In the Wi-Fi screen, select a wireless network and provide the credentials necessary to connect to it. Once you are connected, touch *Next*.
11. Agree to the Terms and Conditions, then touch *Next*.
12. In the Add your account screen, touch the menu icon (the three vertical dots at the top right) and select *Set up work device*.



13. Enter the email address you used to generate the activation code into the *Email address* field, and the generated activation code into the *Activation code* field. Touch *Set Up*.
14. You may be prompted to encrypt your device. If so, touch *Encrypt*, then follow the instructions to continue. Note that your device will reboot as part of this process.
15. Follow the prompts on the device to continue device configuration. If prompted, download and install the Deep Freeze MDM app.
16. If the device runs Android 5.0 or 5.1, you must update the Google Play Store before enrolling in Deep Freeze MDM. For other versions of Android, skip this step.
 - A. When the Enroll in Deep Freeze MDM screen appears, skip the enrollment process. Follow the prompts to complete device configuration.
 - B. Launch the Play Store.
 - C. Under the Settings menu, tap *Play Store version*. The Play Store will update itself to the latest version.
 - D. Close the Play Store.
 - E. Open the Deep Freeze MDM app.
17. In the Enroll in Deep Freeze MDM screen, do one of the following:
 - > Enter the enrollment code displayed by the Deep Freeze Cloud Console at *MDM > Devices > Enrollment > Android* under the *Using DPC Identifier* heading, then touch *Enroll this device*.
 - > Touch the camera icon to activate the camera, then use the camera to scan the QR code displayed by the Deep Freeze Cloud Console at *MDM > Devices > Enrollment > Android*, under the *Using DPC Identifier* heading. Note that this page displays two QR codes; the smaller one is required for this procedure.
18. Follow the prompts to complete device configuration.

Enrolling an Android Device as a User-owned Device

Configuring a mobile device as a user-owned device gives more control to the user. The user of the device can install their own apps in addition to the apps installed by the administrator via Deep Freeze MDM.

While devices enrolled as user-owned devices are typically owned by their respective users, nothing prevents you from enrolling company devices as user-owned.

Complete the following steps on the Android device:

1. Go to the *Google Play Store*.
2. Search for *Deep Freeze MDM*.
3. Click *Install*.
4. Launch the Deep Freeze MDM app.
5. Specify the network ID in the format *XXX-XXX-XXXX*. Alternatively, you can also scan the QR code.
6. Click *Enroll this device*.



Sending Android Enrollment Invitation Emails

You can use Deep Freeze Cloud Console to send emails to users inviting them to enroll their Android devices as user-owned. The recipients will receive an email from "Deep Freeze Cloud" containing a URL that they can use to enroll their device. The recipient can also forward the email to other users.

Note that you must configure a connection to Android for Work before you can send enrollment invitations.

1. Go to *MDM > Devices*.
2. Click the *Android* icon.
3. Click *Enroll Device*.
4. Define the email recipients, and edit the content if desired:
 - > Send link via – enter the email addresses of the recipients in this field. Separate addresses using a comma.
 - > Message – The email will display the text in this field directly before the URL used to enroll devices. Edit the text as desired.
5. Click *Send*.

Provisioning Chromebooks

Deep Freeze MDM does not enroll Chromebooks individually. Instead, it syncs to your G Suite account and provisions all Chromebooks administered by the account.

Your G Suite account can only be synced to one Deep Freeze Cloud site. If you manage multiple sites, you will need a separate G Suite account and Chromebook devices for each site.

Granting Deep Freeze MDM Access to your G Suite Directory

To provision the Chromebooks administered by your G Suite account, grant Deep Freeze MDM access to your G Suite directory.

1. Go to *MDM > Devices*.
2. Click the *Chromebook* icon.
3. Click *Grant Access*.
4. Log into G Suite using your super administrator credentials.
5. When prompted to give deepfreeze.com access to your Google account, click *Allow*.
Once Deep Freeze MDM has access to the directory, all Chromebooks managed by your G Suite account are automatically provisioned, and appear in the *MDM > Devices* list.

Provisioning Newly Added Chromebooks

When you add new Chromebooks to your G Suite account, those devices are automatically provisioned the next time the Deep Freeze MDM syncs with your G Suite account.

Deep Freeze MDM automatically syncs to G Suite whenever you log into the Deep Freeze Cloud Console. You can also force a sync at any time using the *Sync with G Suite* command.

1. Go to *MDM > Devices*.



2. Click the *Chromebook* icon.
3. Click *Sync with GSuite*.

Installing the Deep Freeze Chrome MDM Extension

The Deep Freeze Chrome MDM Extension is an extension for the Chrome browser that enables the following Deep Freeze MDM features:

- Send messages to devices as an on-demand action.
- Collection of the following device data: OS version, memory stats, storage capacity, battery level, user name of the current user, OU of the current user, whether the device is currently using work or home group, what group is currently applied to the device.

While individual users can install the Chrome extension, installation is best managed by an administrator using the Google Admin Console.

Visual instructions for installing the extension are found within Deep Freeze MDM:

1. Go to *MDM > Settings*.
2. Click the *Chromebook* icon.
3. Click the *Chrome Extension* tab.

The instructions are reproduced below:

1. Log in to your Google Admin Console with your Super Admin credentials.
2. Navigate to *Device Management* in the Google Admin Console.
3. Select *Chrome Management*, then *User Settings*.
4. Choose OUs to which the extension should be installed in the left navigation pane.
5. Navigate to *Force-install App and Extensions* section and click the *Manage force-installed apps* link.
6. Under Chrome Web Store, search for *Deep Freeze MDM* and add the extension. Click *Save*.
7. Scroll to *Incognito Mode* and select *Disallow incognito mode* to prevent users from bypassing the extension.
8. Navigate to *Device Management > Chrome > Device Settings*. Scroll to *Guest Mode* and select *Do not allow guest mode* to ensure the extension is always applied.

Removing devices

If a device has been retired, or if an employee has left the organization and you do not want to manage the device through Deep Freeze MDM, you can remove it from the Deep Freeze MDM web interface.

Note that removed devices can be re-enrolled, if needed.

Removing iOS or Android Devices

1. Go to *MDM > Devices*.
2. Click the *iOS* or *Android* icon.



3. Use the checkboxes to select one or more devices.
4. Click *Remove*.
5. Click *Yes* in the confirmation prompt to confirm the operation.

De-provisioning Chromebooks

1. Go to *MDM > Devices*.
2. Click the *Chromebook* icon.
3. Use the checkboxes to select one or more devices.
4. Click *De-provision*.
5. Select the reason you are de-provisioning the device(s) from the following options:
 - > The device is being upgraded or being replaced with a newer model.
 - > The device is being resold, donated, or permanently removed from use.
 - > A hardware issue was encountered and the device is being replaced with the same model or a like-model replacement.
6. Click *OK* to confirm.



Managing Apps

Adding apps to the Deep Freeze MDM enables you to automatically install those apps onto devices, and in the case of Kiosk Mode, limit devices to using a single selected apps.

Adding iOS apps

Apps for iOS devices can be sourced from the Apple App Store, or if you have in-house apps, you can add them using their .ipa files.

Adding Apps from the Apple App Store

1. Go to *MDM > Apps*.
2. Click the *iOS* icon.
3. Click *Add Apps > App Store App*.
4. Select the *iPad Apps* or *iPhone Apps* tab depending on what app type you want to add.
5. Use the *Store* field to select which country's app store you want to acquire apps from.
6. Enter a search string into the *Search Terms* field, then click *Search*.
A list of apps is displayed matching the search string.
7. Scroll through the list of apps. When you locate an app you want to add, click the associated *Add* button.

Adding in-house iOS Apps

1. Go to *MDM > Apps*.
2. Click the *iOS* icon.
3. Click *Add Apps > In-house App*.
4. There are two ways to upload an in-house app: provide an IPA file (an archive file for your app), or a manifest URL (the location of metadata associated with your web application).
 - > To upload an IPA file, select *Upload an IPA*, then click *Add*.
In the Add Source window that opens, click *Browse*. Use the browser window to locate and select the app's IPA file, then click *OK*.
 - > To enter a manifest URL, select *Specify a manifest URL*, then click *Add*.
In the Add Source window that opens, enter the URL of the web app manifest, then click *OK*.
5. Back in the Add new In-house App window, check that the displayed app properties look correct. Click *Save* to add the app.

Configuring iOS App Settings

Once an iOS app is added to the Deep Freeze MDM, you can configure app settings such as whether Deep Freeze can automatically install updates, delete the app, and the like.



1. Go to *MDM > Apps*.
2. Click the *iOS* icon.
3. Scroll through the list of apps and locate the app you want to configure. Click on the app name to open the app details.
4. Click *Manage Options and Configurations* and configure the app settings as required:

Options

- > Automatically update app – Select this option to automatically detect and install updates for this app on managed devices. Any updates to the app's description, logo, version number, and other properties will be automatically reflected in the MDM console. Note that unmanaged instances of the app, such as those installed before the app was added to the MDM, will not be updated.

This option is not available for in-house apps (apps not acquired from the Apple App Store).

- > Manage app (if currently installed as unmanaged) – Select this option to enable the MDM to manage all instances of the app on managed devices, regardless of whether the app was already installed on the device when it was added to the MDM. If this option is not selected, instances of the app that were installed before the device/app was added to the MDM will remain unmanaged.
- > Remove app when Deep Freeze MDM profile is removed – Select this option to automatically remove the app from managed devices if the app is removed from the MDM. Note that unmanaged instances of the app, such as those installed before the app was added to the MDM, will not be removed.
- > Prevent backup of the app data to iCloud or iTunes – Select this option to prevent the app's data from being backed up to iCloud or iTunes.
- > Allow Autonomous Single App mode – Select this option to enable the Single App mode. When you launch the app with this option enabled, you need to tap on the screen three times to enable Single App mode. The device will be locked down to the app. To disable Single App mode, tap on the screen three times.

Configuration

- > Add Values – Select this option and click *Add*. Specify the *Key*, data *Type* (string, integer, or boolean), and the *Value*. Click *Add* when finished.

Click on the pencil icon under the Actions column to edit a Value, or the X icon to delete a Value.

- > Choose XML File – Select this option and click *Choose File*. Select the .xml or .plist file and click *Open*.

5. Click *Save*.

Adding Android apps

Adding Apps from the Google Play Store

The first stage is to add Apps from the Google Store to the Deep Freeze MDM. Complete the following steps:

1. Go to *MDM > Apps*.
2. Click the *Android* icon.
3. Click *Add Apps*.



The Google Play Store opens.

4. Locate the app you want to add. Note that you can use the *Search* field to locate apps by name.
5. Click the app to open its App Details screen.
6. Click *Approve*.
7. Click *Approve* again in the confirmation prompt to confirm the operation.
8. Select one of the following settings for app permissions:
 - > Keep approved when app requests new permissions – Users will be able to install the updated app.
 - > Revoke app approval when this app requests new permissions – App will be removed from the store until it is reapproved.
9. Click *Save*.

Configuring Android App Settings

Once an Android app is added to the Deep Freeze MDM, you can configure app's settings. What settings are available vary widely according to the app, but they typically include permissions to access device resources such as using the camera or saving data externally.

1. Go to *MDM > Apps*.
2. Click the *Android* icon.
3. Scroll through the list of apps and locate the app you want to configure. Click on the app name to open the app details.
4. In the App Details screen, click the *Permissions* tab.
5. Configure the app's permissions—which device resources the app is permitted to access. What resources are listed depends on the app, but for each permission you can select *Allow* (the app is permitted to access this resource), *Deny* (the app cannot access this resource), or *User Control* (the device user can set this permission).

Some common device resources are listed below. This list is by no means exhaustive.

- > *Access_Course_Location* – permits the app to access the device's general location calculated using location data from cell towers and Wi-Fi.
 - > *Access_Fine_Location* – permits the app to access the device's precise location calculated using location data from GPS, cell towers, and Wi-Fi.
 - > *Camera* – permits the app to use the camera.
 - > *Read_External_Storage* – permits the app to read files that are not stored on the device.
 - > *Record_Audio* – permits the app to access the microphone.
 - > *Write_External_Storage* – permits the app to write files to storage that is not on the device.
6. Click the *Configurations* tab.
 7. Use the Configurations screen to apply configurations to the app. What configurations (if any) are available depends entirely on the app, but each field should include a tool tip provided by the app developer to assist you.



Managing Chromebook Apps

Apps for Chromebooks are not managed or assigned using the Deep Freeze Cloud Console. Chromebook apps are managed in G Suite; use G Suite's administration tools to assign users to organizational units (OU), and to define what apps are available to each OU.

Removing Apps

If you no longer need devices to use an app, it can be removed from the MDM.

1. Go to *MDM > Apps*.
2. Click the *iOS* or *Android* icon.
3. Locate the app you want to delete. Click the app name to open the app details.
4. Click *Delete*.
5. Click *Yes* in the confirmation prompt to confirm the operation.



Managing Groups

Groups are collections of settings that are used to configure and restrict what features are available to users. Depending on device type, these settings can include what apps will be installed on the device, whether the device is limited to running a single app, what administrative functions are available to the device user, which sites are blocked on the device, and the like.

Groups for iOS and Android devices

iOS and Android groups are assigned to devices. An iOS or Android device is subject to the settings of its group regardless of who uses the device.

All devices must be assigned to a group. Devices can only be assigned to one group, although they can be transferred between groups at any time. As the settings available vary by device type each group is specific to a certain device type. You can create multiple groups for each device type, but all devices within those groups must be the same type.

Groups for Chromebooks

Chromebook groups are assigned to Organizational Units (OUs). Whenever a user belonging to a given OU signs into a Chromebook, they are subject to the group settings associated with their OU. This means that the user will experience the same group settings regardless of what Chromebook device they use.

Chromebook MDM has an additional feature, Work Settings, that enables you to apply different group settings to the user depending on whether they are at work/school or at home. When using the Work Settings feature, two groups are assigned to the OU: one that is active while the user is at work, and one that is active at home.

Creating Groups for iOS devices

Creating a Group for iOS Devices

1. Go to *MDM > Groups*.
2. Click the *iOS* icon.
3. Click *Add Group*.
4. Define a *Group Name*.
5. Define the following settings as required:
 - > *Wireless Network* – click *Add Wireless Network*, then use the checkboxes to select wireless networks that will be made available to devices in the group. If a desired network does not appear in the list of options, you need to add it to the MDM from the *MDM > Settings* page.

Alternately, if no wireless networks have been pre-defined, clicking *Add Wireless Network* opens a window where you can define a new wireless network. Define the network properties and click *OK*.



- > Web Clips – click *Add Web Clips*, then use the checkboxes to select Web Clips to be installed on all devices in the group. If a desired Web Clip does not appear in the list of options, you need to add it to the MDM from the *MDM > Settings* page.

Alternately, if no Web Clips have been pre-defined, clicking *Add Web Clips* opens a window where you can define a new Web Clip. Define the Web Clip properties and click *OK*.

- > Email Settings – click *Add Email Settings*, then use the checkboxes to select an email account to be used by all devices in the group. This option is useful if you want all devices to use a common email to submit their coursework in a school or all the organizations to communicate using the same email address.

If a desired email account does not appear in the list of options, you need to add it to the MDM from the *MDM > Settings* page.

Alternately, if no email settings have been pre-defined, clicking *Add Email Settings* opens a window where you can enter email account information. Enter the account properties and click *OK*.

- > Certificates – click *Add Certificates*, then use the checkboxes to select certificates to be installed on all devices in the group. If a desired certificate does not appear in the list of options, you need to add it to the MDM from the *MDM > Settings* page.

Alternately, if no certificates have been pre-defined, clicking *Add Certificates* opens a window where you can provide certificate information. Enter the certificate properties and click *OK*.

- > Global HTTP Proxy – use this field to select an HTTP proxy if the devices in the group require one. If the desired HTTP proxy does not appear in the list of options, you need to add it to the MDM from the *MDM > Settings* page.
- > Wallpaper – use this field to select a wallpaper image if the devices in the group should display the same wallpaper. If the desired image does not appear in the list of options, you need to add it to the MDM from the *MDM > Settings* page.
- > Lock screen message – use this field to define a lock screen message for devices in the group. The text you define here will be displayed at the bottom of the screen whenever the kiosk device is locked.
- > Track Device Location – select this option to track the location of devices in the group. Note that only devices with the Deep Freeze MDM app installed can be tracked.

6. Click the *Apps* tab.

7. Use the checkboxes to select apps to be installed on devices in the group. If a desired app does not appear in the list of options, you need to add it to the MDM from the *MDM > Apps* page.

Note that if Kiosk mode is enabled for the group, the selected apps *may or may not* be installed, depending on the app.

8. Click *Save*.

Configuring iOS Group Passcode Requirements

You can configure groups to enforce passcode requirements on their member devices.

1. Go to *MDM > Groups*.
2. Click the *iOS* icon.
3. Scroll through the list of groups and locate the group you want to edit. Click the group name to open it for editing.



4. Click the *Passcode* tab.
5. Configure the passcode settings:
 - > Require a Passcode – enable this option to enforce a passcode requirement on devices in the group. Enabling this option also enables you to edit the remaining passcode settings.

The following settings are available when the Require a Passcode option is enabled.

 - ~ Require alphanumeric value – enable this option to require passcodes to be entered and defined using a full alphanumeric keypad instead of the default numeric keypad.
 - ~ Allow simple value – enable this option to permit users to define passcodes that include repeating, ascending, or descending character sequences.
 - ~ Minimum length – use this field to define the minimum passcode length.
 - ~ Minimum number of complex characters – use this field to define the number of complex characters (non-alphanumeric characters) that passcodes must contain.
 - ~ Maximum age in days – use this field to define maximum number of days the user may keep a passcode before changing it.
 - ~ Passcode history – use this field to define the number of unique passcodes a user must create before they can reuse an previous passcode. The value can range from 0 to 50.
 - ~ Maximum grace period before lock – use this field to select the length of time device can remain locked before a passcode is required to unlock it.
 - ~ Maximum number of failed attempts – use this field to define the number of failed login attempts before device is erased. The value can range from 1 to 50.
 - ~ Maximum auto-lock time – use this field to select how long the device can remain idle before locking itself.
6. Click *Save*.

Creating Groups for Android Devices

Creating a Group for Android Devices

1. Go to *MDM > Groups*.
2. Click the *Android* icon.
3. Click *Add Group*.
4. Define a *Group Name*.
5. Define the following settings as required:
 - > Wireless Network – click *Add Wireless Network*, then use the checkboxes to select wireless networks that will be made available to devices in the group. If a desired network does not appear in the list of options, you need to add it to the MDM from the *MDM > Settings* page.

Alternately, if no wireless networks have been pre-defined, clicking *Add Wireless Network* opens a window where you can define a new wireless network. Define the network properties and click *OK*.



- > Web Clips – click *Add Web Clips*, then use the checkboxes to select Web Clips to be installed on all devices in the group. If a desired Web Clip does not appear in the list of options, you need to add it to the MDM from the *MDM > Settings* page.
Alternately, if no Web Clips have been pre-defined, clicking *Add Web Clips* opens a window where you can define a new Web Clip. Define the Web Clip properties and click *OK*.
 - > Wallpaper – use this field to select a wallpaper image if the devices in the group should display the same wallpaper. If the desired image does not appear in the list of options, you need to add it to the MDM from the *MDM > Settings* page.
 - > Track Device Location – select this option to track the location of devices in the group. Note that only devices with the Deep Freeze MDM app installed can be tracked.
6. Click the *Apps* tab.
 7. Use the checkboxes to select apps to be installed on devices in the group. If a desired app does not appear in the list of options, you need to add it to the MDM from the *MDM > Apps* page.
 8. For each app you select, use the corresponding checkbox in the *Auto Install* column to toggle the Auto Install feature as needed. Auto Install is enabled by default.
 - > If Auto Install is enabled, the app will be automatically installed on all devices in the group.
 - > If the app is selected but Auto Install is disabled, the app will not be automatically installed. Instead, users will have the option to install the app through the MDM app.
 9. Click *Save*.

Configuring Android Group Passcode Requirements

You can configure groups to enforce passcode requirements on their member devices.

1. Go to *MDM > Groups*.
2. Click the *Android* icon.
3. Scroll through the list of groups and locate the group you want to edit. Click the group name to open it for editing.
4. Click the *Passcode* tab.
5. Enable one or both of the following options:
 - > Require Device Passcode – enable this option to enforce a device passcode requirement on devices in the group. Users are prompted to enter the device passcode when attempting to unlock the device.
 - > Require Work Profile Passcode (Android N and above) – enable this option to enforce a passcode requirement for accessing the work profile on devices in the group. Users are prompted to enter the work profile passcode when attempting to open a work app.

Enabling either option reveals additional settings.

6. Configure the revealed settings. The device passcode and work profile passcode are configured separately, but the settings are the same for each:
 - > Require alphanumeric value – enable this option to require passcodes to be entered and defined using a full alphanumeric keypad.



- > Allow simple value – enable this option to permit users to define passcodes that include repeating, ascending, or descending character sequences.
 - > Minimum length – use this field to define the minimum passcode length.
 - > Maximum age in days – use this field to define maximum number of days the user may keep a passcode before changing it.
 - > Passcode history – use this field to define the number of unique passcodes a user must create before they can reuse an previous passcode. The value can range from 0 to 50.
 - > Maximum number of failed attempts – use this field to define the number of failed login attempts before device is erased. The value can range from 1 to 50.
 - > Maximum auto-lock time – use this field to select how long the device can remain idle before locking itself.
7. Define the Passcode Compliance Grace Period:
 - > Passcode Compliance Grace Period – use this field to define the number of minutes after the password is found non-compliant with policy that all work apps will get disabled.
 8. Click *Save*.

Managing Groups for Chromebooks

Creating a Chromebook group requires two broad steps:

1. Configure a new group by defining its properties and settings. See [Configuring Chromebook Groups](#), below.
2. Associate the group with Chromebook users by assigning it to an OU. See [Assigning Chromebook Groups to users](#), below.

Configuring Chromebook Groups

To configure a new Chromebook group, you must create the group, then define its Web Filtering and YouTube settings.

Creating a new Chromebook Group

1. Go to *MDM > Groups*.
2. Click the *Chromebook* icon.
3. Click *Add Group*.
4. Define a *Group Name*.
5. Click *Save*.

Configuring Web Filtering

Web Filtering enables you to limit which websites can be visited by users in the group.

1. Go to *MDM > Groups*.
2. Click the *Chromebook* icon.
3. In the list of groups, locate the group you want to edit. Click the group name to open it for editing.



4. Use the Web Filtering tab to limit which websites can be visited by users in the group. You can configure filtering as a blacklist, where certain sites are forbidden, or as a whitelist, where only certain sites are permitted.
 - > To filter using a blacklist, select the *Blacklist Mode* option. Chromebooks will be blocked from visiting any site you add to the blacklist.

To add websites to the blacklist, enter the URL into the *Website URL* field, select *Blacklist (block)*, then click *Add Domain*. When you add domain to a list, it affects all paths from that domain. For example, if you added *www.example.com* to the blacklist, then *www.example.com/login* would be blocked when Blacklist Mode is active.

To remove a URL from the blacklist, click the associated Delete icon ✕.
 - > To filter using a whitelist, select the *Whitelist Mode* option. Chromebooks will be blocked from accessing all websites except the ones you add to the whitelist.

To add websites to the whitelist, enter the URL into the *Website URL* field, select *Whitelist (allow)*, then click *Add Domain*. When you add domain to a list, it affects all paths from that domain. For example, if you added *www.example.com* to the whitelist, then *www.example.com/login* would be permitted when Whitelist Mode is active.

To remove a URL from the whitelist, click the associated Delete icon ✕.
5. Click *Save*.

Configuring YouTube filtering

YouTube filtering enables you to limit what YouTube content is available to users in the group.


1. Go to *MDM > Groups*.
2. Click the *Chromebook* icon.
3. In the list of groups, locate the group you want to edit. Click the group name to open it for editing.
4. Click the *YouTube* tab.
5. Adjust the YouTube tab settings as desired:
 - > Enable the *Block Comments* option to prevent users from leaving comments on YouTube videos.
 - > Enable the *Block Sidebar* option to hide YouTube's Recommended Videos sidebar.
 - > In the *Block Categories* section, select categories to block. Users will not be able to view any video belonging to the selected categories.
 - > To block specific channels, enter the channel name or URL into the *YouTube Channel URL or Name* field, then click *Block Channel*. For example, to block the NFL channel, you could enter *www.youtube.com/nfl*, or just *nfl*.
 - > To block specific videos, enter the video URL into the *YouTube Video URL* field, then click *Block Video*.
6. Click *Save*.




Assigning Chromebook Groups to users

Chromebooks operate on a cloud model, so a given Chromebook's capabilities depend less on the device itself and more on who is using it. When a user logs into a Chromebook, the user's OU determines which group's settings are applied to the device they are using.

Assigning groups to an OU

1. Go to *MDM > Groups*.
2. Click the *Chromebook* icon.
3. Click the *OU Assignments* tab.
4. Optionally click *Sync with G Suite* to ensure Deep Freeze MDM displays the most current information from your G Suite account.
5. In the list of OUs, locate the OU you want to assign groups to. Click the associated Edit icon .
6. Select an *Assigned Work Group*. This group's settings are active when a user belonging to the OU logs into a device.

If you are using the Work Settings feature, this group's settings are active while the device is at work/school.
7. If you are using the Work Settings feature, optionally select an *Assigned Home Group* for the OU. This group's settings are active while the user's device is not at work/school.

If you do not define an *Assigned Home Group*, the *Assigned Work Group* is applied at all times.
8. Click the Save icon .

Determining which OUs are associated with a group

Each OU can be associated with one or two groups, and a given group can be assigned to any number of OUs. Sometimes you may need to know which OUs a group is assigned to.

1. Go to *MDM > Groups*.
2. Click the *Chromebook* icon.
3. Click the *Groups* tab if it is not already selected.
4. Optionally click *Sync with G Suite* to ensure Deep Freeze MDM displays the most current information from your G Suite account.
5. In the list of groups, locate the group you want more information on, then check the following columns:
 - > OUs Assigned (Work) – the group is assigned to these OUs as a work group.
 - > OUs Assigned (Home) – the group is assigned to these OUs as a home group.

Assigning iOS or Android Devices to a Group

Adding a device to a group both configures and categorizes the device; it takes on the settings associated with the group, such as what apps it can run and what features are locked out.



1. Go to *MDM > Devices*.
2. Click the *iOS* or *Android* icon.
3. Use the checkboxes to select one or more devices.
4. Hover over *Move to Group* to display the groups available for the selected device type.
5. Select a group to move the selected devices to that group.

The devices will inherit the group's settings the next time they check in. If the group settings included apps, those apps will be installed.



On-Demand Actions

This chapter explains the various on-demand actions that can be performed on the mobile devices from Deep Freeze MDM web interface.

Sending Messages to Devices

You can use the Deep Freeze Cloud Console to send messages to devices. Such messages are displayed as push messages. Messages are not cached, however; if a recipient computer is powered down or no user is logged in when the message is received, the message will not appear on that computer.

Note that the devices receiving a given message must be all of the same type (iOS, Android, or Chromebook). Chromebooks can only receive messages if they have the Deep Freeze MDM Chromebook Extension installed; see [Installing the Deep Freeze Chrome MDM Extension](#) for more information.

1. Go to *MDM > Devices*.
2. Click the *iOS, Android, or Chromebook icon*.
3. Use the checkboxes to select one or more devices.
4. Select *Message*.
5. Enter the message.
6. Click *Send*.

Locking a Device

Complete the following steps to lock a device:

1. Go to *MDM > Devices*.
2. Click the *iOS or Android icon*.
3. Select one or more devices.
4. Select *Lock*.



If a passcode has been specified on the device, a user must enter the passcode to unlock the device.

Assigned Apps for Devices

Complete the following steps to push or update assigned apps on the device:

1. Go to *MDM > Devices*.
2. Click the *iOS or Android icon*.
3. Select one or more devices.



4. Select *Assigned Apps* and click *Push Assigned Apps* or *Update Assigned Apps*.

Clearing the Passcode on an iOS Device

Complete the following steps to clear the passcode on the device:

1. Go to *MDM > Devices*.
2. Click *iOS*.
3. Select one or more devices.
4. Select *Clear Passcode*.



If the iOS device is part of a Group where passcode is required, the user will be prompted to enter a new passcode on the device as per the passcode policy.

Resetting the Passcode on an Android Device

Complete the following steps to reset the passcode on the device:

1. Go to *MDM > Devices*.
2. Click the *Android* icon.
3. Select one or more devices.
4. Select *Reset Passcode*.

Disabling and Re-enabling Chromebooks

You can use the MDM to remotely disable Chromebooks, which renders the device inoperable by immediately logging out current users and preventing users from logging in.

Disabled Chromebooks display a message to users stating that the device is disabled. The text of this message can be customized using G Suite administration tools.

Disabled Chromebooks can be re-enabled at any time.

Disabling Chromebooks

1. Go to *MDM > Devices*.
2. Click the *Chromebook* icon.
3. Optionally click *Sync with G Suite* to ensure Deep Freeze MDM displays the most current information from your G Suite account.
4. Use the checkboxes to select one or more Chromebooks with a *Status* of *Active*.
5. Click *Disable*.

Re-enabling Chromebooks

1. Go to *MDM > Devices*.
2. Click the *Chromebook* icon.



3. Optionally click *Sync with G Suite* to ensure Deep Freeze MDM displays the most current information from your G Suite account.
4. Use the checkboxes to select one or more Chromebooks with a *Status* of *Disabled*.
5. Click *Re-enable*.

Customizing the Chromebook Disabled Message

When a Chromebook is disabled, it displays the following message: "This device was locked by <account> administrator". You can use G Suite administration tools to add custom text to this message.

1. Log into G Suite using your administrator credentials.
2. Navigate to *Device Management > Chrome > Device Settings*.
3. Edit the *Disabled device return instructions*. The text you enter will be appended to the disabled message.

Wiping a Device

A mobile device can be wiped in the following two ways:

Select Wipe

A select wipe action is used to remove all the apps that are installed on the device. The device configuration and all the settings are left unchanged. Complete the following steps to perform a select wipe:

1. Go to *MDM > Devices*.
2. Click the *iOS* or *Android* icon.
3. Select one or more devices.
4. Select *Select Wipe*.



To re-install apps that are removed using Select Wipe, select the mobile devices and click *Push Assigned Apps*. The apps that are selected in the group to which the mobile device belongs are re-installed.

Full Wipe

A full wipe action is used to restore the device to its original settings. Complete the following steps to perform a full wipe:

1. Go to *MDM > Devices*.
2. Click the *iOS* or *Android* icon.
3. Select one or more devices.
4. Select *Full Wipe*.
5. The message *Do you want to perform Full Wipe action for selected Device(s)?* appears. Click *Yes*.



Moving Chromebooks Between Organizational Units (OU)

OUs are normally managed through G Suite, but you can also use Deep Freeze Cloud Console to move Chromebooks between OUs if needed.

1. Go to *MDM > Devices*.
2. Click the *Chromebook* icon.
3. Use the checkboxes to select one or more devices.
4. Hover over *Move Device OU* to reveal a list of available OUs.
5. Click an OU to move the selected Chromebooks to that OU.



The *Move Device OU* command assigns the device to a new OU, not the user. This means that it has no effect on what group settings are applied to the device; group settings depend on the user's OU, not the device's OU.

Updating iOS on Devices

You can prompt supervised iOS devices to update their operating system. Complete the following steps to update iOS on one or more devices:

1. Go to *MDM > Devices*.
2. Click *iOS*.
3. Use the checkboxes to select one or more devices. Devices with an out-of-date version of iOS are indicated with an orange icon.
4. Click *Update iOS*.

Note that only those selected devices that are supervised and are running an out-of-date version of iOS will update.

5. Specify the name of the group and click *Save*.



Setting Restrictions

Restrictions are group-specific options that enable you to limit what device features are available to users. For example, you can prevent users from installing new apps, disable the camera, or prohibit Bluetooth connections.

Restrictions for iOS and Android Devices

Restrictions for iOS and Android devices can be set through Deep Freeze MDM when creating a group. Restrictions can be set by the following steps:

1. Create a group.
2. Configure the restrictions in the *Restrictions* tab.
3. Save the group.
4. Assign devices to the group.



The restrictions will take effect only when the mobile device is assigned to the group.
If a mobile device is removed from a group, the restrictions are removed.

The restrictions can be set in the following location:

iOS: *MDM > Groups > iOS > Restrictions* tab

Android: *MDM > Groups > Android > Restrictions* tab

Restrictions for Chromebook Devices

If you need to restrict what features are available to Chromebook users, use the administration tools in your G Suite account. That said, Deep Freeze MDM provides web filtering options for Chromebook devices.

- For group-specific filtering settings, see [Creating Groups for Android Devices](#).
- For universal filtering settings to be applied to all Chromebooks, see [Configuring Universal Filtering Settings for Chromebooks](#).

Settings Restrictions for iOS Groups

The restrictions can be set in the following location:

MDM > Groups > iOS > Restrictions tab

The following configuration options are available:

- Device Functionality
 - > Allow camera – select this option to allow the camera. If this option is not selected, the camera icon is hidden and removed from the Home screen. Users can't take photographs or videos, or use FaceTime.
 - > Allow screenshots – select this option box to allow the user to take screenshots. If this option is not selected, save a screenshot or screen recording of the display.



- > Always require iTunes Store password – select this option if you want the user to always enter the password to iTunes.
- > Allow Siri – select this option to allow Siri. If this option is not selected, users will not be able to launch Siri.
- > Allow Siri when locked – select this option box to allow Siri when the device is locked.
- Content Rating
 - > Allow Bookstore erotica – select this option to allow the device to access erotica through the Bookstore.
 - > Allowed App rating – select the allowed app rating from the drop-down.
 - > Allowed Movie rating – select the maximum permitted movie rating from the drop-down.
 - > Allowed TV rating – select the maximum permitted TV rating from the drop-down.
- iCloud
 - > Allow Photo Stream – select this option to allow Photo Stream. If this option is not selected, *Upload to My Photo Stream* is hidden in *Settings > [your name] > iCloud > Photos*.
 - > Allow Shared Photo Stream – select this option to allow shared Photo Stream. If this option is not selected, *iCloud Photo Sharing* is hidden in *Settings > [your name] > iCloud > Photos*.
 - > Allow iCloud backup – select this option to allow users to perform iCloud backup. If this option is not selected the *iCloud Backup* option in *Settings > [your name] > iCloud > iCloud Backup* is disabled and the backup can only be performed using iTunes.
- Supervised Devices Only – the following restrictions can be set only for supervised devices:
 - > Allow AirDrop – select this option to allow AirDrop. If this option is not selected, the users will not be able to share files with other iOS devices using the AirDrop feature.
 - > Allow account modification – select this option to allow users to log on to the iTunes Store. If this checkbox is not selected, the users will not be able to log on to the iTunes Store and change the password.
 - > Allow apps to modify cellular data usage – select this option to allow users to select which apps can use cellular data. If this option is not selected, users can't change any settings regarding what apps use cellular data.
 - > Allow app removal – select this option to allow users to uninstall apps from the device.
 - > Allow Siri to access user generated content – select this option to allow Siri to obtain user generated content. If this option is not selected, Siri can't obtain content from sources that allow user-generated content, such as Wikipedia.
 - > Allow Bookstore – select this option to allow iBooks. If this option is not selected, iBooks app will be empty and users will not be able to access books.
 - > Allow iMessage – select this option to allow iMessage. If this option is not selected, only text messages will be allowed and iMessage will be disabled.
 - > Allow FaceTime – select this option to allow FaceTime video and audio calls. To allow FaceTime, Camera has to be allowed on the device.
 - > Allow Bluetooth modifications – select this option to allow modifying the Bluetooth settings.



- > Allow device name modifications – select this option to allow users to modify device name. If this option is not selected, users cannot modify the device name from *Settings > General > About > Name*.
- > Allow Find My Friends modifications – select this option to allow modifications in the My Friends app such as *Current Location, Share My Location, Send As, Allow Friend Requests and Show Geofence Alerts from*.
- > Allow Game Center – select this option to allow the Game Center application. If this option is not selected, Game Center is disabled and the icon is not visible.
- > Allow host paring – select this option to allow iOS devices with hosts such as a MacBook or iMac. If this option is not selected, users will only be able to pair the device with MacBook or iMac from where the device was first supervised using the Apple Configurator.
- > Allow interactive installation of profiles and certifications – select this option to enable the *Install* option while installing End User Digital Certificates and profiles. If this checkbox is not selected, the *Install* option will be disabled and the user cannot install End User Digital Certificates.
- > Allow News – select this option to allow the iOS News widget. The news widget will not be shown if this option is not selected.
- > Allow Wallpaper Modification – select this option to allow users to modify their wallpaper. The *Wallpaper* option will be disabled in *Settings* if this option is not selected.
- > Allow USB Restricted Mode (iOS 11.4.1) – select this option to lock down the device charging port into power-only mode when connected to the computer one hour after it was last unlocked.
- > Allow AutoFill Password (iOS 12+) – select this option to enable password AutoFill or choosing from saved passwords.
- > Force automatic Date & Time (iOS 12+) – select this option to set the device to adjust automatically for date and time changes such as daylight savings time or time zone changes.
- > Allow explicit content – select this option to allow explicit content.
- > Allow iCloud document sync – select this option to allow syncing documents to iCloud from Pages or iWork. If this option is not selected, Pages or iWork will not be able to sync with iCloud.
- > Allow App installation – select this option to allow users to install apps from the Apple App Store. If this option is not selected, users will be prevented from installing apps on their own.
- > Allow Safari – select this option to allow the Safari browser. If this option is not selected, Safari browser will be disabled.
- > Delay OS Software Updates until x days after release date (iOS 12+) – select this option to delay OS software updates until up to 90 days.

Setting Restrictions for Android Groups

The restrictions can be set in the following location:



MDM > Groups > Android > Restrictions tab



Samsung SAFE V2+ certified – Administrators can manage SAFE Android smartphones and tablets securely and remotely by deploying mobile applications and controlling overall device functionality.

- Device Functionality
 - > Allow camera – select the checkbox to allow the user to launch the camera through a camera app. Clear the checkbox to disable the camera. The default camera can always be launched. This setting only works for camera apps other than the default camera app.
 - > Allow microphone (SAFE v2+, Device Owner) – select the checkbox to disable the microphone used voice calls. The built-in voice recorder can still use the microphone if this checkbox is cleared (depending on the device manufacturer).
 - > Allow screen capture (SAFE v2+, Device Owner, Profile Owner) – select the checkbox to allow user to capture the screen. Clear the checkbox to disable this feature. The user will not be able to take a screenshot on the mobile device if the checkbox is not selected.
 - > Allow adding accounts (SAFE v2+, Profile Owner, Device Owner) – select the checkbox to allow users to add accounts on the device. Clear the checkbox to disable this feature. The *Add Accounts* option on the mobile device will be disabled if this option is not selected.
- Sync and Storage
 - > Allow Google Account Sync (SAFE v2+) – select the checkbox to allow users to automatically sync Google Account. The options in *Settings > Accounts > Accounts > Google* are disabled if this option is not selected.
 - > Allow use of SD card (SAFE v2+) – select the checkbox to allow Secure Digital (SD) cards on mobile devices. SD cards cannot be used on mobile devices if this option is not selected. The SD card will be shown as *Not inserted* and the user will not have an access to the SD card if this option is not selected.
 - > Allow use of USB (SAFE v2+) – select the checkbox to allow USB devices to connect to the mobile device. If this option is not selected, USB devices will not be detected by the mobile device.
 - > Allow USB storage device (SAFE v2+) select the checkbox to allow USB storage devices to connect to the mobile device. This option can be enabled only if *Allow use of USB* is enabled.



For Samsung devices (supporting Knox SDK) in Device Owner mode, clearing *Allow use of USB*, will only disable USB data transfer between device and the computer. However, storage media (like OTG pen drive) will be mounted to device if *Allow USB storage device* is selected.

- > Enforce Storage Encryption – select the checkbox to encrypt data on the mobile devices for security. Data will not be encrypted if this option is not selected. If the device has been encrypted previously, it cannot be decrypted by clearing the checkbox.
- Default Runtime Permissions for Work apps



- > Default Apps Permission: select the appropriate permission for all the apps. Select *Prompt* (to prompt the user), *Auto Grant* (automatically grant permission to run the app) or *Auto Deny* (automatically deny permission to run the app). Permissions for each apps can be set manually from *MDM > Apps > Android > Manage Permission & Configurations > Permissions* tab. The settings in the Permissions tab set for each individual app overrides the default app permission.
- Applications
 - > Allow uninstall (SAFE v2+ Profile Owner Device Owner) – select the checkbox to allow users to uninstall apps. Users will not be able to uninstall apps from the mobile device if this option is not selected and the message *Uninstall unsuccessful* will be shown.
 - > Allow stopping of system apps (SAFE v2+) – select the checkbox to allow users to stop Android System apps. If this option is not selected, the option *Settings > Apps > [System_App_Name] > Force Stop* will be disabled.
 - > Allow YouTube (SAFE v2+ Profile Owner, Device Owner) – select the checkbox to allow users to launch YouTube on the mobile device. Users will be prevented from launching you tube if this option is not selected.
 - > Allow Gmail (SAFE v2+ Profile Owner, Device Owner) – select the checkbox to allow users to launch the Gmail app. Users will not be able to launch Gmail if this option is not selected.



If the Allow Gmail option is not selected, the Gmail app cannot be launched. However, users can still access Gmail via the browser.

- > Allow Google Maps (SAFE v2+, Device Owner) – select the checkbox to allow users to launch Google Maps on the mobile device.
- Security
 - > Allow Restore Factory Settings (SAFE v2+ Device Owner) – select the checkbox to allow users to restore to factory settings. Users will not be able to restore the device to factory settings if this option is not selected.



If the Allow Restore to Factory Settings option is not selected, administrators can still restore the device to factory settings remotely from the Deep Freeze MDM web interface.

- > Allow installation from unknown sources (SAFE v2+ Profile Owner Device Owner) – select this option to allow users to install apps from locations other than the Google Play Store.
- > Allow Airplane mode SAFE v2+ – select the checkbox to allow users to put the mobile devices into Aeroplane mode.
- Network
 - > Allow MDM provisioned Wi-Fi only – select this option if you want the mobile device to connect only to the Wi-Fi defined in the Deep Freeze MDM. If this option is selected the user will not be able to connect to any other Wi-Fi Network.



- > Allow Bluetooth – select this option to allow users to enable Bluetooth on their mobile devices and connect to other devices. If this option is not selected, users cannot enable Bluetooth on their devices.
- > Allow Wi-Fi Direct (SAFE v2+) – select this option allow mobile devices to connect to other devices through Wi-Fi direct. Mobile devices will not be able to connect to the other devices through Wi-Fi direct if this option is not selected.
- Miscellaneous
 - > Allow turning device off using the power button (SAFE v2+) – select this option to allow users to power off the mobile devices using the power button on the phone.
 - > Allow date/time change (SAFE v2+ Device Owner) – select this option to allow the users to change the time. Users will not be able to change the date or time manually if this option is not selected.
 - > Use network time (SAFE v2+) – select the checkbox to use the time from the mobile network.



Sort the restrictions from the drop-down as follows:

- All Features
- Core Android
- SAFE V2+
- Device Owner
- Profile Owner

Only devices running Android 5.0 or above can be provisioned as Profile Owner or Device Owner.

Configuring Universal Filtering Settings for Chromebooks

Use Chromebook web filtering to control how Chromebooks can use the internet and what content they can access.

Deep Freeze MDM features both universal and group-specific web filter settings. The settings described here are universal; they will be applied to all Chromebooks in the system.

1. Go to *MDM > Settings*.
2. Click the *Chromebook* icon.
3. Click the *Filtering Settings* tab.
4. Edit the filtering settings as required:
 - > Force SafeSearch on Google, Yahoo, and Bing – enable this option to require all Chromebooks to filter out explicit content using SafeSearch when conducting Google searches, and equivalent content-control software when using Yahoo or Bing.
 - > Block Direct IP Access – Savvy users can bypass URL-based web filtering by entering an IP address rather than a URL into their browser's address bar. Enable this option to prevent Chromebook users from accessing websites in this manner.



Managing Chromebook Work Settings

Work Settings enable Chromebooks in your system to use different settings depending on whether they are at work/school or at home.

- The conditions Chromebooks use to determine whether they are at work or at home are the same for all devices.
- The home and work settings vary by user; each user OU can be assigned a different work group and home group.
- This means that if you have two Chromebooks at the same location at the same time, they will both be using either their work settings or home settings. However the work settings for one user may be very different from the other.

Configuring Work Settings is a four-step process:

1. Enable the feature. See [Enabling Work Settings](#), below.
2. Optionally define a range of IP addresses that activate work settings. See [Defining Work IP Ranges](#), below.
3. Optionally define a schedule for work settings. See [Defining a Work Schedule](#), below.
4. For each user OU, assign a Work Group and Home Group. These groups determine what settings will be active while the device is at work and at home. See [Managing Assigned Work Groups and Assigned Home Groups](#), below.

Enabling Work Settings

The Work Settings feature must be enabled before it will take effect.

1. Go to *MDM > Settings*.
2. Click the *Chromebook* icon.
3. Enable the *Enable Work IP Range and Work Schedule* option.
4. Click *Save*.

Defining Work IP Ranges

You can define a range of IP addresses for work settings. If a Chromebook has an external IP address within this range, it uses its work settings. Otherwise, it uses its home settings.

If both an IP range and schedule are enabled, meeting the conditions of *either* criteria will enable work settings.

1. Go to *MDM > Settings*.
2. Click the *Chromebook* icon.
3. Use the *Work IP Range* section to define IP ranges as required:
 - > To define the range, enter the minimum and maximum IP values in the left and right fields, respectively.
 - > To add another range, click the *Add* icon **+**.
 - > To delete a range, click the associated *Delete* icon **×**.



4. Enable ranges by clicking the checkboxes to the left of the range values. Only enabled ranges are used to determine if a Chromebook should use work settings. You can enable as many ranges as needed.
5. Click *Save*.

Defining a Work Schedule


You can define a weekly schedule for work settings. During the scheduled times, Chromebooks use their work settings. Outside of the schedule, home settings are used.

If both an IP range and schedule are enabled, meeting the conditions of either criteria will enable work settings.

1. Go to *MDM > Settings*.
2. Click the *Chromebook* icon.
3. Use the *Work Schedule* section to define the schedule. For each day, define a start time and end time in the left and right field, respectively.
4. Enable days by clicking the checkboxes to the left. The schedule will only take effect on enabled days.
5. Click *Save*.

Managing Assigned Work Groups and Assigned Home Groups

Once you have configured when work group and home group settings are applied, you need to assign work groups and home groups to OUs. When a user belonging to a given OU logs in, the appropriate group's settings are applied.

1. Go to *MDM > Groups*.
2. Click the *Chromebook* icon.
3. Click the *OU Assignments* tab.
4. Optionally click *Sync with G Suite* to ensure Deep Freeze MDM displays the most current information from your G Suite account.
5. In the list of OUs, locate the OU you want to assign groups to. Click the associated *Edit* icon .
6. Select an *Assigned Work Group*. This group's settings are active while the device is at work/at school.
7. Select an *Assigned Home Group* for the OU. This group's settings are active while the user's device is not at work/at school.

If you do not define an *Assigned Home Group*, the *Assigned Work Group* is applied at all times.

8. Click the *Save* icon .



Chromebook Data

Deep Freeze MDM collects data on each Chromebook enrolled in the system. Note that some data requires that the Deep Freeze MDM Chrome Extension be installed

General Chromebook Information

1. Go to *MDM > Settings*.

2. Click the *Chromebook* icon.

A table lists the following information for each Chromebook:

- > Status – the current status of the device within the MDM. Chromebooks that are functioning normally and available for use are listed as Active.
- > Name – the name of the device. Click on the device name to access additional details.
- > Model – the device model.
- > OU Path – the device's Organizational Unit.
- > Tags – a list of Tags applied to the device, if any.
- > User name – the name of the user currently logged into the device. The user must have the Deep Freeze MDM Chrome Extension for this data to be collected.
- > User OU – the user's Organizational Unit. The user must have the Deep Freeze MDM Chrome Extension for this data to be collected.
- > Effective Group – the name of the group settings currently applied to the device. Click on the group name to navigate to the group properties. The user must have the Deep Freeze MDM Chrome Extension for this data to be collected.
- > Last Reported- timestamp of the device's most recent contact to Deep Freeze MDM.
- > Work / Home – if you are using the Work Settings feature, this column displays whether the device is currently using work group or home group settings. The user must have the Deep Freeze MDM Chrome Extension for this data to be collected.
- > Storage – the total storage available on the device. The user must have the Deep Freeze MDM Chrome Extension for this data to be collected.
- > Battery – the percentage of total battery power remaining on the device. The user must have the Deep Freeze MDM Chrome Extension for this data to be collected.
- > Last Sync – timestamp of the device's most recent sync to Google Admin policy settings.

Chromebook Device Details

1. Go to *MDM > Settings*.

2. Click the *Chromebook* icon.

3. Locate the device of interest in the table of devices. Click the device name.

The Device Details open:



- > Status – the current status of the device within the MDM. Chromebooks that are functioning normally and available for use are listed as Active.
- > Model – the device model.
- > Unique Identifier – the device’s internal unique identifier, assigned at manufacture.
- > Serial Number – the device serial number.
- > OS Version – the version of Chrome OS on the device. The user must have the Deep Freeze MDM Chrome Extension for this data to be collected.
- > Memory Stats – the available / total RAM on the device. The user must have the Deep Freeze MDM Chrome Extension for this data to be collected.
- > Storage Capacity – the total storage available on the device. The user must have the Deep Freeze MDM Chrome Extension for this data to be collected.
- > Battery Level – the percentage of total battery power remaining on the device. The user must have the Deep Freeze MDM Chrome Extension for this data to be collected.
- > OU Path – the device’s Organizational Unit.
- > User name – the name of the user currently logged into the device. The user must have the Deep Freeze MDM Chrome Extension for this data to be collected.
- > User OU – the user’s Organizational Unit. The user must have the Deep Freeze MDM Chrome Extension for this data to be collected.
- > Effective Group – the name of the group settings currently applied to the device. Click on the group name to navigate to the group properties. The user must have the Deep Freeze MDM Chrome Extension for this data to be collected.
- > Work / Home – if you are using the Work Settings feature, this column displays whether the device is currently using work group or home group settings. The user must have the Deep Freeze MDM Chrome Extension for this data to be collected.
- > Last Sync – timestamp of the device’s most recent sync to Google Admin policy settings.
- > Last Reported- timestamp of the device’s most recent contact to Deep Freeze MDM.
- > Annotated Asset Id – the name of the device.
- > Annotated User – typically this is the user who first enrolled the device. This field can be edited in Google Admin.
- > Annotated Location – a description of the device location. This field can be edited in Google Admin.
- > Notes – any notes associated with the device. This field can be edited in Google Admin.
- > Location – a map of the current device location. The user must have the Deep Freeze MDM Chrome Extension for this data to be collected.
- > Tag – a list of Tags applied to the device, if any.



Mobile Kiosks

Mobile kiosks are mobile devices that only permit users to access a single app. Typical uses for these devices include self-service menus, self-guided presentations, and dedicated software demos.

To create kiosks, you must create a group that has Kiosk Mode enabled. Kiosk Mode is a set of restrictions that defines what app the kiosks will run, and what device controls and features the user can access while using the app. Once the group is created, you can add devices to the group to configure them as kiosks. Any number of devices can be added to the group, and you can make any number of kiosk groups—one for each different app.



Note that only supervised iOS devices can be configured as kiosks.

Creating Kiosks

Creating kiosks requires two broad steps:

1. Create a group and configure it with Kiosk Mode enabled.
2. Assign devices to the group.

Creating and Configuring a Kiosk Group

To create kiosks, start by adding and configuring a new group. Note that when configuring this group, you can ignore the *Apps* and *Restrictions* tabs; the settings they contain are ignored once Kiosk Mode is enabled.

Complete the following steps:

1. Go to *MDM > Groups*.
2. Click the *iOS* icon.
3. Click *Add Group*.
4. Define a *Group Name*.
5. Click the *Configuration* tab if it is not already selected.
6. Define the settings in the Configuration tab as you would for a normal group.

Note that while you can add Web Clips to the group, they are unlikely to be used as kiosk devices are dedicated to a single app. Similarly, you can select email settings for the group, but they will only be used if the kiosk app has email capabilities.

7. Click the *Kiosks Mode* tab.
8. Select the *Enable Kiosks Mode (Single App Mode)* option to enable Kiosks Mode.
9. Use the *Select app to run in Single App Mode* field to select which app the kiosks will run.

Note that the app you select will be automatically installed on devices added to the group (if it is not already installed).



10. Select which device features should be *Always Enabled* (if any). If a feature is enabled, it will be always be active/available; users will not have the option to disable it.



You must enable the *Touch* option if you intend users to be able to use the device touchscreen.

- > Touch – enable this option to allow devices to respond to input from the touchscreen.
- > Motion (Screen Rotation) – enable this option to allow the screen orientation to rotate according to the device orientation.
- > Volume Buttons – enable this option to allow devices to respond to input from the volume buttons.
- > Side Switch – enable this option to allow devices to respond to input from the side switch. Note that the side switch is only present on certain iPad models.
- > Sleep/Wake Buttons – enable this option to allow devices to respond to sleep/wake commands generated by pressing the power button.
- > Auto-Lock – enable this option to have the device automatically lock after a defined period of inactivity.
- > Voice Over – enable this option to enable Voice Over mode, where the device automatically reads aloud whatever is touched on the screen using text-to-speech. Note that if you enable this accessibility feature here, it will always be enabled—users will not be able to turn it off.
- > Zoom – enable this option to enable zoom mode, which enlarges everything displayed on the device. Note that if you enable this accessibility feature here, it will always be enabled—users will not be able to turn it off.

Devices added to the group will adopt the current value of this option, but toggling the option has no effect on devices that are already members of the group.

- > Invert Colors – enable this option to invert the display colors. Note that if you enable this accessibility feature here, it will always be enabled—users will not be able to turn it off.

Devices added to the group will adopt the current value of this option, but toggling the option has no effect on devices that are already members of the group.

- > Assistive Touch – enable this option to enable the Assistive Touch feature, which allows users to replace certain touchscreen actions (such as pinching or double-tapping) with a single touch. Note that if you enable this accessibility feature here, it will always be enabled—users will not be able to turn it off.

Devices added to the group will adopt the current value of this option, but toggling the option has no effect on devices that are already members of the group.

- > Speak Selection – enable this option to enable the Speak Selection feature, which gives the user the option to have text they select read aloud using text-to-speech.

Devices added to the group will adopt the current value of this option, but toggling the option has no effect on devices that are already members of the group.

- > Mono Audio – enable this option to restrict audio output to mono audio. Note that if you enable this accessibility feature here, it will always be enabled—users will not be able to turn it off.



11. Select which *Accessibility Shortcuts* (if any) should be available when using the kiosk devices. If a shortcut is enabled, users will be able to turn the associated accessibility feature on and off according to their needs.
 - > Voice Over – enable this option to permit users to toggle Voice Over mode.
 - > Zoom – enable this option to permit users to toggle Zoom mode.
 - > Invert Colors – enable this option to permit users to invert display colors.
 - > Assistive Touch – enable this option to permit users to toggle Assistive Touch mode.
12. Click *Save*.

Adding iOS Devices to the Kiosk Group

To configure devices as kiosks, assign them to a group with Kiosk Mode enabled. Assigned devices must be supervised.

1. Go to *MDM > Devices*.
2. Click the *iOS* icon.
3. Use the checkboxes to select devices.
4. Click *Move To Group* and select the *[Group Name]*.



Frequently Asked Questions

1. What are the differences between a Work Managed Device and a BYOD device for Android?

A Work Managed Device is usually owned by the organization. A Work Managed Device gives complete control to the IT administrator. For example, the mobile user cannot install apps other than the one specified by the IT administrator.

A BYOD device is usually owned by the employee. BYOD gives more control to the mobile device user. The mobile device user can install apps from the Play Store in addition to the apps installed by the IT administrator.

2. Can I prevent users from uninstalling apps on a mobile device?

Yes. You can prevent users from uninstalling apps.

- > iOS devices: Go to *Groups > iOS > Group Name > Restrictions* tab and clear the *Allow app removal* checkbox. This option is available for supervised devices only.
- > Android devices: Go to *Groups > Android > Group Name > Restrictions* tab and clear the *Allow Uninstall* checkbox.

3. How to setup a Supervised device?

- > For Android: To set up the device as a supervised device, enroll the device as a Work Managed Device.
- > For iOS: To set up the device as a supervised device, enroll the device as a DEP device. Go to *Settings > DEP* and select *Place in Supervised mode*.

4. How can I track devices?

Go to *Groups > iOS (or Android) > Group Name > Configuration* tab and select the *Track Device Location* checkbox. The location of the device will now be visible in the Location column (Devices pane).



The Deep Freeze MDM mobile app must be installed on the mobile device and the app must have access to location data. The location tracking on the device must be enabled at all times to ensure tracking.

5. How can I uninstall all the apps without unenrolling the device?

Go to *Devices > iOS (or Android)*. Select one or more devices and click *Select Wipe*. The installed apps are removed from the devices.

6. How to install apps across all mobile devices from Deep Freeze Cloud?

Apps can be added to mobile devices by completing the following actions:

- > Adding Apps from the Apple App Store or Google Play Store
- > Selecting Apps in a group by creating a new group or editing an existing group.
- > Assigning Mobile Devices to the group.

For more information see [Managing Apps](#).

7. How to setup an Apple Push Certificate?



An Apple Push Certificate is required for the Deep Freeze MDM Mobile App to communicate with Deep Freeze MDM. An Apple Push Certificate can be configured by performing the following actions:

- > Go to *MDM > Settings > Push Certificate*. Click *Certificate Request* to download the Certificate Request. Save it on your computer.
- > Go to Apple Push Certificate Portal (<https://identity.apple.com/pushcert/>) and sign in with your Apple ID and password.
- > Click *Create a Certificate*. Click *Choose File*. Browse to select the *Certificate Request* file (.csr) from Deep Freeze MDM and click *Open*. Click *Upload*.
- > Click *Download* to download the Apple Push Certificate (.pem) and save it on your computer.
- > Go to *Deep Freeze Cloud > MDM > Settings > Push Certificate*. Click *Choose File*. Browse to select the *Apple Push Certificate* file and click *Open*. Specify the Apple ID. Click *Upload*.

For detailed instructions, go to [Creating an Apple Push Certificate](#).