



# ShadowControl CMD User Guide

## Table of Content

Table of Content	2
1 CMD Overview	3
1.1 CMD in Operation	4
2 Installing CMD	13
2.1 Installing the CMD Appliance	13
2.2 Installing the CMD Agent	14
3 Understanding the CMD Console	15
3.1 Navigation Panel	15
3.2 Main Panel	24
3.3 Session Panel	32
4 Using Status Rules	33
5 Reporting	35
5.1 Report Scheduling	35
5.2 Sample Report	37
6 Using the CMD Portal	38
6.1 Understanding the Portal Console	38
6.2 Using Org Groups	40
6.3 Portal Report Scheduling	41
6.4 Defining Portal Settings	42

# ShadowControl CMD User Guide

---

Welcome to the StorageCraft® *ShadowControl™ CMD User Guide*. This Guide describes the CMD monitoring technology, how to use the product, and how to derive maximum benefit from CMD.

This Guide includes the following major sections:

- [CMD Overview](#)
- [Installing CMD](#)
- [Understanding the CMD Console](#)
- [Using Status Rules](#)
- [Reporting](#)
- [Using the CMD Portal](#)

## Additional Information

For emerging issues and other resources, see the following:

- The CMD forum at [www.storagecraft.com/support/forum](http://www.storagecraft.com/support/forum).
- The StorageCraft technical support Web site at [www.storagecraft.com/support.html](http://www.storagecraft.com/support.html).
- This User Guide is also available from the Help menu on the CMD console.

## Documentation Conventions

⚠ This symbol designates Note or Warning text that highlights important information about the configuration and/or use of ShadowControl CMD.

# 1 CMD Overview

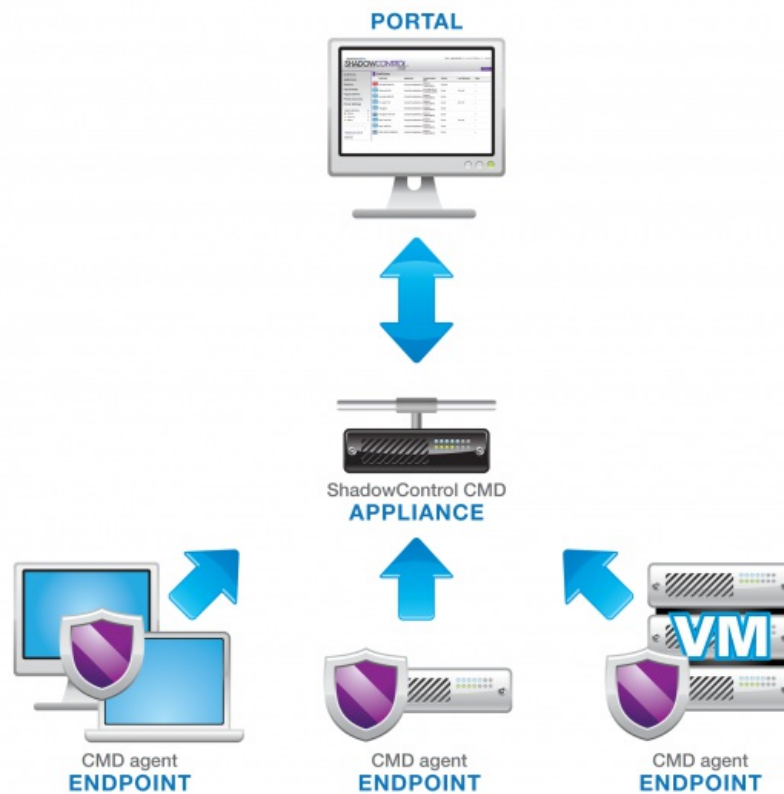
---

Welcome to ShadowControl™ CMD—the superior monitoring tool for ShadowProtect-guarded networks! CMD delivers a central monitoring and reporting console for ShadowProtect and ImageManager operations, either for large sites or for MSPs with multiple clients.

## Theory of Operations

CMD has three components:

- **CMD Appliance**--a Linux-based server running as a VM or on dedicated hardware
- **CMD Agent**--a client installed at each EndPoint
- **CMD Portal**--an optional feature for monitoring multiple CMD appliances



*CMD consists of EndPoints running the CMD agent, an appliance which monitors those Endpoints, and an optional Portal for monitoring multiple appliances.*

The CMD appliance receives status info from the CMD agent installed at each EndPoint. If there are multiple appliances, a CMD appliance can also serve as a Portal to monitor all the appliances and all their EndPoints.

## Administration Schema

To supervise these components, CMD provides a granular schema for administrative roles. These roles differ primarily in the scope of the EndPoints they oversee:

- A **Portal SuperAdmin** manages users and Org Groups on the portal as well as schedules reports on subscribed CMD appliances. A portal superadmin can also view the status of all EndPoints on all subscribed appliances.
- A **CMD SuperAdmin** manages the CMD appliance as well as add, edit, or remove all Organizations, Sites, EndPoints, user Accounts, and Rules applied to this specific appliance.
- An **administrator** can add, edit or remove sites as well as monitor all EndPoints for selected organizations on a specific appliance.
- A **Read-only** account on an appliance can view the status of EndPoints in one or more organizations or one or more sites on that appliance. (A Read-only account created at the Portal level can view the status of EndPoints in one or more organizations or sites from one or more appliances.)

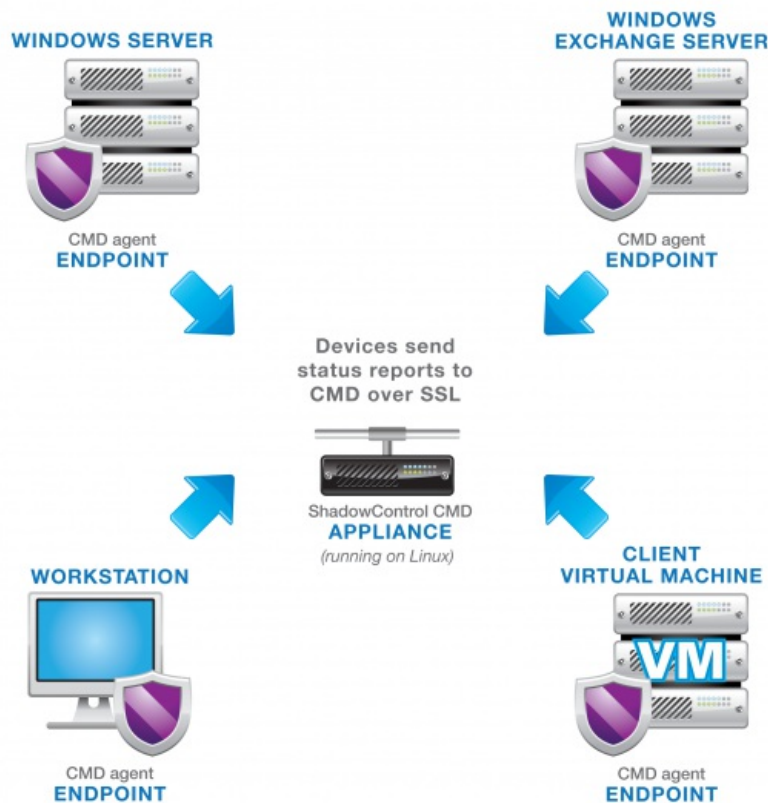
See [Administration](#) for further details on these roles.

## 1.1 CMD in Operation

To begin using CMD, an administrator would:

- Install the CMD appliance either on standalone hardware or as a virtual machine.
- Create one or more organizations to associate EndPoints with similar functions or locations.
- Create one or more sites within each organization to further associate EndPoints with similar requirements.
- Install the CMD agent on each ShadowProtect-guarded system.
- Assign each agent to an organization or to a site to monitor it using the CMD console.

The CMD appliance begins to receive a stream of status data over an encrypted link from each EndPoint every five minutes.



*Each CMD EndPoint reports to the CMD appliance using SSL over Port 443.*

## Status Rules

A major benefit of CMD is the ability to set alert thresholds--called *Status Rules*--on changes occurring in each EndPoint. Status rules can be set at the organization or the site level. Examples of status rules include the number of backup failures, online or offline status, and backup file size.

Using these status rules, the appliance can sort and display the EndPoints based on their condition:

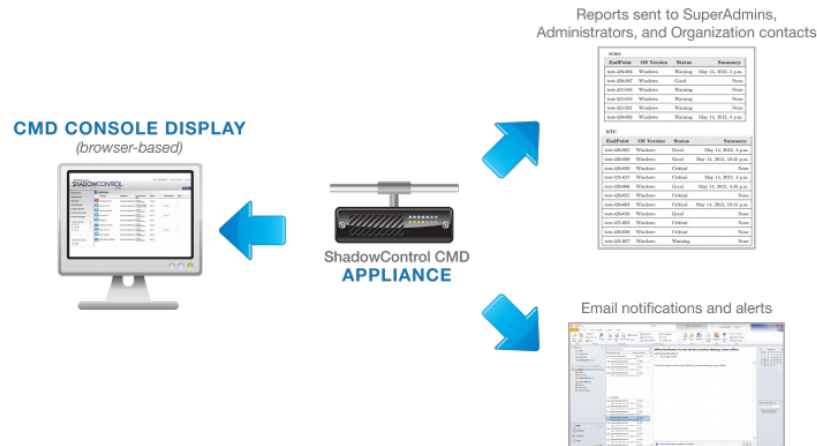
- **Good:** The EndPoint and backups are normal.
- **Warning:** Activity on the EndPoint has exceeded one or more status rule thresholds set at the "Warning" level.
- **Critical:** Activity on the EndPoint has exceeded one or more status rule thresholds set at the "Critical" level.
- **Offline:** The EndPoint is not reporting to the console.

## Notifications

Another benefit of CMD is the ability to send email notifications when an EndPoint exceeds the status rule thresholds. CMD can send these notifications to either or both administrators and other contacts responsible for the affected EndPoint.

## Reports

A final benefit is in scheduling reports. These reports can provide a range of content from a summary to a detailed backup report. CMD can send reports to administrators or other parties on a daily, weekly, or monthly schedule.



CMD displays EndPoint status information in the onscreen console as well as through email notifications and scheduled reports.

## The CMD Appliance

The CMD appliance is the heart of CMD. As mentioned, this Linux-based server receives status reports from each CMD client-equipped EndPoint, providing details on its ShadowProtect and ImageManager installations, backup activity, and hardware configuration details. Administrators use the appliance's browser-based console to:

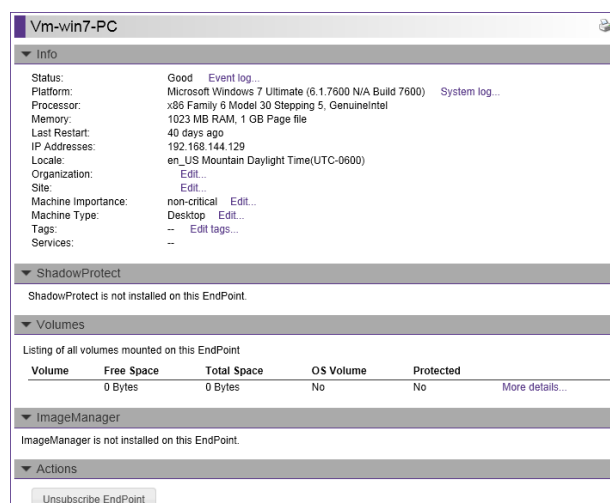
- Monitor EndPoints
- Set status rules for EndPoints
- Schedule reports

The appliance keeps a rolling 30-day log of EndPoint activity information for reporting purposes. Otherwise, all pertinent EndPoint data is maintained at the EndPoints. It is not necessary to perform backups on the appliance. In the event of an appliance failure, either a reboot or a reinstall restores monitoring operations. The replacement appliance then retrieves current status data from the EndPoints.

## The CMD EndPoint

Windows systems (both physical—servers, workstations, laptops—and virtual machines) can become EndPoints with the CMD agent installed. With the agent installed, each new EndPoint can subscribe to a CMD appliance and become a participating node in CMD.

**Note:** The CMD agent does not require ShadowProtect on the EndPoint. However, EndPoints that have ShadowProtect installed provides greater status details than systems with only the CMD agent.



*The CMD agent provides limited details when installed on a non-ShadowProtect-equipped EndPoint.*

## The CMD Portal

The CMD Portal is an optional component. The portal is a CMD appliance which acts as a supervisor for two or more subscribed appliances. It therefore acts similar to the CMD console—displaying the status of EndPoints—with the added benefit that it does this for multiple CMD appliances rather than just one. The Portal supports organizations looking to scale their StorageCraft protection at multiple sites with greater fine-tuning in reports and alert levels.

Administrators can use a portal to:

- Set system-wide status rules for all organizations or sites on the monitored appliances
- Create sets of organizations into Org Groups from various appliances
- Specify status rules for selected Org Groups
- Define system-wide or Org Group-specific reporting schedules

## Dedicated Operation

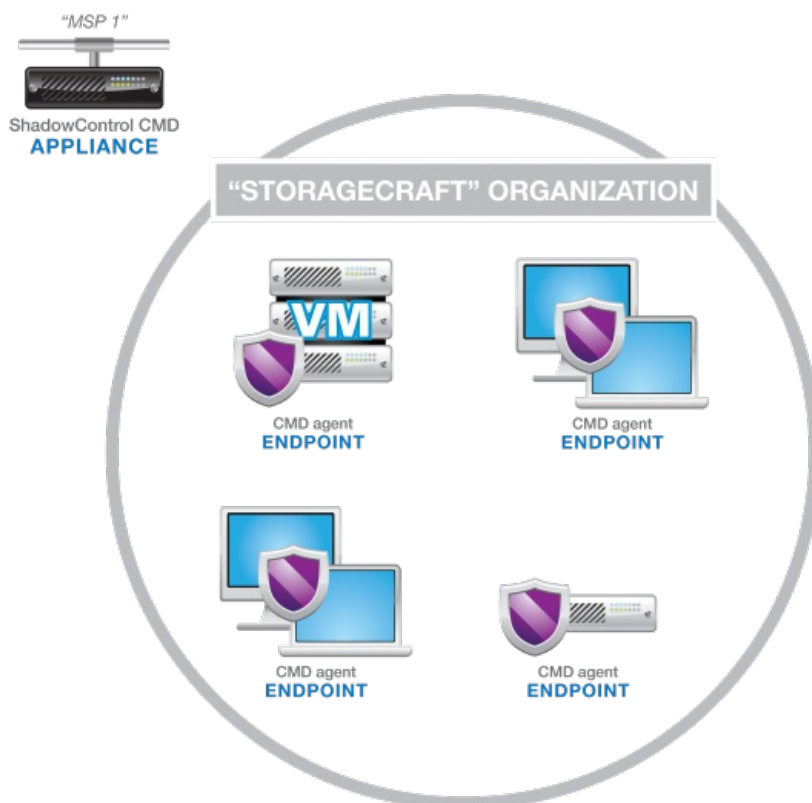
Although the Portal is a standard CMD appliance with the Portal feature activated, we recommend that the Portal be a dedicated install of CMD rather than an "upgrade" of an existing appliance. However, if an existing CMD appliance is upgraded to run as a Portal, the original EndPoints will remain monitored by the Portal appliance. In that case, an additional navigation menu option will appear ("EndPoints") to display the list of monitored devices.

## Org Groups

As CMD's span of control increases with multiple appliances, administrators can define sets of organizations into [Org Groups](#). These Org Groups can include one or more organizations from each of the subscribed appliances.

## Organizations and Sites

CMD administrators can group EndPoints into organizations and sites for ease of management:



**Note:** Although "organization" and "site" imply a company name or physical location, these groupings can represent any common characteristic shared by a set of EndPoints. They can also represent a reporting group--where particular individuals need reports on the selected EndPoints.

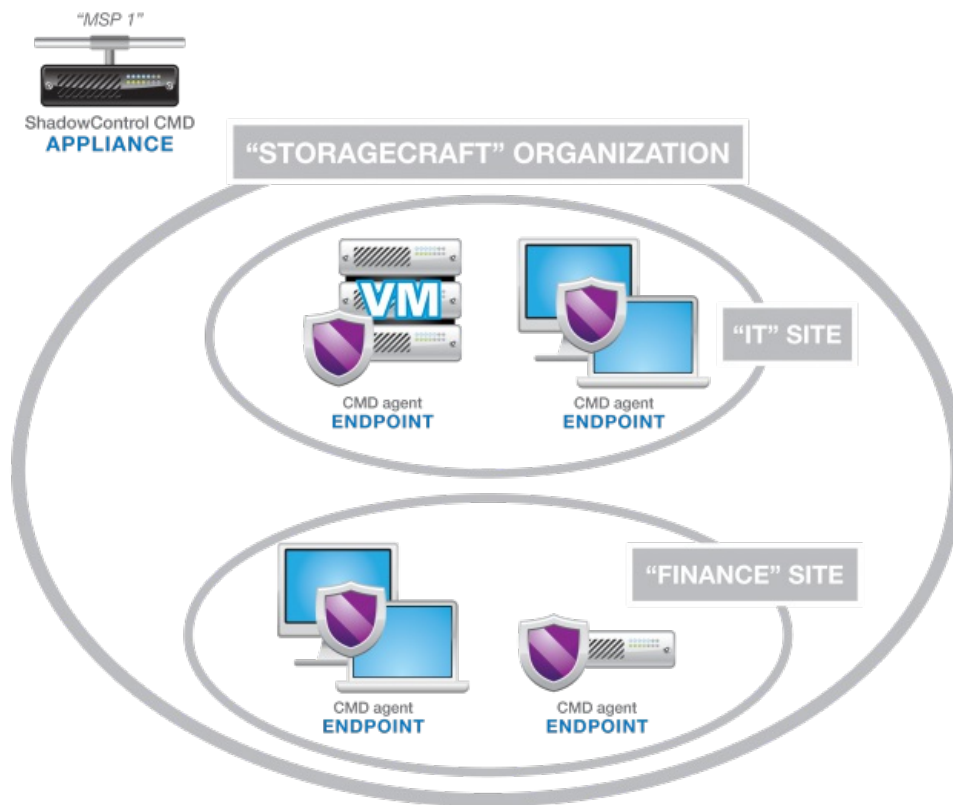
Each organization or site can also have its own set of Status Rules, allowing a high degree of granularity for alerts. For example, a "Servers" organization could have rules specific to their critical role, while a "Laptops" organization could have more lenient rules appropriate to that platform.

## Default Organization and Site

The CMD appliance includes a Default Organization with a Default Site. CMD assigns all new EndPoints to this Default Organization and Site unless the EndPoints are assigned to a defined organization or site during the subscription process. We recommend assigning each EndPoint to an appropriate organization or site rather than keep EndPoints in the Default Organization and Site.

## Using Sites

A CMD organization can be further subdivided into one or more sites:



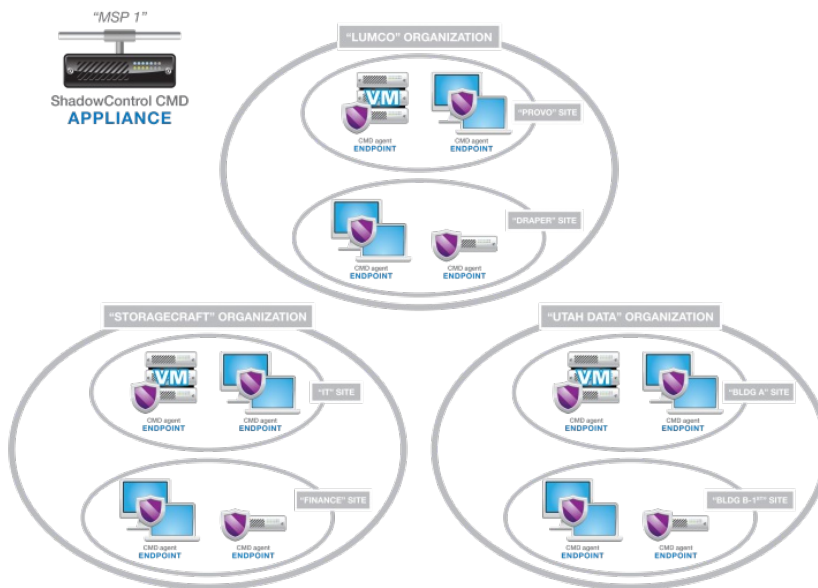
All EndPoints should belong to a defined organization. However, sites are an optional subdivision to an organization. Although optional, sites are useful in focusing attention on specific EndPoints within an organization. They also provide a convenient way to send different individuals (as contacts or administrators) notifications and reports based on their individual roles.

Again, while the name "Site" implies a physical location, a CMD site can represent any shared relationship or characteristic between a set of EndPoints. A relationship could include a company role, division, product, or location. A site could also represent characteristics such as operating system, application, or hardware type.



## Multiple Organizations and Sites

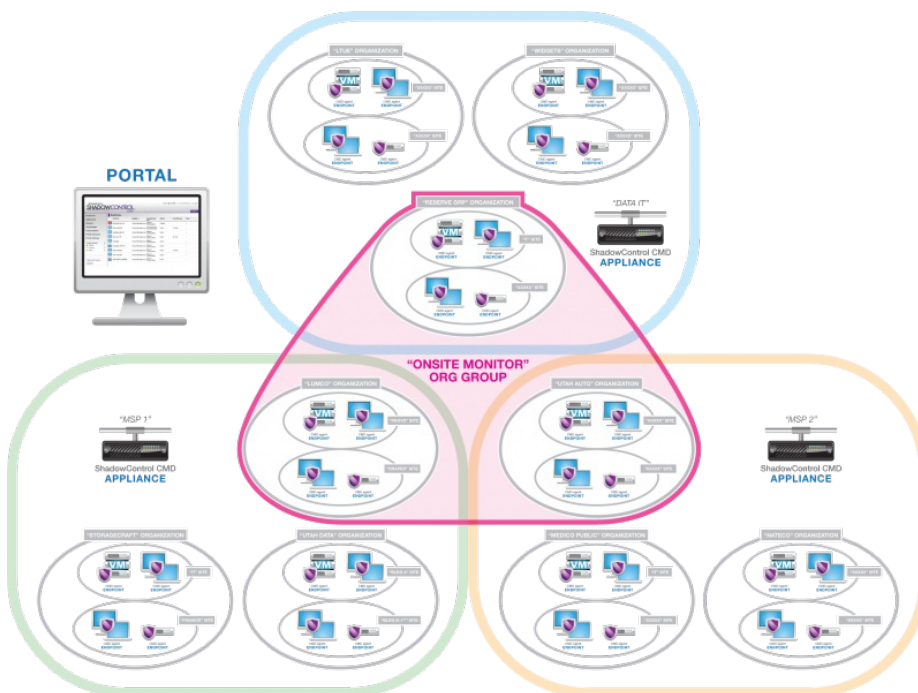
Each appliance can support multiple organizations, each with its own set of sites:



By defining multiple organizations and sites, administrators have a convenient way to send different individuals (as contacts or administrators) notifications and reports based on their roles or area of responsibility. MSPs can define organizations and sites to closely match their client base and their EndPoints.

## CMD Portal Org Groups

Administrators who implement a portal have an additional level of grouping called the *Org Group*. An Org Group is made up of selected sites and organizations from one or more monitored appliances:



Like an individual appliance's organization or site, a portal's Org Group can have separate status rules that flow down to each of its organizations and sites.

**Note:** Assigning status rules to an Org Group overrides any existing status rules applied at the appliance level to the sites or organizations that are part of the Org Group.

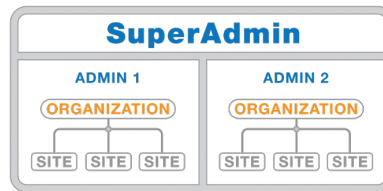
An Org Group can also have a separate set of contacts for notifications and reports.

## Administration

As described earlier, CMD provides a granular schema for administrative roles:

- A **Portal SuperAdmin** manages the portal service and monitors all the portal's subscribed CMD appliances and their EndPoints. A portal superadmin can set status rules for all appliances, schedule reports and their recipients on these appliances; add, edit, or remove Org Groups; and administer user accounts on the portal.
- A **CMD SuperAdmin** manages the CMD appliance and can add, edit, or remove all organizations, sites, and EndPoints; and administer user accounts. The CMD superadmin can also set the Status Rules at the organization and site levels.
- An **administrator** can add, edit or remove sites as well as monitor all EndPoints for selected organizations on the appliance or portal.
- A **Read-only** account on an appliance can view the status of EndPoints in one or more selected organizations or one or more selected sites on that appliance. (A Read-only account created at the portal level is similar. A portal-level read-only account can view the status of EndPoints in one or more organizations or sites from one or more appliances.)

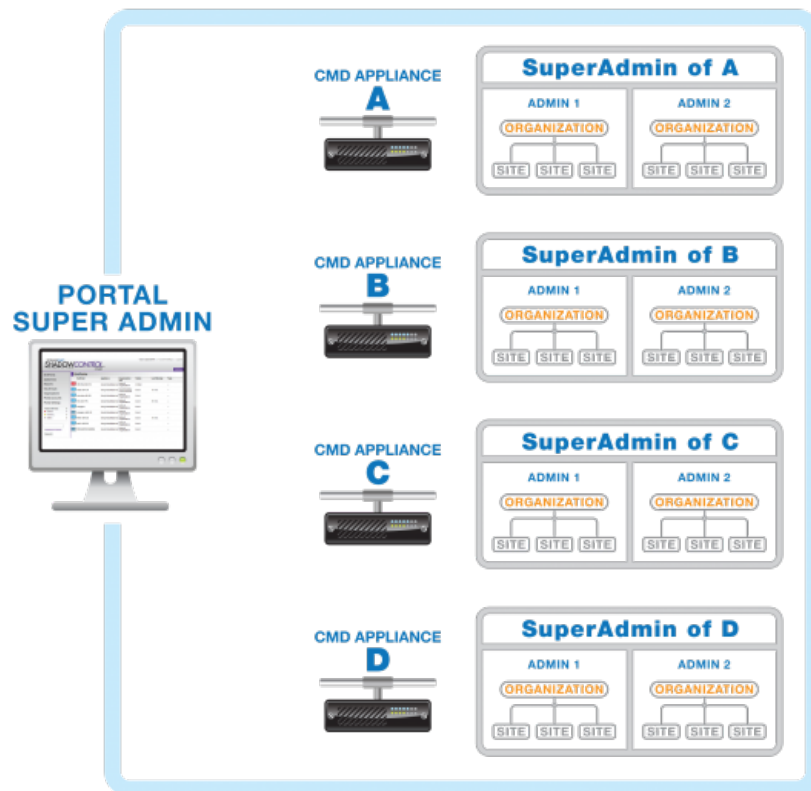
A typical CMD appliance would have one SuperAdmin and several administrators handling the organizations, sites, and EndPoints:



*Administrators on a CMD appliance can monitor EndPoints in one or more organizations or sites.*

The SuperAdmin can define as many administrators and read-only accounts as needed. (For example, additional read-only accounts can be for different personnel to receive notifications or reports.) The SuperAdmin can also assign additional users with SuperAdmin rights if needed to administer the appliance and appliance accounts.

On portal-equipped sites, there is a portal SuperAdmin to oversee subscribed appliances:



*Portal SuperAdmins monitor two or more CMD appliances.*

Again, the Portal SuperAdmin can define additional accounts as needed for reporting or notifications. The Portal SuperAdmin can also assign accounts to monitor specific EndPoint assignments as part of an Org Group.

## Reports

CMD offers three possible sections in a report:

- **EndPoint Summary:** A general report on the monitored EndPoints
- **EndPoint Status:** Provides details on each EndPoint
- **Backup Status:** Lists of the last backup performed on each EndPoint

Reports can be sent to SuperAdmins, administrators, and to organization contacts on each appliance.

**Note:** Portals do not issue reports. Instead, reports defined for an Org Group is handled by multiple reports issued from each of the organizations that are part of the Org Group.

## Report Scheduling

CMD can schedule reports:

- Daily (beginning of the day)
- Weekly (first day of the week)
- Monthly (first day of the month)

**Note:** Report scheduling reflects how often CMD sends a report. It does not reflect the report's contents. Reports reflect only the current status at the time the report is generated. (CMD sends reports at 12:00AM.) For example, a Monthly report is a report that is sent once a month. It does not include a monthly summary of activity for that period.

The CMD Reports dialog displays a list of the last report sent of each type. Selecting a report in this list displays the archived content.

## Report Recipients

SuperAdmins and administrators designate the recipients and the type of report sent (Summary, Status, or Backup Status). The report's recipient dictates which set of EndPoints the report covers:

- **Portal SuperAdmins:** All EndPoints monitored by the portal.
- **CMD SuperAdmins:** All organizations on a specific appliance.
- **Portal Administrators:** Reports on the administrators' designated sub-set of organizations or Org Groups on the portal from one or more appliances.
- **CMD Administrators:** Reports on the administrators' designated sub-set of organizations on a specific appliance.
- **Portal Contacts:** Reports to a single Org Group's contacts.
- **CMD Contacts:** Reports on an organization to the primary or secondary contact for that organization on a specific appliance.

## CMD Scenarios

The concept of centrally monitoring ShadowProtect devices is extremely powerful, particularly for today's business environments where devices quickly multiply. CMD lets you keep tabs on these devices in ways that were previously not possible, as illustrated by the following usage scenarios.

### Custom Rules

**Problem:** You need to keep track of different groups and types of machines across your organization. At the same time, you must have certain rules that apply to everyone and you don't want to manage them for each machine.

**CMD Solution:** ShadowControl CMD uses *Organizations* and *Sites* to create a hierarchy where you can set global rules, while maintaining custom monitoring where you need it.

- Set up your hardware and your organizations and sites.
- Set global status rules for your environment.
- Customize rules for the organizations and sites that need them.

For example, suppose you've organized your EndPoints by department and then by data priority, such as an "Accounting" organization with a subset of vital machines in a "Critical" site. You can set custom rules for the "Accounting" organization, then even more detailed rules for the subset of machines in the "Critical" site.

### Device Priority

**Problem:** Your IT staff has only so much time. They can't always address every individual problem right away, but you know for sure that a problem with a server needs immediate attention while a problem with an employee laptop could be addressed later. You need a way to monitor what's happening by machine type.

**CMD Solution:** ShadowControl CMD gives you ways of seeing the status information you need. It's easy to distinguish between different machine types.

- Install the ShadowControl CMD agent on each server, desktop, and laptop. Subscribe each to a CMD appliance.
- In the ShadowControl CMD console, select each EndPoint and designate it as a Server, Desktop, or Laptop using the provided dropdown.
- Filter through your EndPoints on machine type. (Machine type serves as a predetermined tag for an EndPoint, allowing searches to find them when you need to.

## Senior Management Reports

**Problem:** It's budget time and executives have asked you to let them know how well your backup and disaster recovery plan performs. They need to know if it warrants continued investment. You need a way to generate a report that details your entire backup environment.

**CMD Solution:** ShadowControl CMD lets you create detailed reports for your entire business or any of your individual segments.

- Open the CMD console.
- Select the individual organizations and sites you want reports on. (Or, you can create reports for your entire backup environment.)

- Determine who should get the report. You can associate specific contacts with specific organizations and sites, so it's easy to make sure reports go to the right place. CMD sends reports on a schedule you define, but you can also generate them on demand.

## 2 Installing CMD

---

ShadowControl CMD installs as two components on separate systems:

- [The CMD Appliance](#): A Linux-based system installed on standalone hardware or as a Virtual Machine
- [The CMD Agent](#): A Windows-based client installed on each monitored device.

### 2.1 Installing the CMD Appliance

---

The CMD Appliance installs on standalone hardware or as a Virtual Machine. Both installations use the same ShadowControl\_CMD.iso file.

#### System Requirements

Before installing the CMD appliance, make sure your system meets the following requirements:

- The CMD appliance is based on the 64-bit Ubuntu 12.04 operating system. If you choose to run the appliance on standalone hardware, please review [the Ubuntu 12.04 Supported Hardware Page](#) for detailed requirements for running Linux on various platforms.
- The CMD appliance can also run as a virtual machine on:

- o Microsoft Hyper-V
- o VMWare Workstation
- o VMware ESX/ESXi

**.Note:** Xen and Oracle VirtualBox are currently not supported.

- The appliance's CPU, disk space and RAM requirements are primarily determined by the number of EndPoints that subscribe to the Appliance. As a minimum for either a hardware- or VM-based appliance, we recommend:

- o 2GB RAM
- o 80GB disk space
- o Dual-core processor

- Active Internet connection (to download server components during the install)
- An available IP address (for remote console access)
- Port 443 or 8443 available (for EndPoint-to-appliance and appliance-to-portal communication)
- Port 22 available (only used if the appliance will act as a portal)

#### Using a Domain Hostname

You have the option to use a Domain Hostname rather than an IP address for subscribing EndPoints to the appliance. This allows you to change the appliance's IP address as needed without having to resubscribe EndPoints to that appliance. To use a hostname, however, you will first need to manually create a hostname entry on your DNS server for the appliance's IP address prior to installing CMD.

#### To install the CMD Appliance

1. Boot the physical or virtual machine using the ShadowControl\_cmd.iso.

**Note:** If you are using a physical destination, first burn the CMD ISO to a CD.

2. Select the install language, then click **OK**.
3. On the CMD Wizard *Welcome* page, click **Next**.
4. Follow the steps in the Installation Wizard to install the CMD software.

**Note:** The Install process may run for 10 to 15 minutes or more as it downloads updates. The Install process may then appear to hang, but this extended installation is normal.

5. When the installation completes, click **Finish**. The CMD appliance will begin to run.

All further configuration occurs through the browser-based console. To access the console, open a browser to <https://IPaddress> where *IPaddress* is the address you gave the CMD appliance during the installation.

Note that if you need to reboot or shutdown the appliance, you can do so from this console.

## 2.2 Installing the CMD Agent

---

You must install the CMD agent software on each device you want to monitor.

### System Requirements

These include:

- CMD client's hardware and software requirements are the same as for [ShadowProtect](#).
- CMD supports ShadowProtect versions 4.x and newer.
- The agent communicates with the CMD appliance using Port 443 or 8443 (selectable during installation).

**Note:** While you can monitor devices that do not have ShadowProtect, CMD only provides minimal detail on those systems.

### Installation

To install the agent:

1. Download and run the ShadowControl\_CMD\_Setup\_1.0.2.exe file.
2. In the Setup Wizard, select the language to install. Click **Next**. The Welcome page displays.
3. Click **Next**. The License Agreement page displays. If you wish to review the the agreement, click **Print** to print out a copy.
4. Select I accept the terms of the license agreement. Click Next.  
**Note:** You must accept the license agreement to install CMD.
5. Enter the IP address or hostname for the CMD appliance.
6. Optional: Specify that the agent use the alternative Port 8443 to communicate with the appliance. (Select this only if the default port 443 is in use by another application.)
7. Optional: Specify the organization or site where you want to place this EndPoint. Enter the names exactly as configured or the enrollment won't occur.  
**Note:** Specifying an organization or site eliminates the need to approve the EndPoint enrollment later.
8. Enter the credentials needed to log into the CMD appliance.
9. Click **Next**.
10. Click **Install**.
11. Click **Finish** when the install completes.

The new EndPoint will now appear in the list of subscribed devices. CMD attempts to identify the machine type (Server, Desktop, Laptop, or Virtual Machine) and enter that in the EndPoint's details. If the machine type is incorrect (as shown in the EndPoint list), use the [Info section](#) of the EndPoint Details page to change it.

**Note:** If you did not provide valid credentials or enrollment details, the new EndPoint appears in the list with a request to **Approve** or **Deny** its subscription. A CMD administrator or superadmin must approve the new EndPoint to add it. CMD does not monitor this device until approved.

### Working with Windows 2000 and Other Non-VSS Systems

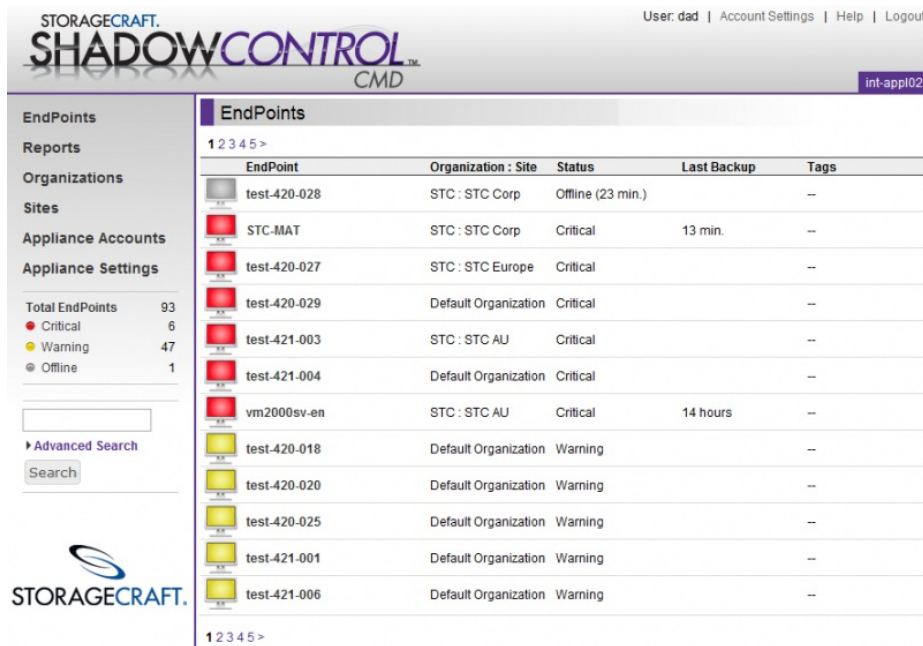
Windows 2000 does not support VSS backups. However, a default CMD Status Rule produces an alert for each non-VSS backup. This results in a continuous flow of notifications for Windows 2000 backups. To avoid this:

1. Create an organization or site for these devices. Name this group "*Non-VSS Systems*" or similar.
2. Group all Windows 2000 devices (and all other non-VSS systems) into this site or organization.
3. Select the non-VSS site or organization and open its *Status Rules* page.

4. Uncheck the **Non-VSS Backup** rule to disable it. This prevents the issuing of notifications for these EndPoints. EndPoints that do use VSS keep the Non-VSS rule and generate alerts if VSS fails.

## 3 Understanding the CMD Console

The CMD console displays current EndPoint status information and provides access to the configuration and operating controls for CMD:



STORAGECRAFT. SHADOWCONTROL™ CMD

User: dad | Account Settings | Help | Logout

int-appl02

EndPoints

1 2 3 4 5 >

EndPoint	Organization : Site	Status	Last Backup	Tags
test-420-028	STC : STC Corp	Offline (23 min.)		--
STC-MAT	STC : STC Corp	Critical	13 min.	--
test-420-027	STC : STC Europe	Critical		--
test-420-029	Default Organization	Critical		--
test-421-003	STC : STC AU	Critical		--
test-421-004	Default Organization	Critical		--
vm2000sv-en	STC : STC AU	Critical	14 hours	--
test-420-018	Default Organization	Warning		--
test-420-020	Default Organization	Warning		--
test-420-025	Default Organization	Warning		--
test-421-001	Default Organization	Warning		--
test-421-006	Default Organization	Warning		--

1 2 3 4 5 >

STORAGECRAFT.

The console is divided into three panels:

**Navigation Panel:** Located at the left side of the console, the Navigation panel provides options for tasks and configuration needed to monitor subscribed EndPoints. (For more information, see [Navigation Panel](#).)

**Main Panel:** Located at the center of the console, the Main panel displays lists of EndPoints or configuration details. (For more information, see [Main Panel](#).)

**Session Panel:** Located at the top right of the console, the Session panel displays the current username and appliance as well as session options. (For details, see [Session Panel](#).)

### 3.1 Navigation Panel

The left-side Navigation panel provides access to CMD tasks and tools:



EndPoints

Reports

Organizations

Sites

Appliance Accounts

Appliance Settings

Total EndPoints93

● Critical6

● Warning47

● Offline1

Advanced Search

Search

The items include:

**EndPoints:** Displays a list of subscribed devices to the appliance in the Main Panel. (This is the default view.) This option will also display the name of a selected EndPoint if an EndPoint is selected in the list. (See [EndPoint List](#) for more information.)

**Reports:** Displays Report settings and an archived report list. (See [Reporting](#) for more information.)

**Organizations:** Displays a list of organizations currently defined on the appliance. Use this option to add, edit, or remove organizations on the appliance; or to view and modify the Status Rules for a selected organization (See [Using Status Rules](#) for more information.)

**Note:** CMD will not delete the Default Organization cannot be deleted. However, administrators can modify the Default Organization's Status Rules.

**Sites:** Displays a list of currently defined sites on this appliance. Use this option to add, edit, or remove sites from the appliance. (Refer to [Sites](#) for more information.)

**Appliance Accounts:** Displays a user list to add, edit, or remove users. (See [Appliance Accounts](#) for more information.)

**Appliance Settings:** Displays the appliance's settings. (See [Appliance Settings](#) for more information.)

**EndPoint Summary:** Displays the total number of EndPoints with a breakdown of their conditions. (See [EndPoint Summary](#) for more information.)

**Search:** Displays a list of EndPoints that match specified search terms or criteria. (See [Search](#) for more information.)

**Newsfeed:** Displays a scrolling list of content on StorageCraft and ShadowControl CMD. (This feature is available in English only.)















## Sites

The Sites option displays a list of currently defined sites on this appliance:



## Sites

Sites are a subset of EndPoints in an Organization that share common settings or a common location.

Site	Organization	Actions
acme north	acme	 
acme south	acme	 
STC AU	STC	 
STC Corp	STC	 
STC Europe	STC	 
XYZ Bldg 2	XYZ Corp	 
XYZ Bldg 2	acme	 

[+ Add Site](#)

To work with a site, you can choose the:

- **Actions** menu to the right to edit or delete the site.
- **Add Site** button at the bottom to add a new one.

## Actions

You have two actions available when working with a selected site:

### Icon Description

### Function



Blue pencil icon

Opens the selected site's configuration page. Use this page to edit the site's name, contacts, or status rules. (See [Using Status Rules](#) for more details.)



Red delete icon

Deletes the selected site. EndPoints that were part of the deleted site revert back to the pool of EndPoints within the organization that held the site.

## Add Site

Click **Add Site** to add a new site to an organization:

### Add Site

Site Name:

Organization:

#### ▼ Contacts

Fill in primary and secondary contact information:

#### Primary Contact

Email Address:

First Name:

Last Name:

Phone:

Company:

Street Address:

City:

State/Province:

Country:

Postal Code:

Preferred Language:

#### Secondary Contact

Email Address:

First Name:

Last Name:

Phone:

Company:

Street Address:

City:

State/Province:

Country:

Postal Code:

Preferred Language:

### To add a new site:

1. Type in a name for the new site. Select a name that reflects the shared characteristic of the EndPoints in this group. This could be a location ("Second Floor"), or it could be a department ("Finance") or a platform ("Windows XP" or "Windows 2K").






**Note:** Site names support multi-lingual characters. However, these names do not support reserved control characters such as "&", "?" or similar.

2. If the site has separate contacts (as opposed to the administrator), type in their information. By typing in valid email addresses, these contacts can also receive reports on the site's EndPoints. Specify the contact's preferred language so CMD will send appropriately formatted reports to that contact.
3. Decide to either use the organization's Status Rules or to define custom rules for this site. (See [Using Status Rules](#) for details.)
4. Click **Save** to save the new site.

New EndPoints can now enroll into this site or the administrator can edit an existing EndPoint's settings to make it a member of this site.

## Appliance Accounts

Appliance Accounts displays a list of the defined users for the appliance:

Accounts				
Username	Email	Role	Organizations	Actions
dad	dad@example.com	Superadmin		
Iara	Iara@example.com	Superadmin		 
superadmin	superadmin@example.com	Superadmin		 
<a href="#">+ Add User</a>				

### Actions

You have two actions available when working with a selected user account:

#### Icon Description Function



Blue pencil icon

Opens the selected account's configuration page. Use this page to edit the user's name, email address, language or role.



Red delete icon

Deletes the selected user account. Note that CMD will not delete the currently logged-in user.

### Add User

The Add User button opens a page where you can add a new user to the appliance.

**Add User**

Configure user account settings for logging into this appliance.

Username:

Password:

Confirm Password:

Email:

Preferred Language: English ▼

Choose a role to set the new user's access:  
**Superadmin** - grants full access.  
**Admin** - grants access to manage only assigned Organizations.  
**Read Only** - grants read-only access to assigned Organizations.

Role: Superadmin ▼

Save

To add a user:

1. Type in a name, password, and valid email address for the user. (The email address is optional, but without it the user does not receive notifications.)
2. Select a preferred language for reports and notifications sent to this user.
3. Select the user role.
4. Selecting either the *Admin* or *Read-Only* user role displays a list of available organizations to assign to this user:

Role: Admin ▼

Organizations:

No access to the following:

- acme (int-appl02)
- STC (int-appl02)
- XYZ Corp (int-appl02)
- acme:acme north (int-appl02)
- acme:acme south (int-appl02)
- STC:STC AU (int-appl02)
- STC:STC Corp (int-appl02)
- STC:STC Europe (int-appl02)
- XYZ Corp:XYZ Bldg 2 (int-appl02)
- acme:XYZ Bldg 2 (int-appl02)

Allow user access to:

Grant Access >>>  
<<< Remove Access

4. To assign an organization to the new user, highlight one or more organizations in the left column.
5. Click **Grant Access**. (Use **Remove Access** to unassign an organization for this user.)
6. Click **Save** to create the new user account.

## Appliance Settings

The Appliance Settings option in the Navigation panel displays the system's current settings:

int-appl02

Subscriptions

This appliance is subscribed to Portal:

Portal Address:	255.255.254.9
Portal IP Port	443

Unsubscribe

Email Settings

Configure SMTP Server and settings used to send reports and alert notifications.

☒ Use this appliance's built-in SMTP server.

From Address:

☐ Use another SMTP server:

Host Name or IP Address:

Port:

Username:

Password:

From Address:

Security: ☐ Use TLS

☐ Don't use an SMTP server. (Warning: if this option is selected, no email will be sent from this appliance)

Save

Send Test Email

Network Settings

Configure network settings for this appliance.

IP Address:

Subnet Mask:

Default Gateway:

DNS Server:

Save

System Info

Version: CMD v1.0.0.17633 [ 1.4-4, 4]

Access Code: asdfasdf

Reboot Appliance

Shut Down Appliance

The sections include:

- [Subscriptions](#)
- [Email Settings](#)
- [Network Settings](#)
- [System Info](#)

## Subscriptions

An appliance can subscribe to a CMD Portal to scale the system for multiple appliances. A portal provides a single view to monitor all EndPoints on all appliances in the CMD system. Each individual appliance's console however remains available. Administrators at that appliance can then continue to monitor that appliance's specific EndPoints using that console.

**Note:** These local CMD appliance administrators could be recreated at the portal level and assigned to this appliance's organizations. However, this requires maintaining a second set of credentials for those administrators.

If this appliance is already subscribed to a portal, the Subscriptions section shows the portal's domain name or IP address and port number.

To *subscribe* to a portal:

1. Type in the portal's Domain hostname or IP address.
2. Accept the default port address (443) or type in the port used by the portal.
3. Click **Subscribe**.

This appliance now appears in the portal console. (See [The CMD Portal](#) for more information.)

To *unsubscribe* from the portal, click **Unsubscribe**.

## Email Settings

Email Settings specifies the SMTP server used to send notifications regarding EndPoint issues. There may be circumstances when you do not want to configure an email server (such as a temporary halt to notifications for testing purposes). However, we recommend that each appliance have an SMTP server configured for sending email.

To configure the email settings:

1. Choose whether to use the default CMD SMTP server or an existing SMTP server.
2. Keep the selected *Built-in SMTP* option to use CMD's SMTP server.
3. Enter an address in the *From Address* field. (This does not have to be a valid address.)
4. Select *Use another SMTP server* to send notifications with an existing server.
5. Specify this server's settings including credentials and whether to use TLS. Enter an address in the *From Address* field as well.
6. Click **Save**.
7. Click **Send Test Email** to confirm the connection.

**Note:** Sometimes email sent from the CMD server may bounce or be routed to a Spam folder on the destination system. Click **Send Test Email** to determine if this is the case. If so, configure CMD to use an existing SMTP server.

## Network Settings

The *Network Settings* section displays the appliance's configured DNS/IP settings. Edit these settings should the network configuration change.

**Note:** Editing the IP address may also require changes at the DNS server. This will be true if any EndPoint uses a host name rather than an IP address to subscribe to the appliance.

## System Info

System Info provides details on the appliance software and options to control the server:

▼ System Info

Version: CMD v1.0.0.17633 [ 1.4-4, 4]

Update Appliance

Access Code: asdfasdf

Reboot Appliance

Shut Down Appliance

These include:

Item	Description
<b>Version</b>	Reports the software version for the CMD appliance (not the Linux version it runs on).
<b>Access Code</b>	Displays the user-defined code that may be used by StorageCraft Support in troubleshooting appliance issues. Treat this as similar to a password.
<b>Reboot Appliance</b>	Click this button to reboot the appliance if a reboot is necessary. (The CMD appliance does not have command line access so it can't be used for reboots.)
<b>Shut Down Appliance</b>	Click this button to gracefully shutdown the appliance.
<b>Update Appliance</b>	Click this button to perform an automatic update to the appliance. <b>Note:</b> This button only appears when CMD detects the availability of an update to the appliance software.

## EndPoint Summary

The EndPoint Summary lists the total number of subscribed EndPoints. It then breaks down the total by status: Critical, Warning, and Offline.

Total EndPoints	92
● Critical	7
● Warning	36
● Offline	2

Click on the status to display in the Main panel a filtered list of the EndPoints with that status.

## Search

The Search function provides a way to filter the list of EndPoints shown in the Main panel.

**Note:** The Search feature appears only when the Main panel displays the EndPoint List.

To do a search:

1. Enter one or more search terms into the Basic Search box. (Search supports multi-lingual characters.)
2. Click **Search**.

CMD displays a list of any EndPoints that match those search terms in the Main panel.

To search for these terms in only a subset of EndPoints, rather than all the EndPoints on the appliance, click **Advanced Search**. You can then select one or more characteristics of EndPoints such as Name, Organization, Site, Tags, Machine Type, and Status to search in:

✕

**▼ Advanced Search**

**Search by**

☒ Name  
☒ Organization  
☒ Site  
☒ Tags

**Type**

☒ Server  
☒ Desktop  
☒ Laptop  
☒ Virtual

**Status**

☒ Good  
☒ Warning  
☒ Critical  
☒ Offline

After you select the characteristics of the EndPoints you want to search, you can click **Search**. (A search term isn't necessary.) The EndPoint List in the Main panel will change to display only those EndPoints that meet those search criteria.

For example, to display all EndPoints that are servers:

1. Uncheck *Desktop*, *Laptop*, and *Virtual* under Type. Leave *Server* checked.
2. Click **Search**.

The EndPoint List now displays only the servers subscribed to this appliance.

Enter one or more search terms to find matches in the EndPoint list. Click **Search** to display them.

You can also search for EndPoints with various characteristics using Advanced Search. For example, to search for a status list or EndPoints that match a search term, check at least one machine type. Next, check the status you want to view. Click **Search**. CMD displays all EndPoints of the selected machine type that also have the selected status.








**Note:** You must select at least one machine type when doing an advanced search. Otherwise, the search will fail.

## Organizations

The Organizations option displays a list of the currently-defined organizations on this appliance:

## Organizations

Organizations are collections of EndPoints.



<input type="checkbox"/> Organization	Actions
<input type="checkbox"/> acme	 
<input type="checkbox"/> STC	 
<input type="checkbox"/> XYZ Corp	 
<input type="checkbox"/> Default Organization	

You can work with organizations using the:

- **Actions** menu at the right to edit or delete organizations.
- **Add Organization** button at the bottom to add a new one.
- **Edit Rules** button to edit the selected organization's status rules.

## Actions

You have two actions available when working with a selected organization:

Icon	Description	Function
	Blue pencil icon	Opens the selected organization's configuration page. Use this page to edit the name, contacts, or status rules. (See <a href="#">Using Status Rules</a> for more details.)
	Red delete icon	Deletes the selected organization. EndPoints that were part of the deleted organization revert back to the Default Organization.

**Note:** You cannot delete the Default Organization.

## Add Organization

Click **Add Organization** to add a new organization:

### Add Organization

Organization Name:

▼ Contacts

Fill in primary and secondary contact information:

Primary Contact	Secondary Contact
Email Address: <input type="text"/>	Email Address: <input type="text"/>
First Name: <input type="text"/>	First Name: <input type="text"/>
Last Name: <input type="text"/>	Last Name: <input type="text"/>
Phone: <input type="text"/>	Phone: <input type="text"/>
Company: <input type="text"/>	Company: <input type="text"/>
Street Address: <input type="text"/>	Street Address: <input type="text"/>
City: <input type="text"/>	City: <input type="text"/>
State/Province: <input type="text"/>	State/Province: <input type="text"/>
Country: <input type="text"/>	Country: <input type="text"/>
Postal Code: <input type="text"/>	Postal Code: <input type="text"/>
Preferred Language: <input type="text" value="Chinese (Simplified)"/>	Preferred Language: <input type="text" value="Chinese (Simplified)"/>

**To add a new organization:**

1. Type in a name for the new organization. Select a name that reflects the shared characteristic of the EndPoints in this group. This could be a location ("Second Floor"), or it could be a department ("Finance") or a platform ("Laptop" or "Windows 2K").  
**Note:** Both organization and site names support non-English characters. They do not, however, support control characters such as "&", "?" and similar.
2. If the organization has separate contacts (in addition to the administrator), type in their information. By typing in valid email addresses, these contacts can also receive reports on the site's EndPoints. Select the contact's preferred language so CMD sends the report in the appropriate language.
3. Decide to:
  - a. Use the Default Organization's status rules or
  - b. Create a set of custom rules for this organization.

See the section on [Using Status Rules](#) for more information on configuring rules.

4. Click **Save** to save the new organization.

New EndPoints can now enroll into this organization or the administrator can edit an existing EndPoint's settings to make it a member of this organization.

**Edit Rules**

All organizations inherit status rules from the Default Organization on the appliance. To edit these rules:

1. Select an organization in the list using the checkbox next to its name.
2. If you want to edit the rules for all of the organizations, check the box next to *Organizations* at the top.
3. Click **Edit Rules** to view the selected organization's status rules and modify them.
4. Click **Save** to keep the changes.

See [Using Status Rules](#) for more information.

## 3.2 Main Panel

---

The CMD console's Main panel can display:

- A default list of all subscribed EndPoints, sorted by status and then by name.
- A specific EndPoint's configuration and status when an EndPoint is selected from the list.
- Various settings pages for the options in the Navigation panel.

This section discusses the first two:

- [EndPoint List](#)
- [EndPoint Details](#)

Refer to the [Navigation Panel](#) for details on the settings pages.
















## EndPoint List

By default, the CMD console displays a list of all subscribed EndPoints on this appliance:



EndPoints

1 2 3 4 5 >

EndPoint	Organization : Site	Status	Last Backup	Tags
 test-420-208	STC : STC Corp	Offline (19 hours)	19 hours	Exchange
 test-420-001	Default Organization	Offline (45 hours)		--
 test-420-002	acme	Critical	3 days	--
 CMD-EP-2008-1	acme : acme north	Critical	2 days	--
 LAP-W7	STC : STC Corp	Critical	46 hours	--
 cmd-endpoint-xp-1	STC : STC Corp	Warning		--
 LAP-W7-DaD	STC : STC Corp	Warning	25 min.	Finance
 test-420-008	STC : STC Corp	Warning	11 min.	--
 test-420-027	STC : STC Europe	Good		--
 test-420-029	Default Organization	Good		--
 test-421-003	STC : STC AU	Good		--
 test-421-004	Default Organization	Good		--
 test-425-030	STC : STC Europe	Good	26 min.	Exchange
 vm2000sv-en	Default Organization	Good		--
 test-420-006	STC : STC Europe	Warning	11 min.	--

1 2 3 4 5 >














The list identifies each with:


Field	Description
<b>Status Icon</b>	Displays the appropriate icon for the device's machine type (server, desktop, laptop, or virtual). Its color represents the EndPoint's current condition (Good, Warning, Critical, Offline).
<b>EndPoint</b>	Displays the name of the device.
<b>Organization:Site</b>	Displays the EndPoint's site and organization as assigned. (If not assigned, it is automatically in the Default Organization.)
<b>Status</b>	Displays the condition of the EndPoint. (If its status is <i>Offline</i> , the field also shows the length of time the EndPoint has been offline.)
<b>Last Backup</b>	Shows the elapsed time since the last backup. If CMD cannot detect this, the field is blank.
<b>Tags</b>	Shows each EndPoint's user defined tag (as assigned in the <a href="#">EndPoint Details</a> screen).

The page shows up to 20 EndPoints. If there are more than 20 subscribed EndPoints, CMD creates additional pages. The EndPoints appear in order of status then by device name.

## Status Icons

The color of the status icon indicates the EndPoint's current condition; its shape the EndPoint's machine type:

Alert Icon	Condition	System Type
	Offline	Server
	Offline	Desktop
	Offline	Laptop
	Offline	Virtual Machine
	Critical	Server
	Critical	Desktop
	Critical	Laptop
	Critical	Virtual Machine
	Warning	Server
	Warning	Desktop
	Warning	Laptop
	Warning	Virtual Machine
	Good	Server

	Good	Desktop
	Good	Laptop
	Good	Virtual Machine

## EndPoint Details

Double-click on an individual EndPoint in the EndPoint list to display its details:

LAP-W7-DaD

Backup Failure: 5 issue(s)

View details...

Clear status: now

Clear

Non-VSS Backup: 5 issue(s)

View details...

Clear status: now

Clear

Backup Consistency: 5 issue(s) out of the last 5 event(s)

View details...

Clear status: now

Clear

Info

Status: Warning

Platform: Microsoft Windows 7 Professional (6.1.7601 Service Pack 1 Build 7601)

Processor: Intel64 Family 6 Model 42 Stepping 7, GenuineIntel

Memory: 3 GB RAM, 1 GB Page file

Last Restart: 16 days ago

IP Addresses: 10.2.10.00

Locale: en\_US Mountain Daylight Time(UTC-0600)

Organization: STC

Site: STC Europe

Machine Importance: non-critical

Machine Type: Desktop

Tags: -

Important Applications: -

ShadowProtect

Version: ShadowProtect 4.2.1.15272 (en)

License: 6.1.7601

Job Name	Status	Next Run Time	Destination
Dave's Laptop	Success	17:00, Apr. 4	F:\

Destination	Path
Infinidisc	\\F:\INFINIDISC\INFINIDISC\F (STC-DaVED)
Test Directory	\\file\Product Management\Cloud

Volumes

Listing of all volumes mounted on this EndPoint

Volume	Free Space	Total Space	OS Volume	Protected
My Passport	31 GB	931 GB	No	No
OS	248 GB	297 GB	Yes	Yes
RECOVERY	623 MB	751 MB	No	No

ImageManager

Version: 5.0.1.13924(en-US) ImageManager

Registered User: DaD

Company: StorageCraft

Serial Number: 5.0.1.13924.2.1.15272

Feature	Assigned to Agent	Available	Total
IntelligentFTP Replication	1	43	50
	1	40	50
	1	41	50
HeadStart Restore	1	40	50
	1	41	50
	1	43	50
ShadowStream Replication	1	43	50
	1	43	50
	1	43	50
Network Replication	1	43	50
	1	43	50
	1	43	50

Actions

Unregister Endpoint

EndPoint Details include sections that describe:

- [Outstanding Conditions](#)
- [Info](#)
- [ShadowProtect](#)
- [Volumes](#)
- [ImageManager](#)
- [Actions](#)

Note: The *EndPoint Details* page supports printer-friendly output for future reference. To print a copy of the EndPoint's details, click on the printer icon in the upper-right corner of the page in the Main panel.

## Outstanding Conditions

The Outstanding Conditions section displays the current outstanding conditions for this EndPoint: These conditions occur when the EndPoint exceeds the threshold of one or more of the status rules.

**Volume Usage:** Exceeded 90% threshold [View details...](#) Clear status:

- Click **View Details** to view the time and any system message relating to the condition. If the condition has occurred on multiple occasions, CMD will list each of these.
- Use *Clear Status* to either remove this alert immediately or to schedule its removal in 1, 3, or 7 days.

## Info

The Info section displays hardware, operating system, IP address, and other details about the EndPoint.

▼ Info

CMD 1.0.0.17667

Status:

Warning [Event log...](#)

Platform:

Microsoft Windows 7 Professional (6.1.7601 Service Pack 1 Build 7601) [System log..](#)

Processor:

Intel64 Family 6 Model 42 Stepping 7, GenuineIntel

Memory:

3 GB RAM, 1 GB Page file

Last Restart:

16 days ago

IP Addresses:

10.2.10.00

Locale:

en\_US Mountain Daylight Time(UTC-0600)

Organization:

STC [Edit...](#)

Site:

STC Europe [Edit...](#)

Machine Importance:

non-critical [Edit...](#)

Machine Type:

Desktop [Edit...](#)

Tags:

-- [Edit tags...](#)

Important Applications:

--

The Info section also provides options for editing various fields. It also has the option to create tags for identifying similar devices using the Search function.

Field	Description	Option
<b>CMD Version</b>	Identifies the installed version of the CMD agent	
<b>Status</b>	Reflects the current condition for the device (Offline, Critical, Warning, Good)	<i>Event Log</i> displays the CMD log (not the Windows System Log) to show the cause of alerts. Acts like the View details option in the Outstanding Conditions section.
<b>Platform</b>	Identifies the operating system version	<i>System Log</i> displays the Windows System Log for the device.
<b>Processor</b>	Identifies the system processor	

<b>Memory</b>	Displays the amount of RAM and page file size	
<b>Last Restart</b>	Gives hours or days since the device restarted	
<b>IP Addresses</b>	Identifies both primary and any subnet addresses	
<b>Locale</b>	Uses the Windows Time Zone data	
<b>Organization</b>	Identifies the device's CMD Organization	Click <i>Edit</i> to display a dropdown box of available CMD organizations
<b>Site</b>	Identifies the site the device is a member of within the current organization shown above	Click <i>Edit</i> to display a dropdown box of available sites within the current CMD organization. It will also offer the <i>Manage Sites</i> option which opens the Sites page.
<b>Machine Importance</b>	Displays critical, semi-critical, or non-critical. The default setting results from CMD best-guess based on the Machine Type.	Click <i>Edit</i> to display a dropdown box for choosing one of the three options.
<b>Machine Type</b>	Shows Server, Desktop, Laptop, or Virtual. The default setting results from CMD analyzing the device to make a best guess as to its type.  A correct Machine Type allows CMD to accurately monitor and report conditions.	Click <i>Edit</i> to display a dropdown box for choosing one of the four options.

<b>Tags</b>	Displays any user-defined tags applied to this device. Use tags in searches to simplify locating or filtering EndPoints displayed based on a common characteristic or role.	Click <i>Edit tags</i> to open the list of defined tags with the option to create more.  <b>Note:</b> Tags support multi-lingual characters.
<b>Important Applications</b>	Displays a list of critical applications running on this device. CMD performs a check to automatically identify these which include <i>SQL</i> , <i>IIS</i> , and <i>Exchange</i> .	

## ShadowProtect

The ShadowProtect section displays the version number and license status of the ShadowProtect install on the EndPoint. It also displays a list of current backup jobs and their destinations. (If ShadowProtect is not installed, CMD will only display a short description of the device.)

▼ ShadowProtect

Version:ShadowProtect 4.2.1.15272 (en)

License:6.1.7601

Jobs

Job Name	Status	Next Run Time	Destination	
Laptop	Success	17:00, Apr. 4	F:\	<a href="#">More details...</a>

Destinations

Destination	Path	
Infinidisc	\\INFINIDISC\INFINIDISC\F (DAD)	<a href="#">Backup Images...</a>
Test Directory	\\file\Product Management\Cloud	<a href="#">Backup Images...</a>

The ShadowProtect section offers options to see further information about the job or destination:

Field	Description	Option
<b>Jobs</b>	Identifies details for all ShadowProtect backup jobs defined for this device	Click <i>More details</i> to show the last backup job's event log.  Note: CMD only displays backup jobs which have names. An unnamed backup job will not appear in the list. If there are no named backup jobs on the EndPoint, CMD will display the message "No backup job information available."

<b>Destinations</b>	Displays details on the configured backup file destinations for this device.	<p>Click <i>Backup Images</i> to display a list of the backup files stored on the selected destination. This list will also show date and time of each file, its name, type, size, and other details.</p> <p>Some destinations require credentials to access them. For this reason, some destination backup file lists may show no entries.</p>
---------------------	--	---

## Volumes

The Volumes section displays details on all volumes mounted on the EndPoint.

▼ Volumes					
Listing of all volumes mounted on this EndPoint					
Volume	Free Space	Total Space	OS Volume	Protected	
My Passport	31 GB	931 GB	No	No	<a href="#">More details...</a>
OS	248 GB	297 GB	Yes	Yes	<a href="#">More details...</a>
RECOVERY	523 MB	751 MB	No	No	<a href="#">More details...</a>

These volume details include:

Field	Description
<b>Volume</b>	<p>Displays the volume label for all partitions on each accessible drive to the device.</p> <p><b>Note:</b> This list might display hidden volumes.</p>
<b>OS Volume</b>	Indicates whether this is a boot volume.
<b>Protected</b>	Indicates whether ShadowProtect performs backups of this partition.
<i>More details</i>	<p>Displays a list including:</p> <ul style="list-style-type: none"> <li>• the mount point</li> <li>• free/total space</li> <li>• sector/cluster size</li> <li>• if ShadowProtect backs up this partition</li> </ul>

## ImageManager

This section displays the ImageManager licensing details for this EndPoint.

**Note:** CMD displays a message if ImageManager is not installed. If ImageManager is installed but not registered, CMD will only show the version number .

▼ ImageManager

Version:  
Registered User:  
Company:  
Serial Number:

5.0.1.13924(en-US) ImageManager  
DaD  
StorageCraft  
5.0.1.13924.2.1.15272

ImageManager Features:

IntelligentFTP Replication	Assigned to Agent	1
	Available	43
	Total	50
HeadStart Restore	Assigned to Agent	1
	Available	40
	Total	50
ShadowStream Replication	Assigned to Agent	1
	Available	41
	Total	50
Network Replication	Assigned to Agent	1
	Available	43
	Total	50

If one or more of ImageManager's premium features are installed, CMD will show:

- The serial number for each of those licenses
- The number of licenses for each type of premium feature
- If any premium feature license is expired

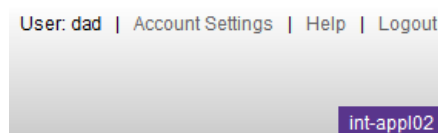
(Refer to the [ShadowControl ImageManager User Guide](#) for details on these premium features.)

## Actions

The Actions section provides the option to unsubscribe the EndPoint from this appliance. Click **Unsubscribe EndPoint** and CMD asks to confirm this action. Once the EndPoint unsubscribes to the appliance, CMD will no longer monitor that EndPoint.

## 3.3 Session Panel

The Session Panel appears at the top right of the console:



This panel displays:

<b>User</b>	Shows the currently logged-in username.  Displays in the Main panel the currently logged-in user's settings. The user can then change their password, email address, or type of notifications to receive (All, Critical, or None). Click <b>Save</b> to save the new settings. (Use the <i>Appliance Accounts</i> option in the Navigation panel to change the administrative role if needed.)
<b>Account Settings</b>	
<b>Help</b>	Opens a new tab in the browser to display this <i>ShadowControl CMD User Guide</i> .
<b>Logout</b>	Logs out the user out of the appliance console
<b>Appliance Identifier</b>	Shows the name of this appliance. This identification is useful for managing multiple CMD appliance systems.



## 4 Using Status Rules

Status Rules are the heart of CMD's monitoring. Both CMD organizations and sites have status rules. (By default, sites inherit settings from their parent organizations. Administrators can choose to have a site not inherit so they can specify unique rules for the site.) The CMD appliance includes the following default Status Rules:

☒ **ImageManger Status** - Trigger an alert if the number of ImageManager errors exceeds the threshold.  
ImageManager Errors:  Alert using Severity:

☒ **Backup File Size** - Trigger an alert if a backup file size exceeds the threshold.  
Size exceeds:  GB Alert using Severity:

☒ **Backup Consistency** - Trigger an alert if the ratio of failed to total backups exceeds the threshold.  
Backup failures:  Compared to total backups:  Alert using Severity:

☒ **Backup Failure** - Trigger an alert if the number of failed backups exceeds the threshold.  
Backup failures:  Alert using Severity:

☒ **Non-VSS Backup** - Trigger an alert when the number non-optimal "crash-consistent" backups exceeds the threshold.  
Non-VSS backups:  Alert using Severity:

☒ **Services** - Trigger an alert if the number of monitored service failures exceeds the threshold.  
Service Failures:  Alert using Severity:

☒ **RAM Usage** - Trigger alert if system RAM percent usage exceeds one of the thresholds.  
Warning Alert level:  % Critical Alert level:  %

☒ **Disk Errors** - Trigger an alert if number of disk or file system events in system log exceeds the threshold.  
Logged Errors:  Alert using Severity:

☒ **Volume Usage** - Trigger an alert if system volume percent usage exceeds one of the thresholds.  
Warning Alert level:  % Critical Alert level:  %

☒ **Critical Machine Offline** - The length of time a Critical machine can be offline before triggering an alert.  
Time offline:   Alert using Severity:

☒ **Semi-Critical Machine Offline** - The length of time a Semi-critical machine can be offline before triggering an alert.  
Time offline:   Alert using Severity:

☒ **Non-Critical Machine Offline** - The length of time a Non-critical machine can be offline before triggering an alert.  
Time offline:   Alert using Severity:

**Note:** By default, all the status rules are active with thresholds set based on best practice. Administrators can select which rules to apply to a given organization or site.

### Severity and Status Icons

Each of the rules includes a setting for severity: *Warning* or *Critical*. CMD uses the severity setting to change the icon shown for the affected EndPoint in the EndPoint list. An administrator can select this severity setting based on their requirements or concerns for their EndPoints.

For example, an administrator may group all servers into one site called "Servers" and set the Non-VSS Backup rule to issue a critical rather than a warning alert when a single non-VSS backup occurs on a server.

### Site vs. Organization Status Rules

Sites inherit their parent organization's status rules by default. Administrators can create unique status rules for a site by choosing to disinherit the site from the parent organization:

▼ Status Rules

Select the rules and conditions that will trigger a status alert.

☒ Inherit status rules from Organization

With the Inherit box checked, the same status rules apply for both the parent organization as well as for the child site. If an administrator unchecks the Inherit box, the default values remain for the status rules remain; only now the administrator can

modify one or more of the thresholds to create a custom set of rules for this site.

## Status Rules Details

Each status rule has specific thresholds and scope:

### ImageManager

This CMD alert activates when ImageManager issues an error. Refer to the ImageManager console for details on the type of error and how to resolve it.

### Backup File Size

This alert provides notice that a ShadowProtect backup image file exceeded a user-defined threshold. This alert might safeguard against running out of storage space on the backup drive or it might indicate an unusual amount of activity on the source device that warrants investigation. This alert displays (until cleared) even when subsequent backup files may not exceed the set threshold.

To clear an alert:

1. Locate the EndPoint detail's Backup File Size alert in the *Outstanding Conditions* section.
2. Click **Clear** to immediately remove the alert. (CMD also supports scheduling this clearing at a later time using the dropdown box.) The alert clears.

### Backup Consistency

This rule works in conjunction with the **Backup Failure** rule. This consistency rule generates an alert if a backup failure occurs not just once, but on multiple occasions within a set number of backups. In essence, Backup Consistency escalates the alert that the Backup Failure rule generates by notifying the administrator that a pattern of failures is occurring (when the failures are not consecutive).

### Backup Failure

This rule generates an alert if there is a single backup failure (if the setting is "1"). If the number is set to "2" or more, it generates an alert only after the set number of failures occur in a row, rather than separately.

### Non-VSS Backup

ShadowProtect leverages Windows VSS support to provide optimal backups for server applications such as SQL or Exchange. If a problem occurs with VSS (such as with an unreliable third-party VSS writer), ShadowProtect may resort to performing a "crash-consistent" backup. A "crash-consistent" backup may require additional recovery effort, so by default CMD will issue an alert whenever a non-VSS backup occurs.

**Note:** Windows 2000 does not support VSS. ShadowProtect backups from a Windows 2000 system therefore do not use VSS. Refer to [Installing the CMD Agent](#) for details on avoiding multiple alerts due to Win2k non-VSS support.

### Services

The Services rule applies to various monitored Windows services, including the ShadowProtect and ImageManager services. View details in the Windows System Log.

### RAM Usage

This rule alerts administrators to possible backup issues should the EndPoint exhaust available RAM.

### Disk Errors

This rule alerts administrators to potential drive problems or impending failure.

### Volume Usage

Alerts administrators that a protected volume may run out of available space.

## Machine Offline Status Rules

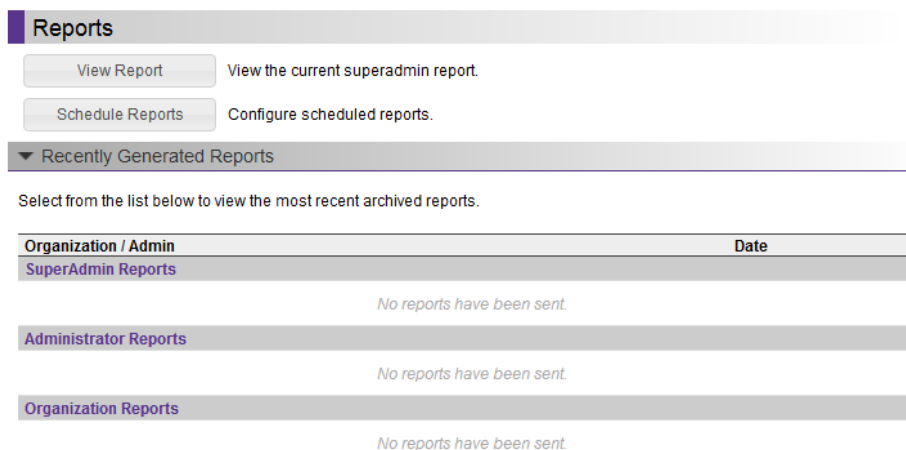
The Machine Offline status rules vary by machine importance. Each EndPoint has a user-definable Machine Importance setting on its EndPoint Details page. These settings are *Non-critical*, *Semi-critical*, and *Critical*. (CMD assigns a default setting of non-critical to all subscribed EndPoints.)

Administrators should determine which EndPoints represent a more significant part of their operations and set an appropriate machine importance to them. For example, all servers may have a Critical machine importance setting. Desktops in "Accounting" may have Semi-Critical or Critical importance.

The Offline rules also include an elapsed time setting. This setting can range from the specified number of minutes, hours, or days for the system to be offline before CMD issues an alert.

## 5 Reporting

The Reports option in the Navigation panel displays report settings and a list of recent archived reports in the Main panel:



This screen has three elements:

Element	Description
<b>View Report</b>	Click this button to view the latest superadmin report in a new browser tab. (See the <a href="#">Sample Report</a> for further details.)
<b>Schedule Reports</b>	Click this button to view the report scheduling page (See <a href="#">Report Scheduling</a> for details.)
<b>Recently Generated Reports</b>	This section lists recently archived reports. (CMD only keeps a rolling 30-day record.) Click on a report in the list to view it in HTML in a new browser tab.

**Note:** Reports are sent to users in the language selected in the user's *Preferred Language* setting.

### 5.1 Report Scheduling

The **Schedule Reports** button on the Reports page displays the *Report Scheduling* settings page:

## Report Scheduling

Schedule the generation of reports tailored to specific administrators and contacts. Reports are sent by email according to the selected schedule.

▼ SuperAdmin Report

Send a report to each SuperAdmin
Send reports: Never

Report will contain a Summary section and any of the following sections:

☒ EndPoint Status: overall status of all monitored EndPoints
☒ EndPoint Backup: listing of last backup for each ShadowProtect installation

▼ Administrator Report

Send an organization report to each Administrator
Send reports: Never

Report will contain a Summary section and any of the following sections:

☒ EndPoint Status: overall status of all monitored EndPoints
☒ EndPoint Backup: listing of last backup for each ShadowProtect installation

▼ Organization Report

Send an organization report to the primary contact of each organization
Send reports: Never

Report will contain a Summary section and any of the following sections:

☒ EndPoint Status: overall status of all monitored EndPoints
☒ EndPoint Backup: listing of last backup for each ShadowProtect installation

Save Schedule

To send a report:

1. Select the Type, Role, and Frequency of the report.
2. Click **Save Schedule**.
3. CMD will issue a report based on the options selected.

## Types of Reports

The scheduler will generate a report with three possible sections based on the selected options:

<b>Summary</b>	Shows an overall list of CMD EndPoints, ShadowProtect and ImageManager installations, and a chart on the breakdown of current EndPoint status.
<b>EndPoint Status</b>	Select this option to add a section to the summary report listing all EndPoints by organization with details and last backup time.
<b>EndPoint Backup</b>	Select this option to add a section to the summary report that lists all EndPoints by organization with the EndPoint's last backup time. Select this only if the Status section is not included for this report. (As it repeats the same information.)

## Specific Role Reports

CMD can send a report to a specific role. Each role receives a report covering a different set of EndPoints:

<b>SuperAdmin</b>	This report covers all EndPoints on this appliance.
<b>Administrator</b>	This report shows only those EndPoints the administrator has been assigned by organization.
<b>Organization</b>	This report (sent to an organization's contacts) lists only the EndPoints in that organization.

## Frequency

CMD can then send these reports on a selected schedule:

**Never** CMD sends no reports.

- Every Day** CMD sends a current status report once a day.
- Every Week** CMD sends the current status once a week. (This only shows the status at the moment when the report generates. It is not a weekly summary.)
- Every Month** CMD sends a report once a month on the EndPoints' current status. (Like the weekly report, this monthly report only shows the status at the time of generation. It is not a monthly summary.)

## 5.2 Sample Report

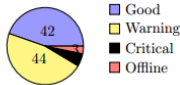
CMD reports can have three sections:

- EndPoint Summary** Displays a chart of EndPoint status and a list of ShadowProtect/ImageManager installations.
- EndPoint Status** Displays a list of the EndPoints by organization, their status, and when their last backup occurred.
- Backup Status** Displays a list of the EndPoints by organization and when their last backup occurred. (This repeats data from the EndPoint Status section.)

A sample report showing all three sections appears like this:

ShadowControl CMD Admin Report  
Appliance "int-appl02"  
ShadowControl CMD  
May 21, 2012

### EndPoint Summary

EndPoint Installs		EndPoint Platforms		EndPoint Status	
ShadowProtect	92	Windows	94		<ul style="list-style-type: none"> <li>Good</li> <li>Warning</li> <li>Critical</li> <li>Offline</li> </ul>
ImageManager	0	Linux	0		
Total EndPoints	94				

### EndPoint Status

XYZ Corp

EndPoint	OS Version	Status	Last Backup
vm2000pro-en	Windows	Good	
test-420-001	Windows	Good	00:00, May. 22
test-420-001	Windows	Offline	
test-420-009	Windows	Good	
test-420-011	Windows	Good	

### Backup Status

XYZ Corp

EndPoint	Last Backup
vm2000pro-en	
test-420-001	00:00, May. 22
test-420-001	
test-420-009	
test-420-011	
test-420-012	

## 6 Using the CMD Portal

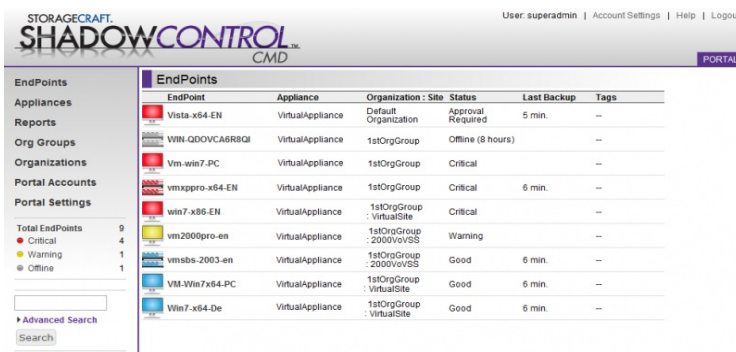
ShadowControl CMD includes the Portal feature. This feature enables CMD to scale to multiple appliances and thousands of monitored devices. A portal is not, however, a distinct software package. Instead, it is simply another installation of the CMD appliance that other appliances subscribe to. Once one appliance (the source) subscribes to another CMD appliance (the target), the target appliance automatically becomes a Portal. This subscription enables the Portal features on the target appliance. Access to the portal is the same as with other appliances via a browser-enabled console.

This section covers:

- [Understanding the Portal Console](#)
- [Using Org Groups](#)
- [Portal Report Scheduling](#)
- [Defining Portal Settings](#)

### 6.1 Understanding the Portal Console

The Portal console provides configuration controls and displays the status of all EndPoints on all subscribed appliances:



EndPoint	Appliance	Organization	Site	Status	Last Backup	Tags
Vista-x64-EN	VirtualAppliance	Default Organization		Approval Required	5 min.	--
WIN-QDOVCA6RRQI	VirtualAppliance	1stOrgGroup		Offline (8 hours)		--
Vm-win7-PC	VirtualAppliance	1stOrgGroup		Critical		--
vmxgpro-x64-EN	VirtualAppliance	1stOrgGroup		Critical	6 min.	--
win7-x86-EN	VirtualAppliance	1stOrgGroup	VirtualSite	Critical		--
vm2008pro-en	VirtualAppliance	1stOrgGroup	2008VoVSS	Warning		--
vm2008-2003-en	VirtualAppliance	1stOrgGroup	2008VoVSS	Good	6 min.	--
VM-Win7x64-PC	VirtualAppliance	1stOrgGroup	VirtualSite	Good	6 min.	--
Win7-x64-De	VirtualAppliance	1stOrgGroup	VirtualSite	Good	6 min.	--

The Portal console is divided into three panels:

**Navigation Panel:** Located at the left side of the console, the Navigation panel provides access to the tasks and tools necessary to configure and monitor EndPoints. For more information, see the CMD console [Navigation Panel](#) section.

**Main Panel:** Located at the center of the console, the Main panel displays various lists or configuration settings depending on the option selected in the Navigation panel. (The default is to display a list of all EndPoints the Portal monitors.) For details, see the CMD console [Main Panel](#) section.

**Session Panel:** Located at the top of the console, the Session panel displays the Portal indicator, the name of the currently logged-in user, and options for account settings, Help, and Logout. For more information, see the CMD console [Session Panel](#) section.

### Portal Navigation Panel

The left-side Navigation Panel provides access to the Portal's tasks, EndPoint summary, and Search capability:

EndPoints
Appliances
Reports
Org Groups
Organizations
Portal Accounts
Portal Settings

Total EndPoints 9  
Critical 4  
Warning 1  
Offline 1

Advanced Search

The selections include:

**EndPoints:** Displays a list of all the EndPoints on all subscribed appliances in the Main panel.

**Note:** Use the *Search* feature to filter the list.

**Appliances:** Displays the list of subscribed appliances in the Main panel. Click on an appliance to display a subset of its configuration settings. These include Organizations, Sites, User Accounts, and Email settings. It also presents options to **Unsubscribe** or **Reboot** the appliance. See [Understanding the CMD Console](#) for further details.

**Reports:** Displays the Report Scheduling settings. Use this to configure reporting (see [Portal Report Scheduling](#) for details).

**Org Groups:** Displays the list of defined Org Groups for this portal. See [Using Org Groups](#) for details.

**Organizations:** Displays a list of Organizations from all subscribed appliances. Use this screen to assign the Organizations to Org Groups. See [Using Org Groups](#) for details.

**Portal Accounts:** Displays the list of defined accounts for this Portal. See [Defining Portal Settings](#) for details.

**Portal Settings:** Displays the various email and network settings for this portal. See [Defining Portal Settings](#) for details.










**EndPoint Summary:** Displays the total number of EndPoints that report to this portal. It also shows the number of EndPoints in Offline, Warning, or Critical Status. Click on the status to display a filtered list of the EndPoints with a specific status in the Main panel.

**Search:** Type in a search term to display a list of EndPoints, organizations, or sites that include the term.. See [Search](#) for more information.

## Portal Main Panel

The Portal Main panel by default shows a list of all EndPoints on all subscribed appliances:

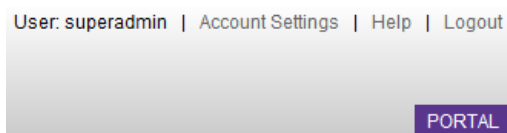


EndPoints						
EndPoint	Appliance	Organization : Site	Status	Last Backup	Tags	
 Vista-x64-EN	VirtualAppliance	Default Organization	Approval Required	5 min.	--	
 WIN-QDOVCA6R8QI	VirtualAppliance	1stOrgGroup	Offline (8 hours)		--	
 Vm-win7-PC	VirtualAppliance	1stOrgGroup	Critical		--	
 vmxppro-x64-EN	VirtualAppliance	1stOrgGroup	Critical	6 min.	--	
 win7-x86-EN	VirtualAppliance	1stOrgGroup : VirtualSite	Critical		--	
 vm2000pro-en	VirtualAppliance	1stOrgGroup : 2000VoVSS	Warning		--	
 vmsbs-2003-en	VirtualAppliance	1stOrgGroup : 2000VoVSS	Good	6 min.	--	
 VM-Win7x64-PC	VirtualAppliance	1stOrgGroup : VirtualSite	Good	6 min.	--	
 Win7-x64-De	VirtualAppliance	1stOrgGroup : VirtualSite	Good	6 min.	--	

The Portal EndPoint list functions the same as the EndPoint list shown in the Main Panel on a single CMD appliance. However, the Portal list does include one additional column--the *Appliance* column--to identify the appliance monitoring this particular EndPoint.

## Portal Session Panel

The Portal Session Panel appears at the top of the console:



This panel displays:

- User** This identifies the name of the currently logged-in user.
- Account Settings** Displays the currently logged-in user's settings in the Main panel. The user can then change their password, email address, or type of notifications to receive (All, Critical, or None). Click **Save** to save the new settings. (Use *Portal Accounts* to change the administrative role if needed.)
- Help** Opens this *ShadowControl CMD User Guide* in a new tab in the browser.
- Logout** Logs the user out of the portal console.
- Portal Identifier** In the lower-right corner of the Portal Session panel is the word "Portal". This indicates that this console is a Portal (as opposed to an appliance) console. An appliance console would indicate the name of the appliance. Portals do not have names, as there can be only one portal per CMD system.


## 6.2 Using Org Groups

Select *Org Groups* from the portal's Navigation panel to display a list of the defined Org Groups and options to add to or edit those Org Groups:



## Org Groups - PhysicalApp



Org Groups are collections of Organizations from one or more appliances.

Org Group	Actions
MSP 1	 


[+ Add Org Group](#)

### Actions

You have three actions on the Org Group page:

Icon	Description	Function
	Blue pencil icon	Opens the selected Org Group's configuration page. Use this page to edit the selected Org Group's name, contacts, or status rules. (See <a href="#">Using Status Rules</a> for more details.)
	Red delete icon	Deletes the selected Org Group.
<b>Add Org Group</b> button		<p>Opens a Org Group configuration page. Specify the name and contact info for this new Org Group.</p> <p><b>Note:</b> Org Group names support multi-lingual characters.</p>

Click **Organizations** in the Navigation panel to add organizations to a defined Org Group shown in the dropdown box:

Organizations		
Assign the Organizations from the Appliances into Org Groups. Use the options in the Appliance views to create new Organizations.		
Organization	Appliance	Org Group
1stOrgGroup	VirtualAppliance	MSP 1 

## 6.3 Portal Report Scheduling

Select *Reports* in the Portal Navigation panel to display the Report Scheduling page in the Main panel:

## Report Scheduling

Schedule the generation of reports tailored to specific administrators and contacts. Reports are sent by email according to the selected schedule.

▼ SuperAdmin Report

Send a report to Appliance SuperAdmins for each appliance
Send reports: Never

Report will contain a Summary section and any of the following sections:

- ☒ EndPoint Status: overall status of all monitored EndPoints
- ☒ EndPoint Backup: listing of last backup for each ShadowProtect installation

▼ Administrator Report

Send Appliance-level, organizational report to Administrators of each Appliance
Send reports: Never

Report will contain a Summary section and any of the following sections:

- ☒ EndPoint Status: overall status of all monitored EndPoints
- ☒ EndPoint Backup: listing of last backup for each ShadowProtect installation

▼ Organization Report

Send an organization report to the primary contact of each organization on all appliances
Send reports: Never

Report will contain a Summary section and any of the following sections:

- ☒ EndPoint Status: overall status of all monitored EndPoints
- ☒ EndPoint Backup: listing of last backup for each ShadowProtect installation

Copy Schedule to Appliances

These report scheduling settings are similar to the [Appliance Reports](#) settings for a CMD appliance with these exceptions:

- These portal report settings are sent to each of the appliances. These settings will then supercede any existing settings on the appliances for the associated reports. The individual appliance's SuperAdmin or administrators can, however, adjust these settings on their individual appliances as needed afterwards.)
- These settings apply globally to all reports for the affected organizations, appliances, or SuperAdmins.
- These settings are not stored at the portal level. Instead, they are copied down to and stored at the affected appliances.

## 6.4 Defining Portal Settings

This section covers:

- Portal Accounts
- Portal Settings

### Portal Accounts

The *Portal Accounts* option in the Navigation panel acts the same as the [Appliance Accounts](#) option on an individual appliance. Use this option to specify SuperAdmins, administrators, and read-only access for this portal. The difference is that an administrator or read-only account on the portal can be assigned to organizations from multiple, rather than just one, appliance.

### Portal Settings

Select this Navigation panel option to display the portal settings in the Main panel:

▼ Email Settings

Configure SMTP Server and settings used to send reports and alert notifications.

☒ Use this appliance's built-in SMTP server.

☐ Use another SMTP server:

Host Name or IP Address:

Port:

Username:

Password:

Security:

☐ Use TLS

☐ Don't use an SMTP server. (Warning: if this option is selected, no email will be sent from this appliance)

Save

Send Test Email

▼ Network Settings

Configure network settings for this appliance.

IP Address:

10.3.1.40

Subnet Mask:

255.255.255.0

Default Gateway:

10.3.1.1

DNS Server:

199.101.231.134

Save

▼ System Info

Version:

CMD v1.0.0.17593 [ 1.4-1, 4]

Access Code:

12345

Reboot Appliance

Shut Down Appliance

These sections appear, and the settings function, the same as fo the [Appliance Settings](#) on a single CMD appliance. The difference is the lack of a subscription section at the top, as a portal cannot subscribe to another portal or appliance.