ShadowControl User Guide

Table of Content

ShadowControl User Guide

Welcome to the StorageCraft® *ShadowControl™ User Guide*. ShadowControl monitors and manages backup jobs on ShadowProtect-equipped systems This Guide describes the ShadowControl technology, how to use the product, and how to derive maximum benefit from ShadowControl.

This guide covers ShadowControl v3.0.2

This user guide includes the following major sections:

Additional Information

For emerging issues and other resources, see the following:

- The ShadowControl ReadMe.
- The ShadowControl forum at www.storagecraft.com/support/forum.
- The StorageCraft technical support Web site at www.storagecraft.com/support.html.
- The StorageCraft glossary.
- This User Guide is also available from the Help menu on the ShadowControl console.

Documentation Conventions

This symbol designates either a **Note**, which contains a explanation or exceptions to the text, or an Important item which provides details on making a selection about the configuration and/or use of ShadowControl.

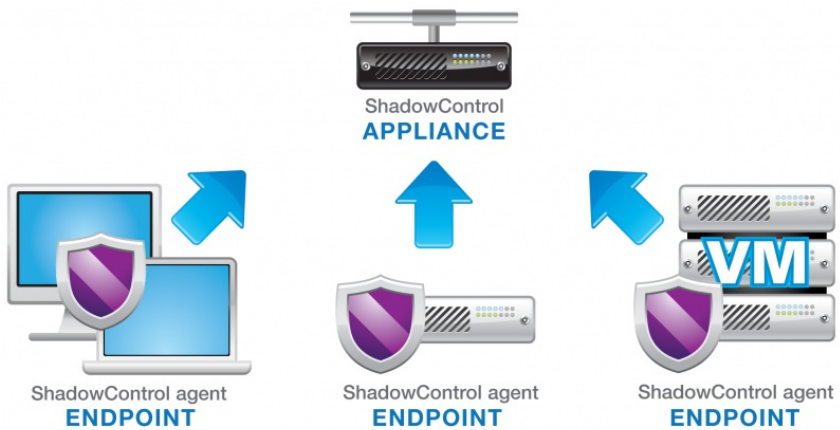
This symbol designates **a Warning** text. A warning highlights critical information that affects backup job performance or potential loss of data.

1 ShadowControl Overview

Welcome to ShadowControl™ —the central monitoring, managing and reporting console for ShadowProtect and ImageManager operations ShadowControl also provides a critical secondary monitor on ShadowProtect and ImageManager services in the event of either failing without notification.

ShadowControl has two main components:

- **ShadowControl Appliance**--a Linux-based server running as a VM or on dedicated hardware
- **ShadowControl Agent**--a client installed at each endpoint



ShadowControl consists of endpoints running the ShadowControl agent and an appliance which monitors those Endpoints.

The ShadowControl appliance communicates with the ShadowControl agent installed on each endpoint.

The **ShadowControl appliance** is the heart of ShadowControl. It receives status reports from each agent-equipped endpoint. These reports provide details about the endpoint's ShadowProtect and ImageManager installations, backup activity, and hardware configuration details. The appliance also manages backup jobs on SPX endpoints. Administrators use the appliance's browser-based console to:

- Configure Endpoint status rules
- Configure alert and notification settings
- Configure SPX Policies for distributing backup job templates
- Monitor Endpoints
- Schedule reports
- Manage SPX Policy-based backup jobs

The appliance keeps a rolling 90-day log of endpoint activity information for reporting purposes while each endpoint maintains its own log. ShadowControl provides an appliance backup function to preserve and restore the system history log and system configuration In the event of an appliance failure.

The **ShadowControl agent** allows a system (either physical or virtual machines) to become endpoints. Each new endpoint can subscribe to an appliance and become a participating node in ShadowControl.

Note: The agent does not require ShadowProtect on the endpoint. However, endpoints that have ShadowProtect installed provide greater details and management options than systems with only the agent.

Administration Schema

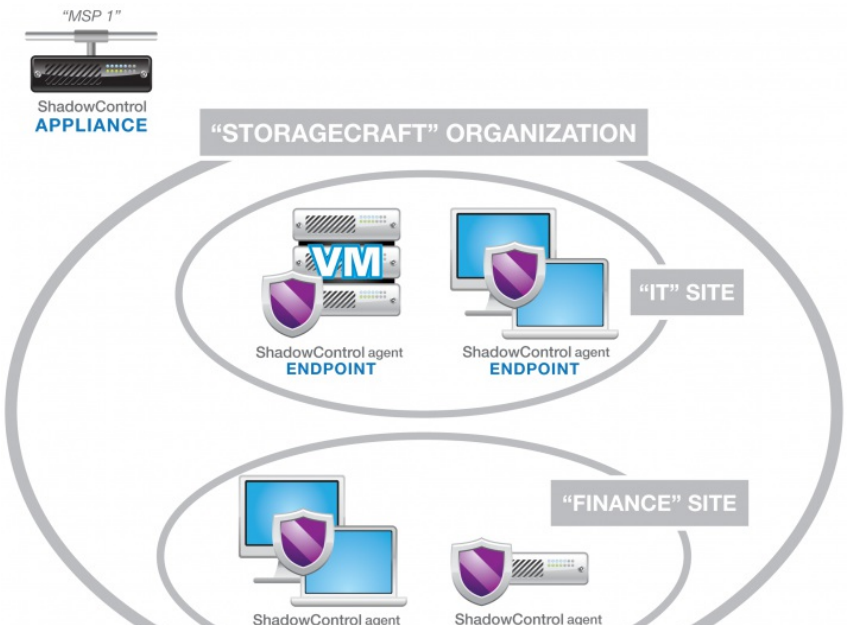
To supervise these components, ShadowControl provides various administrative roles that differ primarily in the scope of the endpoints they oversee:

- A **superadmin** manages the appliance as well as add, edit, or remove any or all organizations, sites, endpoints, user accounts, SPX Policies, and Rules applied from 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.

For more information, see User Roles.

Organizations and Sites

Administrators can group ShadowControl endpoints into organizations and sites for ease of management. Each new appliance creates a single Default Organization in which every endpoint becomes a member. Administrators can then create one or more custom organizations and assign endpoints to them. Each of these new organizations in turn can also contain one or more sub-organizations called Sites:



Administrators can also assign endpoints to a defined organization or site either during the subscription process or after.

Note: StorageCraft recommends assigning each endpoint to an appropriate organization or site rather than keep endpoints in the Default Organization

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.

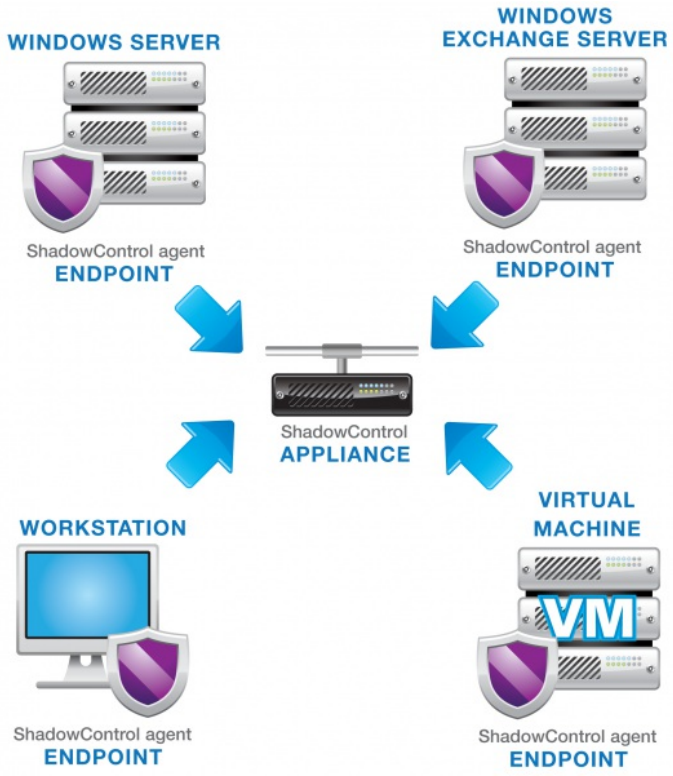
.

2 ShadowControl Operations

To begin using ShadowControl, an administrator would:

1. Install the ShadowControl appliance either on standalone hardware or as a virtual machine.
2. Create one or more organizations to associate endpoints with similar functions or locations.
3. Create one or more sites within each organization to further associate endpoints with similar requirements.
4. Install the ShadowControl agent on each ShadowProtect-guarded system.
5. Assign each agent to an organization or to a site to monitor it using the ShadowControl console.
6. Create and apply backup job policies for ShadowProtect SPX-equipped systems.

The ShadowControl appliance begins to receive a stream of status data over a encrypted link from each endpoint every five minutes.



Each ShadowControl endpoint reports to the appliance using SSL over Port 443 or 8443.

Status Rule Policies

A major benefit of ShadowControl is the ability to set alert thresholds--called *Status Rule Policies*--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.
- **Unknown:** The endpoint is not reporting to the console.

SPX Backup Job Policies

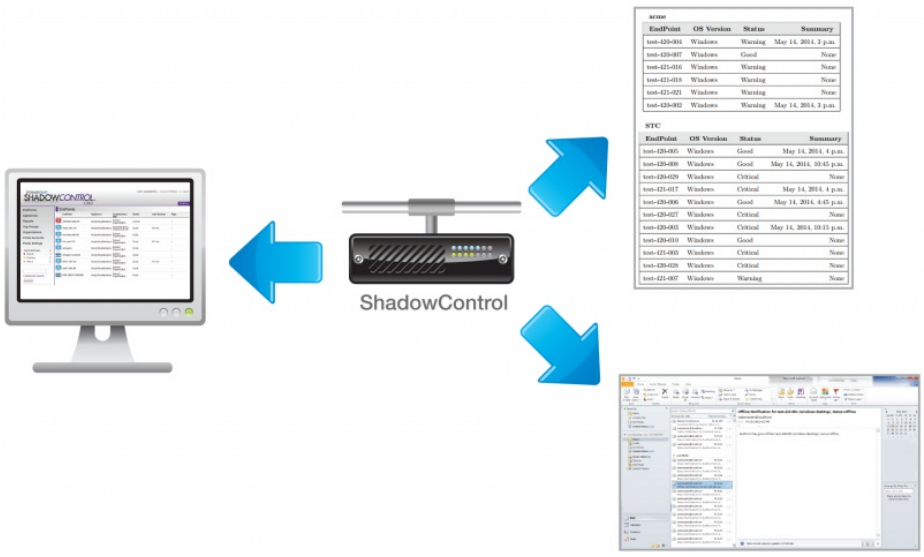
A second major benefit of ShadowControl is the ability to create and deliver backup job templates--called *SPX Policies*--to ShadowProtect SPX-equipped endpoints. Once SPX applies the policy on the endpoint, the ShadowControl console manages the remote backup job. The endpoint user cannot modify or control the job using their install of SPX.

Notifications

Another benefit of ShadowControl is the ability to send email notifications when an endpoint exceeds the status rule thresholds. ShadowControl can send these notifications to administrators or organization contacts responsible for the affected endpoint, or to an ITSM system.

Reports

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



ShadowControl issues endpoint status information to the browser-based console and to email notifications and scheduled reports.

3 Installing ShadowControl

ShadowControl installs as two components:

- The ShadowControl Appliance: A Linux-based system installed on standalone hardware or as a Virtual Machine.
- The ShadowControl Agent: A Windows- or Linux-based client installed on each monitored device.

3.1 Installing the ShadowControl Appliance

The ShadowControl appliance installs on standalone hardware or as a Virtual Machine. Both installations use the same ShadowControl file on either Windows or Linux hypervisors.

System Requirements

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

- The appliance uses the 64-bit Ubuntu 12.04 operating system. 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 appliance can also run as a virtual machine on:
  - Microsoft Hyper-V
  - VMware ESX/ESXi

Caution: Xen, Oracle VirtualBox, and VMware Workstation may work in a test environment, however, they are not supported by StorageCraft for production use.

- 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, StorageCraft recommends:
  - 2GB RAM
  - 80GB disk space
  - Dual-core processor
- Active Internet connection (to download server components during the install)
- An available IP address (for remote console access)
- Either Port 443 or 8443 available (for endpoint-to-appliance communication)
- Port 5556 available.
  Important: Port 5556 is a required second port for endpoint-to-appliance communication. If this port is not open, ShadowControl cannot perform endpoint updates or other bi-directional services.
- Port 25 or 587 available (if email notifications are enabled)
- Supports endpoints running ShadowProtect v4.2.7 or newer. (Older ShadowProtect versions do not correctly report their licensing information.)
- Supports monitoring StorageCraft ImageManager v6 or newer.
- Remote console access requires a contemporary browser. In the case of Internet Explorer, ShadowControl requires IE v10 or newer.

Using a Hostname

You have the option to use a 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 must manually create a hostname entry on your DNS server before attempting to subscribe an endpoint or access the appliance UI.

To install the ShadowControl appliance:

1. Download the ShadowControl install file from the StorageCraft website..
2. If you are using a physical destination for the appliance, burn the ISO to a CD.
3. Boot the physical or virtual machine using the ShadowControl ISO.
4. Accept the default language of **English** for the Ubuntu install.
5. Follow the steps in the Installation Wizard to:
   - Specify a secure password for the superadmin account.
   - Verify the necessary network information to install the ShadowControl appliance: IP address, netmask, primary gateway, DNS servers, host name, and domain.
6. On the *Initial Appliance Setup* dialog, select **Setup a new appliance**.
   Note: The Install process can take 15 minutes or more as it downloads Ubuntu and StorageCraft packages for the install.

After the ShadowControl appliance finishes its start-up routine, it displays a login screen. At this point, the appliance is running and all further configuration occurs through the browser-based ShadowControl console. To access the console, open a browser to https://<*IPaddress*>where <*IPaddress*>is the address you gave the appliance during the installation.

Note: If you need to reboot or shutdown the appliance, you can do so from the Appliance Settings page in the ShadowControl console.

3.2 Installing the ShadowControl Agent

You must install the ShadowControl agent software on each device you want to monitor. and manage.

System Requirements

- ShadowControl client's hardware and software requirements are the same as for ShadowProtect or for ShadowProtect SPX.
- Automatic endpoint updates by the ShadowControl appliance requires the existing endpoint agent to be v2.0.0 or later.
- The ShadowControl agent supports ShadowProtect versions 4.2.7 and newer. (Remote activation requires endpoints running ShadowProtect 4.2.5 or newer.)
- ShadowControl can monitor StorageCraft ImageManager 6 and newer.
- The agent communicates with the ShadowControl appliance using two required ports: either Port 443 or 8443 (selectable during installation) and Port 5556.

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

Linux Installation

Use the endpoint install instructions prov ided on the ShadowControl console at either:

- **Configure ShadowControl > Appliance Settings > Endpoint Installation**
- Click **EndPoint Installation Instructions** on the ShadowControl Dashboard

Note: On CentOS and RHEL endpoints, the ShadowControl 3.x agent requires the EPEL package installed. If the endpoint has ShadowProtect SPX already installed, then it has this package. If the endpoint does not have SPX installed, then download and enable the EPEL repositories. Go to the Fedora website, **https://fedoraproject.org/wiki/EPEL**, to get the EPEL package.

Windows Installation

Warning: ShadowControl does not support Windows 2000 endpoints.

You can install the Windows ShadowControl agent:

- Directly on the endpoint
- Via Silent Install

Note: The StorageCraft Virtual Plug-ins (for vCenter or System Center) will install the ShadowControl agent as part of the ShadowProtect push install.

After installing the endpoint agent, you must subscribe the endpoint to the appropriate ShadowControl appliance. A direct install lets you open a separate subscription application. A silent install requires a separate command-line operation to manually subscribe the endpoint.

Windows Direct Install

To install the ShadowControl agent directly on the endpoint:

1. Run the ShadowControl console and display the Dashboard.
2. Click **Endpoint Installation Instructions** at the lower right.
   Note: These instructions also appear under **Configure ShadowControl** > **Appliance Settings** > **Endpoint Installation**.
3. Click on the download link shown in the onscreen Step 1 under *Windows.*
   Note: The user's ShadowControl appliance generates this custom IP address which points to the install folder on the appliance.
4. Using an administrative account, double-click on the ShadowControl_Installer.msi icon to launch the installer at the desktop.
5. The ShadowControl agent installer can also run from a command (CMD) shell using the command:

   ```
   msiexec.exe /i ShadowControl_Installer.msi /quiet
   ```

6. Follow the onscreen prompts to complete the agent install.

When the install completes, subscribe the endpoint to the appliance (refer to the *Endpoint Subscription* section)..

Windows Silent Install

ShadowControl supports a silent install of the WIndows ShadowControl agent. This allows a push install of the agent via a policy.

To create a silent install package and subscribe the endpoint to the appliance:

1. Select **Dashboard** > **Endpoint Installation Instructions** in ShadowControl.
2. Use the commands from the onscreen Steps 1, 2, and 3 as part of a remote install package.
   ⚠ **Note**: ShadowControl customizes the commands to include the appliance's IP address.
   The commands are::

   ```
   https://xxx.xx.xx.xxx/api/installer/msi/download/
   msiexec.exe /i ShadowControl_Installer.msi /quiet
   C:\Program Files (x86)\StorageCraft\CMD\stccmd subscribe xxx.xx.xx.xxx
   ```

The last command subscribes the endpoint to the appliance. Refer to the *Endpoint Subscription* section for details.

Manual Windows EndPoint Subscription

The majority of Windows endpoint subscriptions occur using the steps shown via the ShadowControl Dashboard. In some cases, however, the endpoint may require a manual subscription to a ShadowControl appliance. (For example, as part of a Silent Install.)

To perform a manual subscription of an endpoint to an appliance:

The majority of Windows endpoint subscriptions occur using the steps shown via the ShadowControl Dashboard. In some cases, however, the endpoint may require a manual subscription to a ShadowControl appliance. (For example, as part of a Silent Install.)

To perform a manual subscription of an endpoint to an appliance:

1. Run a command prompt as Administrator on the unsubscribed endpoint.
2. Navigate to the install directory of ShadowControl.
   ⚠ **Note:** The default is Program Files (x86)\StorageCraft\ShadowControl.
3. Enter the command:

   ```
   stccmd.exe subscribe <IP address/Server Name>
   ```

   where *IP address* is the address to the appliance and *Server Name* is the DNS name. Use either the address or the server name if the appliance is on an external address.

The endpoint Agent subscribes to the specified ShadowControl appliance.

Note: An endpoint agent can subscribe to only one appliance at a time.

Command Line Options

The agent supports various options using the *stccmd subscribe* command:

Option	Description
–a	Forces the endpoint and appliance to communicate using the alternative port 8443.
–U {user}	Specifies the appliance's username. Use the -P option to specify a password if needed. **Note:** This is the only way to create an endpoint's username and password without rerunning the installation.
-T {token}	Allows an endpoint to log in and subscribe to an appliance without credentials. The connection permits only the subscription process to run. It does not permit running the ShadowControl console or other utilities. **Note:** The Token option uses a capital "T". The Tag option uses a lower-case "t". Locate the Token on the *Configure ShadowControl* > *Tokens* list.
–P {password}	Specifies the appliance's user password. Must be used in conjunction with the -U option.
–t {tags}	Identifies any desired Tags for this endpoint.
-m {server, desktop, laptop, virtual)	Specifies the endpoint's System Type (server, desktop, virtual, laptop). (Note that this option is case sensitive. Use lowercase.)
-g (normal, semi, critical)	Specifies the importance of this endpoint (Normal, Semi, or Critical).
–o {org:site}	Specifies the endpoint's Organization and optionally the Site.
-h	Displays a list of the subscribe options. Note that Help is available for each sub-command. For example, for help with the Subscribe sub-command, type *stccmd subscribe -h* or type *stccmd unsubscribe -h* to view help with the unsubscribe command.

These options can be combined as needed:

Task	Command Example	Description
Subscribe the endpoint to an appliance on the same local network	`stccmd.exe subscribe 192.0.0.2`	Use the local IP address for onsite endpoints. Use the exterrnal IP addrss or DNS name for an offsite ShadowControl appliance.
Subscribe the endpoint to an appliance on the same local network using a Token	`stccmd.exe subscribe 192.0.0.2 -T 433a615464aab889485106b`	Use the local IP address for onsite endpoints. Use the exterrnal IP addrss or DNS name for an offsite ShadowControl appliance. Generate the Token in *Configure ShadowControl* > *Tokens* list.
Unsubscribe the endpoint from an appliance	`stccmd.exe unsubscribe`	Since an endpoint can only subscribe to one appliance, the command does not require the appliance's IP address.

3.3 Endpoint Subscription

ShadowControl supports subscribing an endpoint in one of two ways:

- **Subscription Application**--Windows-only
- **Command Line**--Windows or Linux

Subscription Interface

When the agent install completes, the wizard displays the option to *Launch ShadowControl Subscription Application*.

1. Launch the application.
2. Specify the ShadowControl appliance to subscribe the endpoint to in this application. Accept the default if this is a new agent install. If it is an upgrade, uncheck the box.
3. Specify the *ShadowControl Agent Settings* in the console as outlined below.

DNS Host Name/IP	Provide the hostname or IP address of the appliance to specify where to subscribe this endpoint.
Use alternate port (8443)	Check **Use alternate port (8443)** to have the endpoint communicate with the appliance on port 8443 if the default SSL port (443) is already in use.
Machine Type	Enter the endpoint's type, or class. Options include **Desktop**, **Laptop**, **Server**, and **Virtual**. ShadowControl uses this information to classify systems within its interface. **Note:** If the Machine Type needs to change later (Server, Desktop, Laptop, or Virtual Machine), use the Info section of the Endpoint Details page to update it.
Use Appliance Admin credentials	*Optional.*Provide the appliance admin credentials to have the endpoint subscription request approved immediately. Also, specify the Organization and Site to include the endpoint. **Note:** Without valid credentials or enrollment information, the new endpoint appears in the list with a request to **Approve** or **Deny** its subscription. An administrator or superadmin must approve the new endpoint to complete the subscription. ShadowControl does not monitor or manage this endpoint until it is approved.

4. Click **Subscribe**. The installer displays a success message. (It may also display a dialog to unsubscribe. Simply close that dialog.)

When the subscription process completes, the endpoint appears in the list of subscribed devices on the selected ShadowControl appliance.

Command Line Subscription

The agent also supports subscribing the endpoint using a command shell in either Linux or Windows.

1. Open a command shell.
2. Run the command

```
C:\Program Files (x86)\StorageCraft\CMD\stccmd subscribe xxx.xxx.xx.xx
```

Substitute the actual ShadowControl appliance's IP address at the end of the command.

Note: ShadowControl can generate this command automatically with the appliance's specfic IP address appended. Refer to Step 2 of the agent install instructions.

Working with Non-VSS Systems

Some endpoints may not support VSS backups. On these non-VSS systems, an optional ShadowControl ShadowProtect Policy produces an alert for each non-VSS backup. When active, this rule results in a continuous flow of notifications for these non-VSS endpoints. To avoid this when using this policy rule:

1. Create an organization or site for these devices. Name this group "*Non-VSS Systems*" or similar.
2. Group all non-VSS systems into this site or organization.
3. Select the non-VSS site or organization and open its *Status Rule Policy* page.
4. Confirm that the **Last VSS Backup** rule is unchecked. This prevents the issuing of notifications for these endpoints. endpoints that do use VSS can keep the Non-VSS rule and generate alerts if VSS fails.

This prevents the issuing of continuous notifications for these endpoints. endpoints that do use VSS, however, should keep the Non-VSS rule and generate alerts if VSS fails.

3.4 Using Tokens

Tokens let you perform certain tasks, including endpoint subscription and accessing the Report API, without exposing administrator login credentials. A Token provides access to only a single operation--either subscriptions or reports--not both.

To view and create tokens, browse to **Configure ShadowControl** > **Tokens**.

To add a token:

1. From the Tokens page, click **Create Token**.
2. In the Create Token dialog, provide the required information, then click **Save**.

Field	Description
Token Name	Specify a name for the token.
Type	The type of token you want to create: **endpoint Subscription** and **Report API Access**.
Expires	(Optional) Select a date in the future when you want the token to expire. Upon expiration, ShadowControl deletes the token and it is no longer valid for use.
Description	(Optional) Specify a more detailed description for this token.
Organization Access	Select the scope associated with this token: • **Unrestricted** gives the Token access to all organizations on the ShadowControl appliance. • **Restricted To:** limits the token access to only the selected organization.

4 The ShadowControl Console

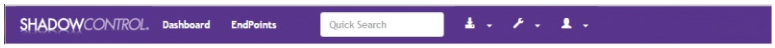
The ShadowControl main console screen includes various parts described below:

- Menu Bar
- StorageCraft Message Feed
- Dashboard
- Endpoints List
- Appliance Info Bar

Note: The ShadowControl console may appear distorted when viewed using Internet Explorer with Compatibility View enabled. To correct this, set Compatibility View to Off.

Menu Bar

The **Menu Bar** gives access to ShadowControl management functions:



These functions include:

- Displaying either the Dashboard or the appliance's endpoint List
- Search Box
- Options dropdown menus

Search

The *Search Box* performs two types of searches:

- **Quick**--Returns a list of items that include the entered term(s). This list could include endpoint names, Organizations, or Tags.
- **Advanced**--Returns a list of items that match two or more terms entered or for a specified field. For example, searching for term "Tag=Windows7" displays a list of all endpoints labeled with the tag "Windows7". Searching for "Org=Utah Name=Win7" displays a list of endpoints that are in the Utah organization and contain the term "Win7" in their name.

Options Menus

The three *Options* dropdown menus are:

Icon	Menu	Details
	Manage Endpoints	Provides options for: • Managing Backup Stores • Configuring ShadowProtect SPX Policies • Configuring VM Deployment for the e optional StorageCraft Plug-In for Virtual Machines integration.
	Configure ShadowControl	Provides options for: • Appliance Settings • User Accounts and Roles • Tokens • Policies • Organizations • Tags • Reports
	User Profile	Provides: • Identification of the current console user • the user's account settings • Access to *Help* and *About* options • User Logout option

StorageCraft Message Feed

The StorageCraft Message Feed appears under the menu bar. At a minimum, this section can display messages of the following types:

Message Type	Details
Appliance Update Available	Use the *Appliance Settings* dialog to update this appliance.

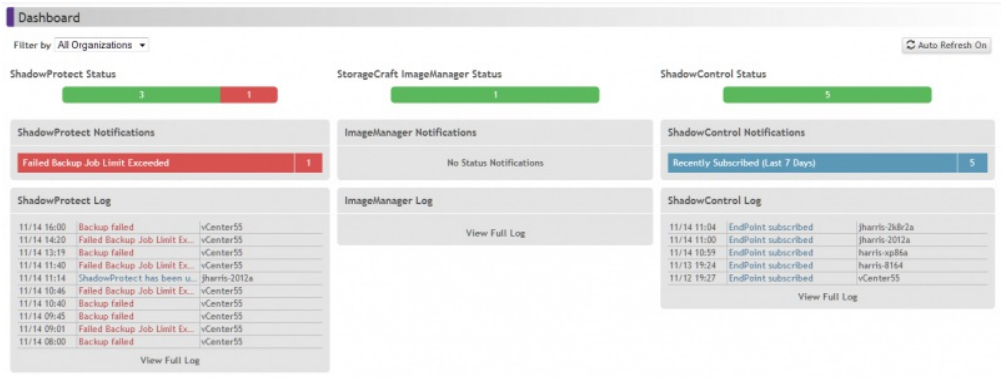
Reboot Appliance	The appliance has updated its operating system and needs to reboot. Use the button in the *Appliance Settings* dialog to reboot the appliance.

These update-related messages remain on the Dashboard until the related update task has been completed.

ShadowControl 3.0.2 and later includes an enhanced message feed that lets StorageCraft distribute important and relevant communications in addition to update-related messages, such as breaking news about known issues; upcoming releases; and tips and tricks. Appliance administrators can view and dismiss these messages as needed.

Dashboard

The **Dashboard** is the ShadowControl console's default view:



This shows alerts, current endpoint ShadowProtect and ImageManager status information, and recent log entries.

Note: The Dashboard allows filtering for a specific organization's endpoints using the dropdown menu in the upper-left of the dialog.

Endpoint List

Refer to the Endpoints List section for details.

Endpoint Installation Instructions

This button opens the *Endpoint Installation* dialog. This dialog provides both instructions and customized links for distributing the ShadowControl agent to systems on the network. The custom links point to the location on the appliance for the:

- Windows installer
- Linux source files

as well as the specific IP address in the command shell instruction to do endpoint subscriptions to this appliance. These instructions simplify the ShadowControl endpoint configuration process.

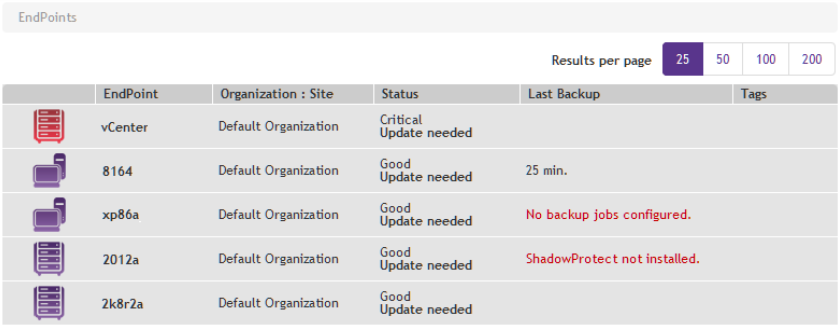
Appliance Info Bar

The *Appliance Info* bar at the bottom of the console shows:

Item	Details
ShadowControl version	Indicates the installed version of the software on this appliance.
Appliance Date and Time	Shows the current date and time for this ShadowControl appliance. ⚠ **Note:** This is useful in multi-regional networks where the time and date may differ between various monitored endpoints and the appliance.

4.1 EndPoints List

Use the Endpoints option in the ShadowControl menu bar to display a list of all subscribed endpoints on this appliance:



The list identifies each with:

Field	Description
Status Icon	Displays the appropriate icon for the device's machine type (server, desktop, laptop, or virtual). Its color represents the endpoint's current condition (Purple=Good, Yellow=Warning, Red= Critical, Grey=Unresponsive).
endpoint	Displays the name of the device.
Organization:Site	Displays the endpoint's site and organization as assigned. (If not assigned, it is automatically in the Default Organization.)
Status	Displays the condition of the endpoint. (If its status is *Offline*, the field also shows the length of time the endpoint has been offline.)
Last Backup	Shows the elapsed time since the last backup. If ShadowControl cannot detect this, the field is blank.
Tags	Shows an endpoint's user-defined tag (as assigned in the *Endpoint Details* screen).

Results Per Page

The page defaults to show up to 25 endpoints. Use the selector at the upper-right to increase the number of results from 25 to 50, 100 or 200. If there are more than the selected number of subscribed endpoints, the system creates additional pages. The endpoints appear in order of status then by device name.

Sorting the Endpoint List

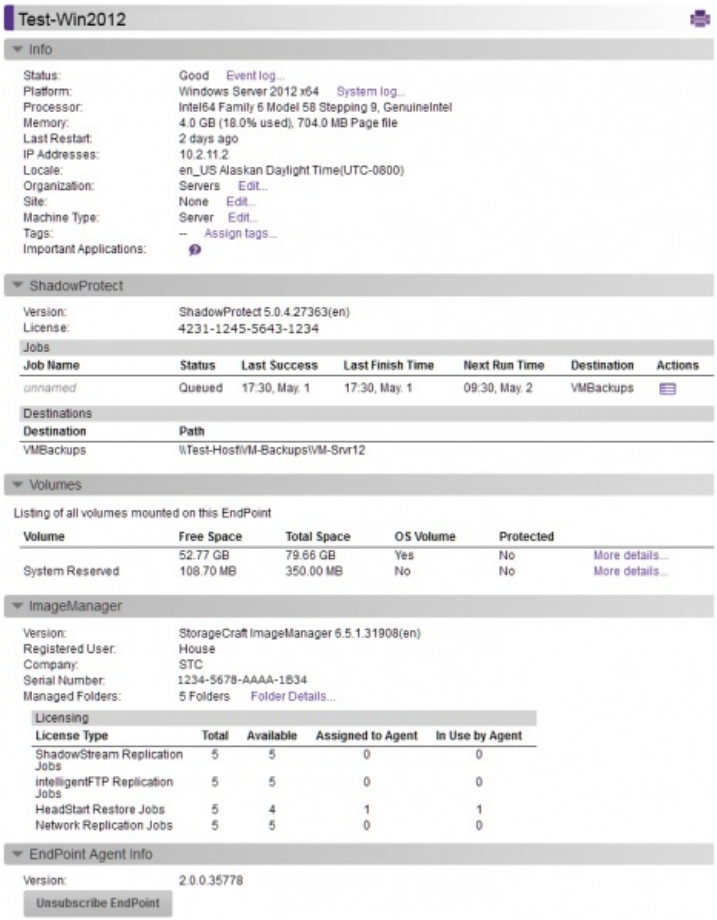
Click on a column heading to sort by that column. (Click on the title again to reverse the order.) ShadowControl can sort the Endpoint List by:

Column	Sorting Hierarchy
Name	Alphabetically
Organization	Alphabetically, then each Site within each organization is listed alphabetically, followed by each Site's endpoints listed alphabetically.
Status	Lists endpoints in this order: Unapproved, Offline, Critical, Warning, and Good.
Last Backup	Lists oldest to newest.

Tags	Click on a tag to display a new list showing only those endpoints identified with that tag.

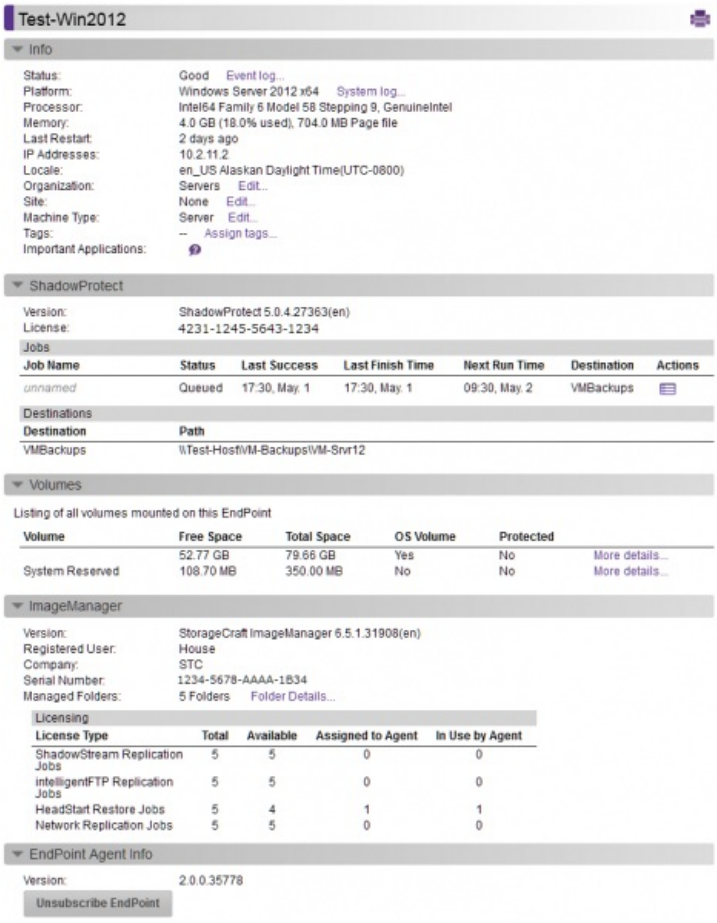
4.2 EndPoint Details

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



Endpoint Details include sections that describe:

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



Endpoint Details include sections that describe:

- Info
- ShadowProtect
- Volumes
- ImageManager
- Endpoint Agent Info

Info

The Info section displays general information about endpoint characteristics, and the ability to edit some of these characteristics. The Info section includes the following fields:

Field	Description	Option
Status	Reflects the current condition for the device (Unresponsive, Critical, Warning, Good)	*Event Log* displays the ShadowControl log (not the Windows System Log) to show the cause of alerts. Acts like the View details option in the Outstanding Conditions section.
Platform	Identifies the operating system version	*System Log* displays the Windows System Log for the device.

Processor	Identifies the system processor	
Memory	Displays the amount of RAM and page file size	
Last Restart	Gives hours or days since the device restarted	
IP Addresses	Identifies both primary and any subnet addresses	
Locale	Uses the Windows Time Zone data	
Organization	Identifies the device's Organization	Click *Edit* to display a dropdown box of available organizations
Status Rule Policy	Identifies which policy applies to this endpoint.	Use Configure ShadowControl > ShadowControl Policies to select a different policy.
Backup Policy	Identifies the name of the ShadowControl SPX Policy applied to this endpoint.	Use the ShadowControl SPX Policies to manage this endpoint's backup job configuration.
Machine Type	Shows Server, Desktop, Laptop, or Virtual. The default setting results from ShadowControl analyzing the device to make a best guess as to its type. A correct Machine Type allows ShadowControl to accurately monitor and report conditions.	Click *Edit to* display a dropdown box for choosing one of the four options.

Tags	Displays any user-defined tags applied to this device. Tags simplify locating specific endpoints based on a common characteristic or role.	Click *Assign tags* to open the list of defined tags and select one or more for this endpoint. The list includes the option to create more. **Note**: Tags support multi-lingual characters.
Important Applications	Displays a list of critical applications running on this device. ShadowControl performs a check to automatically identify these which include *SQLServer*, *IIS*, and Microsoft *Exchange*.	

ShadowProtect

The ShadowProtect section displays the ShadowProtect version and license status on the endpoint. It also displays details about the endpoint's configured backup jobs, destinations, and backup job status.

Note: If ShadowProtect is not installed on this endpoint, this section displays the message "ShadowProtect is not installed on this endpoint".

ShadowProtect Licensing

ShadowControl detects if the endpoint's ShadowProtect license is a Trial version, or Expired. In either case, it provides the option to activate ShadowProtect.

Note: Remote activation works only with ShadowProtect version 4.2.5 and newer.

To activate a ShadowProtect License:

1. In the ShadowProtect section of the Endpoint Details page, click **Activate**.
2. In the Activate ShadowProtect dialog, provide the required information, then click **Activate**.

Field	Description
Serial Number	Enter a valid ShadowProtect product key.
Customer Name	(Optional) Enter a company name to associate with this activated ShadowProtect license. This simplifies working with StorageCraft Support.

Backup Jobs

The ShadowProtect section provides sub-sections for Jobs and Destinations so users can see exactly how backup jobs are configured on this endpoint.

	Description	Fields
Jobs	Displays details for all ShadowProtect backup jobs configured for this endpoint.	• **Job Name:** The name of the backup job, if it has one. • **Volumes:** The volumes backed up by this job. • **Last Success:** Date and time the job last completed successfully. • **Last Finish Time:** Date and time the job last ran, whether success or failure. • **Next Run Time:** Date and time of the next scheduled backup job. • **Destination:** The name of the ShadowProtect destination used by this backup job. • **Actions:** Opens a separate pane that displays additional information about the backup job, along with the most recent backup job log.
Destinations	Displays details about the ShadowProtect destinations used with this endpoint.	• **Destination:** The name of this destination. • **Path:** The full path associated with this destination, which could be a local or network location.

Volumes

The Volumes section displays details on all volumes mounted on the endpoint. It contains the following informational columns:

Field	Description
Volume	Displays the volume label for all partitions on each accessible drive to the device. **Note:** This list might display hidden volumes.
Free Space	Displays the amount of available space in the volume.
Total Space	Displays the total capacity of the volume.
OS Volume	Indicates if this is a boot volume.
Protected	Indicates whether ShadowProtect performs backups of this partition.

More details	Displays a list showing: • the mount point • device ID • free/total space • Boot volume (yes/no) • sector/cluster size • if ShadowProtect backs up this partition

ImageManager

The *ImageManager* section displays ImageManager licensing details for this endpoint.

Note: If ImageManager is not installed, this section displays "ImageManager is not installed on this endpoint".

The ImageManager fields include:

Field	Description
Version	The installed version of ImageManager. Depending on the version, an unregistered version of ImageManager could display different information: • ImageManager 5 or older: Displays only the unlicensed status, not the version number. • ImageManager 6 or newer: Displays the version number as well as the unlicensed status.
Registered User	The name specified when registering ImageManager.
Company	The company name specified when registering ImageManager.
Product Key	The ImageManager product key.
Managed Folders	The number of managed folders on this ImageManager endpoint. Click **Folder Details** to open a second pane with detailed information about each managed folder.

Additionally, the ImageManager section displays information about premium features licensed with this ImageManager install:

Field	Description
License Type	The type of premium license. Options include ShadowStream, intelligentFTP, HeadStart Restore, and Network Replication.
Total	The total number of premium licenses available to this registered user.
Available	The number of premium licenses available for use.
Assigned to Agent	The number of premium licenses assigned to this ImageManager agent.
In Use by Agent	The number of premium licenses actually in use by this ImageManager agent.

For more information about ImageManager premium features, refer to the *ShadowControl ImageManager User Guide*.

EndPoint Agent Info

The Endpoint Agent Info section displays the version number of the installed ShadowControl agent. It also provides the option to unsubscribe the endpoint from this appliance.

To unsubscribe from an appliance:

1. Click **Unsubscribe Endpoint**.
2. Confirm this action.

Once the endpoint unsubscribes from the appliance, ShadowControl no longer monitors or manages that endpoint. All historical data on the endpoint is erased from the appilance's logs.

4.3 Configure ShadowControl Menu

The *Configure ShadowControl* menu offers options for:

- Appliance Settings
- User Roles
- Status Rule Policies
- Organizations
- Tokens
- Tags (see below)
- Reports

Refer to the relevant sections in this guide for details on these options.

Tags

This dialog displays the list of existing user-defined tags with the option to create, edit, or delete tags. Tags simplify endpoint searches as a filter to display only those sharing a common characteristic or role.

To create a tag:

1. Enter a name.
2. Click **Create Tag**.

ShadowControl also supports adding tags directly from the Endpoint Details dialog.

Note: Tags support multi-lingual characters.

To assign a tag:

1. Click **Endpoints** on the ShadowControl menu bar.
2. Click on an endpoint.
3. Click **Assign Tags** in the Info section.
4. Check an existing tag and click **Done** to assign a tag.

Rename a Tag

Click to change the tag's name. ShadowControl updates the name and preserves the link to all endpoints using this tag.

Delete a Tag

Click to delete the tag. ShadowControl also removes the deleted tag from all endpoints previously using it.

Appliance Settings

The Appliance Settings option in the *Configure ShadowControl* menu displays the system's current settings in these categories:

- System Info
- Appliance Backup
- Network

System Info

System Info provides details on the ShadowControl appliance and options to control the server. These include:

Item	Description
Version	Reports the software version for the ShadowControl appliance (not the version of Linux it runs on).
Release Notes	Displays the ShadowControl ReadMe file when clicked. Since the ShadowControl update process is automatic, viewing this file allows administrators to note new software requirements or changes to ShadowControl prior to installing the update.
Access Code	Displays the user-defined code (set during the install) that may be used by StorageCraft Support in troubleshooting appliance issues. Treat this as similar to a password.
RAM Usage	Displays the amount of RAM the ShadowControl appliance is using. ⚠ **Note:** The percentage references the Linux OS RAM usage, not the CMD appliance.
Disk Usage	Displays the amount of disk space used by the ShadowControl appliance.
CPU Usage	Displays the appliance's current CPU utilization.
Load Average	Shows the average work load on the CPU over the last five minutes. As a baseline, an average of 1.00 is 100% utilization of a single core, a 2.00 is 100% of two cores, etc. Monitor this to keep the average under the maximum for the number of cores installed (if a dedicated system) or the number assigned to CMD (if a virtual machine).
Update Appliance	Performs an automatic update to the appliance when clicked. (View the ShadowControl ReadMe to see what enhancements come with the update.) ⚠ **Note:** This button only appears when ShadowControl detects an update to the appliance software.
Schedule Appliance Update	Performs the appliance update immediately or at a later time. using this option's *Schedule Appliance Update* dropdown box. ⚠ **Note:** This button only appears after clicking **Update Appliance**.
Endpoint Update Window	Sets the time when the automated updating of endpoint agents should end; or to mandate a manual update of each agent. ShadowControl then updates each agent at random intervals in the selected time. This prevents saturating network bandwidth. ⚠ **Note:** Automated updating is supported only with endpoint agents v2.0 or newer. This dropdown box also only appears after clicking **Update Appliance**.
Appliance Timezone	Provides a selector box to find and highlight the appliance's timezone. Click **Set Timezone** to accept it.
Reboot Appliance	Reboots the appliance if a reboot is necessary. (The appliance does not have command line access so that can't be used for reboots.)
Shut Down Appliance	Gracefully shuts down the appliance.

Network

Network displays the appliance's DNS/IP configuration as specified during the appliance install. Edit these settings as required should they change.

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

Use the *Public Appliance Address* field to specify what address external users should use to access the appliance. The default is to use the configured IP address. To use an alternate address:

1. Select *Other*... in the Public Appliance Address dropdown box.
2. Enter the alternate address.
3. Click **Save**.

Mail Server

Mail Server specifies the settings used to send ShadowControl reports and notifications, as well as the branding used in those notifications.

These settings are:

Setting	Description
Use this appliance's built-in SMTP server	Select this option to use ShadowControl's own SMTP server. This is the default.
From Address	Specify the email address that will appear in the From field. (This does not have to be a valid address.)
Use another SMTP server	Select this option if emails from ShadowControl's own SMTP bounce or routed to Spam folders.
Host Name or IP address	Specify this external SMTP server's name or address.
Port	Specify the port to use for the sending emails or reports. ⚠ **Note:** ShadowControl uses Port 25 by default. If necessary, substitute Port 587 if ShadowControl fails to send email reports.
Username	Provide a valid login name for the SMTP server.
Password	Provide the user's valid password.
From address	Indicate what address should appear in the From field. (This does not have to be a valid address.)
Security	Select whether to use TLS.
Don't use an SMTP server	Use this option to perform testing of ShadowControl without issuing alerts. ⚠ **Caution:** Without an SMTP server, ShadowControl cannot send email alerts or reports.

After specifying the email settings, Click **Send Test Email** to confirm the settings function. Click **Save** when finished.

⚠ **Note:** Sometimes email sent from the ShadowControl 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 ShadowControl to use an existing SMTP server.

Branding

To personalize the branding for ShadowControl reports and notifications:

1. Specify a name for this branding (for example, a company name).
2. Select **Upload custom logo.**
3. Click **Choose** File, then browse to and select the image you want to use. The *Current Logo* field then updates to display the newly uploaded image.
   Note: If the image does not refresh, try reloading the page to refresh the browser cache.
4. Click **Save**.

ITSM Notifications

Sites using IT Service Managment (ITSM) can specify an email address to send alert messages. Normally, ShadowControl sends alerts in digest form. With the ITSM option, ShadowControl sends each notification in a separate email to more easily trigger an action in an external system such as a ticketing system or RMM. ITSM notifications use a fixed subject line so they can be easily parsed.

To enable ITSM notifications:

1. Select **Enable IT service management notifications**.
2. Enter the ITSM email address.
   ⚠ **Note:** This should be an email address used exclusively by the external system.
3. Specify the language for the notifications.

Security

ShadowControl supports encrypted communications between endpoints and the ShadowControl appliance. The default certificate provided with the appliance is not recommended for production use. From the Security tab you can upload an SSL certificate issued by a recognized certificate authority.

To install a custom SSL certificate

From the Security tab, provide the locations to the three required certificate files, then click **Save**.

- Certificate File
- Key File
- Intermediate Bundle File

The ShadowControl appliance uploads the certifcate files and restarts its Web server to bring the new certificate online.

Important: ShadowControl is built using the Apache Web server. This server requires a certificate bundle that contains all three of these files. Because of this, you should use an Apache-supported tool, such as OpenSSL, to generate the certificate bundle. Generating a certificate using Microsoft IIS provides only the Certificate file and will not import successfully into the ShadowControl appliance.

⚠ **Caution:** The certificate cannot have a passphrase.

Endpoint Installation

The *Endpoint Installation* dialog provides both instructions and customized links for distributing the ShadowControl agent to systems on the network. The custom links point to the location on the appliance for the:

- Windows installer
- Linux source files

The links also include the specific IP address in the command shell instruction to do endpoint subscriptions to this appliance. These instructions simplify the ShadowControl endpoint configuration process.

Note: This dialog also appears after clicking on the ShadowControl Dashboard's **Endpoint Installation Instructions** button.

Product Registration

The Product Registration section offers the option to register the software with StorageCraft. This improves response time if support issues arise.

To complete the registration:

1. Enter a primary contact name for the ShadowControl administrator and other details.
2. Click **Save**.

Note: This information is used only for supporting ShadowControl.

User Accounts

ShadowControl provides two ways to administrator access rights to the ShadowControl features:

- User Roles--control the permissions and scope of user accounts.
- User Accounts--give access to a ShadowControl user role to a specific individual.

For example, Admin and SuperAdmin are user roles in ShadowControl. User "Jane Doe" can be assigned via a user account to the Superadmin user role. The advantage of the User Role is that the ShadowControl Admin can add or remove a specific user from a role without having to change the login credentials for that role.

To add a user account:

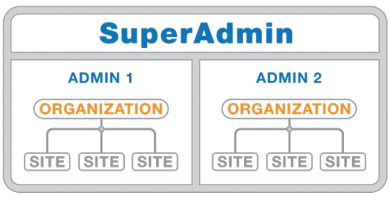
1. Access **Configure ShadowControl** > **User Accounts**.
2. Specify credentials for the user and a valid email address.
3. Select which role(s) the user has access to.
4. Click **Save**.

User Roles

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

- A **superadmin** manages the appliance and can add, edit, or remove all organizations, sites, and endpoints; and administer user accounts. The superadmin can also set the Status Rule Policies 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 typical ShadowControl appliance has one superadmin and one or more Administrators to manage the organizations, sites, and endpoints:



Administrators on an appliance can monitor endpoints in one or more organizations or sites. The superadmin can manage all organizations and sites.

The superadmin can create as many user roles as needed with appropriate administrator or read-only rights to specific organizations. (For example, read-only accounts can allow different personnel to receive notifications or reports.)

Add a Role

To view and create user roles, browse to **Configure ShadowControl** > **User Roles**.

To add a user role:

1. From the User Roles page, click **Add Role**.
2. In the Add Role dialog, provide the required information, then click **Save**.

Field	Description
Role name	Specify a name for the user role.
Description	(Optional) Specify a more detailed description for the user role.
Permission level	Select the type of user role to create. Options include **Admin** for full access to administer endpoints, and **Read-Only** for the ability to view but not change any settings.
Organizations	Select the organizations where this role provides rights.

Once created, you can assign a user role to one or more user accounts to grant them the privileges associated with the user role.

To assign a user role:

1. Browse to **Configure ShadowControl** > **User Accounts**.
2. Click the **Edit** icon for the user account to which you want to assign a role.
3. On the Edit User Account page, select the user roles to assign to this user account, then click **Save**.

4.4 User Profile Menu

The *User Profile* dropdown menu appears at the far right of the menu bar. Its options are:

User	Identifies the current logged-in user.
Account Settings	Displays the currently logged-in user's settings. The user can then change their password, email address, the type of notifications to receive (All, Critical Only, or None), or the user's preferred language. Click **Save** to save the new settings. **Note:** Use the *Appliance Accounts* option in *Configure ShadowControl* to change the administrative role if needed.
Help	Opens a new tab in the browser to display this *ShadowControl User Guide*. (Requires Internet access.)
About	Shows the version and access to license info on ShadowControl.
Logout	Logs the user out of the appliance console

5 Reports

ShadowControl can generate cumulative reports at these intervals:

- Daily
- Weekly
- Monthly

It can send these reports to:

- Superadmin
- Administrators
- Organization Contacts

The *Reports* option in the **Configure ShadowControl** dropdown menu displays report settings and a list of recent archived reports. This screen has four elements:

Element	Description
View Report	Displays the latest superadmin report in a new browser tab. (See the *Sample Report* for further details.)
Schedule Reports	Displays the report scheduling page (See *Report Scheduling* for details.)
Recently Generated Reports	Displays a list of recently archived reports. (ShadowControl only keeps a rolling 30-day record.) Click on a report in the list to view it in HTML in a new browser tab.
Additional Reports	Provides further information that is not included in the standard reports. For example, this section includes an on-demand report showing ShadowProtect license usage. (For details, see ShadowProtect Licensing.)
Experimental	May provide beta release versions of new report types. This allows StorageCraft to receive valuable feedback from users on the value of the beta reports prior to incorporating them in the standard ShadowControl release. The current beta release report is *ShadowProtect Backups*, which shows the daily backup success rates.

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

Custom Reports

Use the ShadowControl Reports API to retrieve endpoint information and history from the system database to an external reporting system. The API supports using tokens to allow database access without exposing administrator credentials.

5.1 Report Scheduling

The **Schedule Reports** button on the Reports page displays the *Report Scheduling* settings page. To send a report:

1. Select the *Type*, *Frequency*, and *Role* of the report.
   Note: The defaults send a complete report every day to superadmin and administrators as well as the primary contact for each organization.
2. Click **Save Schedule**.

ShadowControl issues reports based on the options selected.

Types of Reports

The scheduler generates a report with four possible sections based on the selected options:

Summary	Displays a chart of endpoint status (Critical, Warning, Good or Offline), a list of the backup succcess rate for the report's time period, and a list of ShadowProtect/ImageManager installations and platforms.
Endpoint Backup	Displays a list of the endpoints by organization, their backup success rate for the report's time period, and when their last backup occurred.
Endpoint Status	Displays a list of the endpoints by organization with their: • Length of time CMD actively monitored the endpoint • Average number of times per day the endpoint is offline • Operating system version details.
Storage Summary	Displays a set of daily averages for the amount of disk space used by backup image files. CMD uses this data to create a chart of projected storage space requirements for the next 3, 6, and 12 months. **Note:** This is only a rough estimate and varies based on the rate of change of data in each backup.

Specific Role Reports

ShadowControl can send a report to a specific role. Each role receives a report covering a different set of endpoints:

SuperAdmin	This report covers all endpoints on this appliance.
Administrator	This report shows only those endpoints in organizations assigned to each administrator.
Organization	This report lists only the endpoints in that organization. This report is sent to an organization's primary contact).

Frequency

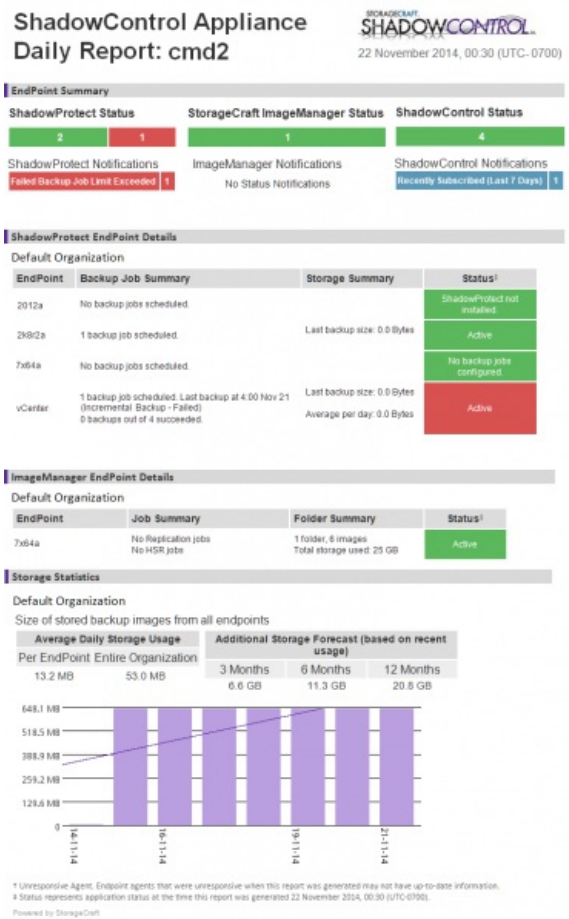
ShadowControl can then send these reports on a selected schedule:

Never	ShadowControl sends no reports.
Every Day	ShadowControl sends a summary report of the last 24 hours once a day.
Every Week	ShadowControl sends a summary report of the last 7 days once a week.

Every Month	ShadowControl sends a summary report for the last 30 days once a month.

5.2 Sample Report

A ShadowControl report can have four sections:



These four sections are:

Endpoint Summary	Displays a chart of the number of endpoints that are Critical, Warning, Good or Unresponsive and a list of ShadowProtect, ImageManager, and ShadowControl agent notifications.
ShadowProtect Endpoint Details	Lists the endpoints by organization, their backup job success summary for the report's time period, the size of the endpoint's last backup file and the average size for these files per day, and the endpoint status. **Note:** Supports ShadowProtect v4.2.7 and newer.

ImageManager Endpoint Details	• Number of replication and HSR licenses • Managed Folder summary (number of managed folders, number of images, and total disk space used) • Current endpoint status **Note:** Requires ImageManager 6 or newer.
Storage Statistics	Displays a set of daily averages for the amount of disk space used by backup image files. CMD uses this data to create a chart of projected storage space requirements for the next 3, 6, and 12 months. **Note:** This is only a rough estimate. It does not account for file consolidation or other ImageManager processes.

5.3 ShadowProtect Licensing

The *Additional Information* section under Reports can display ShadowProtect license usage for endpoints subscribed to this appliance. Click **ShadowProtect Licensing** to display this report. It shows:

Category	Description
Section header	The report is separated into organizations, then by endpoint name, in alphabetical order.
License	Shows the endpoint's ShadowProtect license key.
endpoint	Displays the name of the endpoint

Note: Accurate licensing reports requires ShadowProtect v4.2.7 or newer on the endpoint.

6 Organizations

The *Organizations* option displays a list of the currently-defined organizations and their sites on this appliance. Organizations are collections of endpoints. Sites are a subcollection of endpoints from an Organization that share common settings or a common location. The list displays:

Column	Description
Organization/Site	Shows the organization's name and any sites that are part of it.
Endpoint Count	For organizations, lists the total number of endpoints subscribed to an organization. For sites, lists the number of endpoints assigned to the site.
Actions	Displays icons for functions available to manage a site or organization.
Add Organization	Provides an Add Organization button to create a new one.

Note: Administrators cannot delete the Default Organization. While ShadowControl assigns endpoints to the Default Organization, administrators cannot.

Actions

The Action options include:

Icon	Description	Function
	Add site icon	Opens a dialog to configure a new site for the organization.
	Assign endpoints icon	Displays a filtered list of available endpoints. Checkmark one or more to add them to the site or organization.

Blue pencil icon	Opens the selected organization's configuration page. Use this page to edit the name, contacts, or status rules. (See *Using Status Rules* 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.

Assigning endpoints

When you click the organization's *Assign Endpoints* icon, ShadowControl displays a filtered list of endpoints from the Default Organization. To modify the list of endpoints, use the filtering dropdown options at the upper left of the list:

Filter	Description
Organization	Displays all endpoints matching the selected organization from the dropdown box. Initially, this is the Default Organization. endpoints marked with a checkmark are members of the selected organization in the previous dialog.
Tag	Displays all endpoints labeled with the selected tag from the dropdown box.
All endpoints	Displays all endpoints subscribed to this appliance. Those endpoints already assigned to the selected site or organizations have a checkmark.

Organizations and Status Rule Policies

Status rule policies apply to endpoints, not to organizations. This allows granular and flexible control over which endpoints in an organization use which rule policy. For example, dividing endpoints into organizations can be based on location--New York, London, Tokyo. The endpoints in each of these organizations can then be assigned different policies: a Server Policy, a PC Policy, or a Laptop Policy; rather than a single organization-wide policy.

6.1 Add Organization

When adding a new organization, select a name that reflects the shared characteristic of the endpoints in the group. For example:

endpoint Group Characteristic	Sample Names
Location	"East Campus" "Second Floor" "New York"
Department	"Accounting" "Development" "Sales"
PC Platform	"Windows 7" "Windows 2K" "Servers" "Laptops"

Note: Both organization and site names support non-English characters. They do not, however, support control characters such as "&", "?" and similar.

1. 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 organization's endpoints.
2. Select to send the contact(s) either or both reports and alerts.
3. Select the contact's preferred language. ShadowControl will send the report in the appropriate language.
4. Click **Save** to save the new organization.

New endpoints can now enroll into this organization. The administrator can also edit an existing endpoint's settings to make it a member of this organization.

6.2 Add Sites

Organizations are collections of endpoints. Sites are a subcollection of endpoints from an Organization that share common settings or a common location.

To add a site to an organization:

1. Click **Configure ShadowControl** > **Organizations** in the menu bar.
2. Select an organization to add a site to.
3. Click **Add Site** in the organization's *Actions* column.
4. In the *Add Site* dialog, enter a name for the new site.

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

5. Type in contact information for either a primary or secondary contact if the site has separate contacts (in addition to the administrator).
6. Select to send either of these contacts reports or email alerts.
   Note: The contact must have a valid email address to receive reports.
7. Specify the contact's preferred language for reports and alerts.
8. Click **Save**.

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.

Naming Sites

When naming a site, select a name that reflects the shared characteristic of the endpoints in this group. Some examples could be:

Characteristic	Examples
Location	"Second Floor" "London"
Department	"Finance" "Sales"
Platform	"Windows XP" "Windows 7"

7 Status Rules

Status Rules are the heart of ShadowControl's monitoring. These rules set thresholds for various alerts on endpoint and backup health based on extensive experience. All endpoints use the Default policy unless assigned to a specific new policy. ShadowControl provides settings for:

Status Rules are the heart of ShadowControl's monitoring. These rules set thresholds for various alerts on endpoint and backup health based on extensive experience. All endpoints use the Default policy unless assigned to a specific new policy. ShadowControl provides settings for:

- ShadowControl Rules
- ShadowProtect Rules
- ImageManager Rules

Note: Some status rules are active by default, while others are optional. Administrators can select which rules apply to an endpoint.

Severity and Status Icons

Most of the rules include a setting for severity: *Warning* or *Critical*. ShadowControl uses the severity setting as the threshold to change the icon shown for the affected endpoint in the endpoint list as well as issue notifications. An administrator can select this severity setting based on their requirements or concerns for their endpoints.

For example, an administrator may create a unique set of status rules for a Policy called "Servers" that have appropriate thresholds for this critical component. The adminstrator can then add all server endpoints to use this policy.

Endpoint-Based Rules

ShadowControl is an endpoint-focused monitoring and management tool. This means that it issues alerts for a change of state for each endpoint, not for each threshold exceeded. For example, if the endpoint's ImageManager encounters two or more backup file verification errors, ShadowControl reports the first occurence not subsequent ones. The date of this first occurence appears in the logs and is not updated for subsequent errors.

Organizations and Status Rule Policies

Status rule policies apply to endpoints, not to organizations. This allows granular and flexible control over which endpoints in an organization use which rule policy. For example, dividing endpoints into organizations can be based on location--New York, London, Tokyo. The endpoints in each of these organizations can then be assigned different policies: a Server Policy, a PC Policy, or a Laptop Policy; rather than a single organization-wide policy.

7.1 ShadowControl Rules

The Status Rules for ShadowControl include:

Rule	Description	Active by Default?	Severity Options
Endpoint Unresponsive	When checked, ShadowControl issues an alert when an endpoint has not communicated with the appliance within the specified time period.	Yes	Critical (Default), Warning

7.2 ShadowProtect Rules

The Status Rules for ShadowProtect include:

Rule	Description	Active by default?	Default Value	Rule Options	Severity Options
Failed Backup Job	When checked, triggers an alert if the endpoint has not communicated with the appliance within the specified time period.	Yes	1 Hour	Minutes, Hours (Default), Days	Critical (Default), Warning
Backup Failure Rate	When checked, triggers an alert if the endpoint exceeds the specified ratio of backup failures to backup attempts. This rule works if a backup failure occurs not just once, but on multiple occasions within a set number of backups. This rule escalates the alert that the Failed Backup Job rule generates by notifying the administrator that a pattern of failures is occuring (in other words, when the failures are not consecutive).	No	3 failures in the last 5 backup attempts	Number of backup failures, Number of toal backups	Critical (Default), Warning

Last 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" non-VSS backup. A "crash-consistent" backup may require additional recovery effort, so ShadowControl issues an alert whenever the set period of time passes without a VSS backup.	No	1 Day	Minutes, Hours, Days (Default)	Critical (Default), Warning
Paused Backup Job	When checked, ShadowControl issues an alert whenever a backup job remains paused for the set period of time.	Yes	3 days	Minutes, Hours, Days (Default)	Critical (Default), Warning
Destination Disk Usage	When checked, ShadowControl issues an alert whenever the amount of used space in the image file destination drive exceeds the specified threshold.	Yes	90% usage for Warning, 95% for Critical	Warning percentage, Criical percentage	Critical (Default), Warning
License Status	When checked, ShadowControl issues a Warning alert when a system using a ShadowProtect MSP license is 5 days from expiration. It issues a Critical alert when the MSP license expires.	Yes	N/A	None	None
Service Status	When checked, ShadowControl issues an alert if the ShadowProtect service is not responding.	Yes	N/A	None	Warning (Default), Critical

7.3 ImageManager Rules

The Status Rules for ImageManager include:

Rule	Description	Active by Default?	Default Value	Rule Options	Severity Options
Managed Folder Disk Usage	When checked, ShadowControl issues an alert if the used space on the drive with the managed folders exceeds the set threshold.	Yes	Warning: 90% Critical 95%	Specify the percent of disk space used	N/A
Verification Status	When checked, ShadowControl issues an alert if an image file fails its verification test. (This test confirms the fidelity of the file for restoration.)	Yes	Critical	Severity level	Critical, Warning
Consolidation Status	When checked, ShadowControl issues an alert if an ImageManager consolidation job fails.	Yes	Critical	Minutes, Hours, Days	Critical, Warning
Replication Queue Status	When checked, ShadowControl issues an alert when the list of files waiting to replicate exceeds the specified threshold. (This could indicate a failed network connection or destination server.)	Yes	20 files	Specify the maximum number of files in the queue	Warning (Default), Critical
License Status	When checked, ShadowControl issues a Warning alert when a system with an ImageManager MSP subscription is 5 days from the license expiration. It issues a Critical alert when the MSP license expires.	Yes	N/A	N/A	N/A
Service Status	When checked, ShadowControl issues an alert if the ImageManager service has not responded in the last five minutes.	Yes	Warning	Severity level	Warning (Default), Critical

8 SPX Policies

ShadowControl SPX policies provide a system for delivering SPX backup jobs to multiple SPX endpoints. Once created, ShadowControl applies the policy-defined backup job configuration to the selected endpoints.

An SPX policy provides two major benefits across a variety of endpoints on a network:

- Central backup job management
- Consistent backup configurations

For example, an MSP might create and apply a unique backup schedule job to each client. Once configured on each endpoint, these jobs run independently. So even if communication is lost with the ShadowControl appliance, the endpoint's backups continue.

When assigning SPX policies, ShadowControl never changes or replaces any existing backup job on the endpoint. This is true whether the existing job is locally managed or a job based on a previous SPX policy assignment. This ensures that SPX policies do not cause an endpoint to start a new backup image chain, which would require a new full backup image.

The following sections outline some important details about how SPX Policies work.

8.1 Creating a Backup Store

ShadowControl requires at least one backup store prior to creating an SPX policy. A *backup store* is a storage location, typically at a local network location, where each endpoint managed by an SPX policy stores its backup image files. When pushing a policy-based backup job to an endpoint, ShadowControl automatically generates a unique folder in the backup store for use by that endpoint. (This differs from SPX destinations which require manual creation of sub-folders for each endpoint storing backups on that device.)

Important: When creating a backup store, ShadowControl does not provide an option to browse the network to the desired location because, often, a backup store path is valid only on the endpoint and not from the ShadowControl appliance.

To add a Backup Store:

1. Select **Manage endpoints > Manage Backup Stores** in ShadowControl.
2. Click **Add Backup Store** in the *Manage Backup Stores* dialog.
3. Enter the requested data in the *Add Backup Store* dialog. Click **Save**.
   Note: Both Windows and Linux can use the same backup store. Provide a properly formatted path for both operating systems.

Field	Description
Name	Enter a descriptive name for the backup store.
Windows Path	Enter the local or network path to the destination drive and folder to use as the backup store.
Use Credentials	Check the box for destinations using Windows authentication.
Domain, User Name, Password	Specify valid credentials used to access the Windows destination.
Linux Path (Mount Point)	Specify the local mount point for the Backup Store. **Note:** Each Linux endpoint that uses this backup store must have this path defined as a local mount point.

8.2 Creating a new SPX Policy

ShadowControl guidelines for an SPX policy include:

- SPX policies only apply to endpoints running ShadowProtect SPX.
- ShadowControl can assign only one policy to each SPX endpoint.
- ShadowControl preserves any existing local backup job for a given volume on an endpoint. This prevents disrupting or ending the volume's current backup chain.

To add a new backup policy:

1. From the ShadowControl header, select **Manage Endpoints** > **ShadowProtect SPX Policies**.
2. In the *ShadowProtect SPX Policies* page, click **Add Backup Policy**.
3. In the ShadowProtect SPX Backup Policy page, provide the required information, then click **Save**.

Note: After creating a new policy, StorageCraft recommends backing up the ShadowControl appliance to ensure the policy configuration is not lost in the event of a major failure of the ShadowControl appliance. (For more information, see *Appliance Backup and Restore*.)

Settings Tab

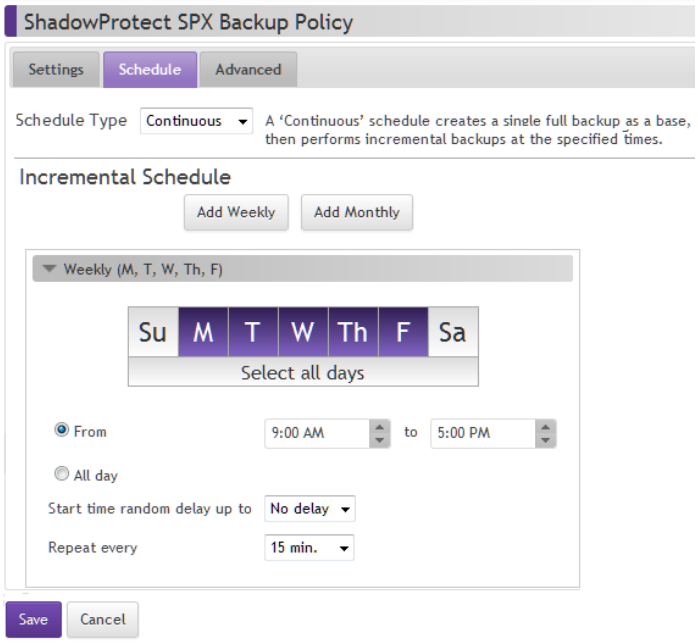
The *Settings* tab contains general information about the backup job created by this SPX policy. It contains these fields and settings:

Field	Description
Policy Name	Enter a descriptive name for the policy.
Protection Scheme	Select the type of volumes to back up: • All volumes • System Volumes only (those with an OS or a boot loader) • Data Volumes only (Any without an OS or a boot loader)
Backup Store	Select a backup store to use with this SPX policy.
Compression	Select the type of data compression to use: • *None*—Use no compression. Uses the fewest system resources but the most disk space. • *Standard*—Typically compresses data by about 40%. • *Best*—Typically compresses data by about 50%. Uses the most CPU resources but the least amount of disk space. **Note:** Most contemporary processors can provide the *Best* compression level without impacting performance.

Encryption	Select the type of data encryption to use: • None • RC4 128-bit • AES 128-bit • AES 256-bit **Note:** StorageCraft strongly recommends encrypting all backup files, particularly when replicating backup image files to StorageCraft Cloud Services or offsite.
Password	(Conditional) Provide a password for encrypting the backup image files. **Warning:** Guard this encryption password carefully. ShadowControl cannot replace an existing password nor can StorageCraft recover a lost password.

8.3 SPX Policy Scheduling

SPX provides far more flexible scheduling for backups.



Note: ShadowControl can assign only one policy to each SPX endpoint. For example, an administrator cannot run continuous incremental backups on a set of endpoints on weekdays in one chain, then have a full backup run on the*Manage Backup Stores* dialog same set of endpoints at the last day of the month independent of the continuous incremental chain.

The Schedule tab contains the following fields and settings:

Field	Description

Schedule Type	Select which type of backup to perform: **Continuous:** A *Continuous* backup schedule creates a single Full backup of the volume as a base image file. All subsequent backups are Incremental backups that capture changes to the volume. **Mixed:** A *Mixed* backup schedule creates a new Full backup of the volume on the specified day of the week or month. Subsequent backups are Incremental backups that capture changes to the volume until the next scheduled Full backup. **Full:** A *Full* backup schedule creates a new Full backup of the volume on the specified day of the week or month. **Full, Manual:** A Full, Manual schedule creates an on-demand Full backup job that runs when the endpoint receives the policy-based backup job. Administrators can create subsequent Full backups by clicking the job's **Play** control.
Full Schedule	(Mixed or Full schedule types) Specify the desired schedule for Full backups. Click **Add Weekly** or **Add Monthly** to add another layer to the schedule, up to a maximum of three. Each Full schedule layer includes the following settings: **Days of Week:** Select the specific days where this schedule layer applies. Select one or more days. **Start time:** Select the time of day to start the Full backup. **Start time random delay:** Add a random offset to the start time to help prevent a large number of Full backups from running at the same time. This helps mitigate the impact on network and storage resources. **Repeat:** Select how often this schedule resets.
Incremental Schedule	(Mixed or Continuous schedule types) Specify the desired schedule for Incremental backup. Click **Add Weekly** or **Add Monthly** to add another layer to the schedule, up to a maximum of three. Each Incremental schedule layer includes the following settings: **Days of Week:** Select the specific days where this schedule layer applies. Select one or more days. **From** or **All Day:** Select the time span during the day to create Incremental backups. All Day specifies that SPX create Incremental backups continuously. **Start time random delay:** Add a random offset to the start time to help prevent a large number of Incremental Full backups from running at the same time. This helps mitigate the impact on network and storage resources. **Repeat every:** Select how often to create incremental backups within the specified time span.

Schedule Type

Use the *Schedule Type* dropdown menu on the Schedule tab to select which type of backup to perform:

- **Continuous**
- **Mixed**
- **Full**
- **Full, Manual**

Note: SPX supports only one continuous backup job per volume.

Continuous

The Continuous incremental backup schedule type first creates a full backup of the volume as a base image file. Subsequently, SPX creates incremental backup images on the specified schedule to capture changes to the volume.

To create a continuous incremental backup schedule:

1. Select **Schedule Type** > **Continuous**.
2. Select the start time for the initial full backup: *Immediately* or *Later*. If Later, select a specified date and time to perform the backup.
3. Select the schedule for each subsequent incremental backup:

- **Add Weekly**—Creates incremental backups at the selected time and day(s) selected. Click *Add Weekly* a second or third time (not to exceed three) to add more backups at days and times that differ from the initial weekly incremental schedule.
- **Add Monthly**—Creates incremental backups at the specified days and times on a monthly schedule. Click *Add Monthly* a second or third time (not to exceed three) to add more backups at days or times that differ from the initial monthly incremental schedule.

Important: Each backup job can support up to a total of 3 scheduling rules using either or both *Add Weekly* and *Add Monthly* schedules.

4. Selecting *All day* uses a 24-hour day. Selecting *All day* is the same as specifying "00:00 to 23:59" in the *From* field.
5. Use the *Repeat every* setting to specify how often to run an incremental backup.

Scheduling Example

Unlike a typical fixed schedule function in most backup software, the flexible SPX backup scheduling feature could support one job performing a backup:

- Every 30 minutes during business hours Monday-Friday.
- Every hour at night from 6PM to 12AM to capture online transactions.
- Every 15 minutes from 6PM to 10PM on first Monday or Friday of each month to capture sales totals and reports from the field.

Mixed

The Mixed backup type starts a new backup chain on the specified day of the week or month. This job type includes a combination of a full backup then daily incremental backups run on the set schedule until the next scheduled full backup.

Important: Like in a Continuous job, the Mixed backup job supports up to three rules using a combination of *Add Weekly* and *Add Monthly* schedules.

Full

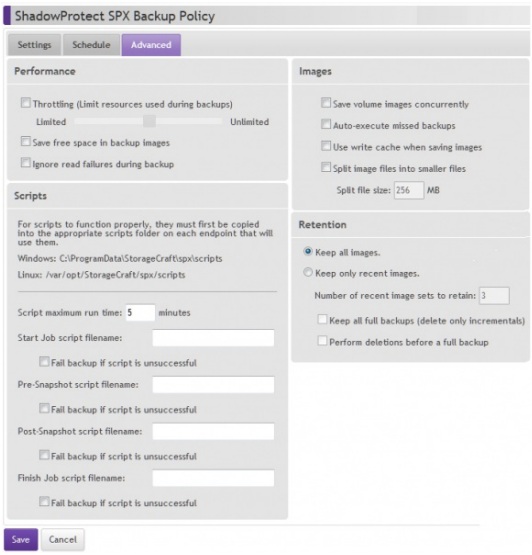
This schedule executes a full backup at the scheduled time(s) each week or month.

Full, Manual

This option executes a one-time full backup of the selected volume. This backup occurs outside of any existing scheduled backup. The one-time backup can start immediately or at a later specified date and time.

Note: If SPX is currently running a scheduled backup job when it receives the request for a manual full backup, it will automatically delay the manual request until the current job completes.

8.4 SPX Policy Advanced Settings



The *Advanced* tab options provide for more granular control over SPX backups. The Advanced tab organizes settings into these sections:

- Performance
- Scripts
- Images
- Retention

Note: The *Retention* section appears only for Mixed backup jobs.

Performance

The SPX Performance options include:

Option	Default	Description
Throttling	OFF	Limits system resources used during the backup process. For example, I/O bandwidth used by SPX to create a backup image file. (The default is 50% of resources.) Move the slider bar towards *Unlimited* to increase the amount of resources available to SPX. Move the slider towards *Limited* to reduce the resources available. **Note:** Reducing (throttling) the resources available to SPX slows its performance.
Save Volume Free Space in Backup Images	OFF	Creates a backup of all sectors on the volume including those sectors marked as free space. This can result in a much larger image file, but may help preserve previously deleted files. **Note:** This option can be changed at a later date without creating a new job.
Ignore read failures during backup	OFF	Instructs SPX to ignore disk read errors that occur during the creation of backup image files. Use this option with caution, as it may back up disk corruption and prevent a restored volume from working properly. However, in the event of a failed or failing disk, it may help preserve any remaining intact data.

Scripts

The *Scripts* section specifies command files to execute at key points in the backup image file creation process. Scripts cannot rely on any user interaction, so test each command file before using them with SPX. SPX allows from 1 to 30 minutes at each stage for command files to complete. (The default is 5 minutes.) If the command files do not complete in the specified time, SPX proceeds with the backup while the command files continue executing.

To use a command file for a particular stage in the backup process:

1. Login as a user with admin rights (in Windows) or ROOT privileges (in Linux).
   ⚠ **Caution:** Without admin rights or ROOT privileges, SPX won't copy command files into the scripts folder.
2. Copy the command file(s) into the Scripts directory in Linux:

```
/var/opt/StorageCraft/spx/libexec

in Windows, copy the files to:

C:\ProgramData|StorageCraft\spx\scripts
```

3. With the scripts copied into their folder, use the *Advanced* tab in ShadowControl to specify which scripts to run:
   - **Start Job:** Executes the specified file to prepare the system for the backup job.
   - **Pre-Snapshot:** Executes the specified script file before taking the backup. For example, you might execute a pre-snapshot script which places transaction applications or databases into a backup state.
   - **Post-Snapshot:** Executes the specified command file after taking the image snapshot. For example, to execute a post-snapshot command file to return transaction applications or databases back to their normal operating mode.
   - **Finish Job:** Executes the specified command file after SPX creates the backup image file.

   ⚠ **Note:** SPX has a 5-minute execution limit for post-backup command files. If post-backup commands require longer than five minutes, have the script call a command file that executes another command file and then finishes. This lets SPX complete the associated command file in the 5-minute allotment while the secondary command file performs tasks that take longer to complete. For example, synchronizing or copying the backup image files to an alternate location, scanning the backup image file for viruses, etc.
4. Select to have SPX halt the backup if it cannot execute a specified script.

⚠ Caution: Script paths and names must match exactly with the entries in the Advanced dialog in order to run.

Images

Provides various options for backup job actions:

Option	Default	Description
Save volume images concurrently	OFF	Enables or disables creating backup images simultaneously for multiple volumes rather than creating one backup image at a time. The system hardware needs to support a high disk load to use this option.
Auto-execute missed backups	OFF	Enables or disables executing the last scheduled backup job if it was missed. (For example, because the system was powered off.) If SPX missed more than one scheduled job, this option runs only the last unexecuted backup job.
Use write cache when saving images	OFF	Bypasses the file transfer API in SPX and instead uses Windows processes when there are issues with prolonged backup times.

Split Image Files into smaller files	OFF	*Spanned Image Set*. For example, use a spanned image set to save a large backup image file into smaller files for later transfer onto fixed-length media such as optical discs. Specify the maximum file size for each of the smaller files in the set. The default is 256MB.

Retention

SPX retention options can reduce the amount of space required for backup storage when choosing to perform a Mixed weekly or monthly backup schedule. While keeping all backup image files may provide the most options for restoring data, this type of approach has two drawbacks:

- Rapidly consumes available backup storage space
- Increases the complexity in determining which point-in-time file(s) to select for restoring

In practice, determine what points-in-time provide the desired level of protection against data loss. Select the schedule and retention policy that best matches this level of protection.

Note: SPX retention policy only applies to a *Mixed* (weekly or monthly) backup schedule. It does not apply to a *Continuous* schedule. To manage continuous incremental backup files and the space required for these files, use ImageManager.

The Retention policy options are:

Option	Default Setting	Description
Keep all images	ON	Retains all backup image files. Note that this uses the most storage space.
Keep only recent images	OFF, Retain 3 sets	Specifies the maximum number of recent image sets to keep. When SPX reaches this set maximum, it deletes the oldest image set *after* running the next backup. The default is to retain 3 sets of backups.
Keep all full backups (delete only incrementals)	OFF	Instructs SPX to delete only the incremental backup images when removing an old image set.
Perform deletions before a full backup	OFF	Instructs SPX to make room for a new image set by deleting the oldest image set *before* creating the new image set. This reduces the total amount of disk space needed to adhere to the specified retention policy. However, if the backup job is interrupted or fails, then there will be fewer remaining sets for restoring the volume.

After SPX performs the retention policy and deletes one or more backup files, it still retains the names of the deleted files and the date and time the backups occurred in its log.

8.5 Assigning SPX Policies

Administrators can assign a backup policy to endpoints in one of two ways:

- Directly from the **Manage endpoints > ShadowProtect SPX Policies** page.
- Indirectly by applying a default SPX policy to a ShadowControl Organization. Any endpoints assigned to the Organization automatically receive the default SPX policy if they do not already have a backup job configured.

Note: The *Manage Endpoints* page includes various indicators that identify the current state of each endpoint.

To assign endpoints directly:

1. From the ShadowControl header, select **Manage Endpoints** > **ShadowProtect SPX Policies**.
2. In the ShadowControl SPX Policies page, click **Manage Endpoints** <add icon> of the policy to which you want to assign endpoints.
3. In the Manage Endpoints page, select the endpoints to add to the policy.
4. Select the interval during which each endpoint randomly begins its first full backup.
   Note: This prevents overwhelming the Backup Store with multiple full backups simultaneously.
5. Click **Review Changes**.
   Note: This displays a list of all endpoints with a change from this session.
6. Click **Save** to confirm the changes made as appropriate.and finalizes the endpoint assignment.

To assign endpoints through a default policy:

1. Create the SPX policy.
2. Select **Configure ShadowControl** > **Organizations**.
3. If needed, click **Add Organization** to create a new Org group or click the *Edit Organization* icon to modify an existing organization. ShadowControl displays the Org group's configuration page.
4. In the *Default SPX Policies* section, select the desired policy in the dropdown list.
5. Select the interval during which the each endpoint randomly begins its first full backup.
   Note: This prevents overwhelming the Backup Store with multiple full backups simultaneously.
6. Click **Save**.

Note: ShadowControl applies the default policy only to endpoints assigned to the organization after configuring the default SPX policy. The default policy does not apply to existing endpoints in that organization. Also, the default policy assignment fails if the endpoint has an existing backup job or is already assigned to a different SPX policy.

8.6 SPX Policy Endpoint List

The SPX Policy Endpoint list provides:

- Indicators of endpoint SPX policy status
- Filtering to view specific groups of endpoints

Policy Indicators

Depending on their purpose, indicators appear to both the left and the right of the endpoint name. Each indicator is described in the following table:

Indicators	Description
	Indicates that no backup policy currently applies to this endpoint.
	Indicates that the endpoint is assigned to this policy. **Note:** When removing an endpoint from an SPX policy, ShadowControl asks the user what to do with the backup job created by the policy. Options include: • Convert it into a local job • Delete the job from the endpoint. **Caution:** This terminates the image chain and removes backup protection from the endpoint. However, the existing backup files remain at the Backup Store.

	Indicates that the endpoint is assigned to a different SPX policy. Click the Lock icon to reassign the endpoint to this policy. **Caution:** Reassigning an endpoint to a new policy ends the current backup job and its associated image chain. The endpoint then begins a new one under the new backup job. However, the existing backup files remain at the Backup Store.
	Moving this endpoint to a different policy.
	Unassigning this endpoint from the policy.
	Assigning this endpoint to this policy.

Filtering the Endpoint List

The Manage Endpoints page includes two different options for filtering the list of available endpoints:

Quick Search: Filters the endpoint list to those whose names include the entered criteria.

Filter Dropdown: Filters the endpoint list to include endpoints that fit in the selected category:

Category	Description
All endpoints	Shows all subscribed endpoints on the appliance
Unassigned endpoints	Shows only those endpoints not assigned to a ShadowControl SPX policy
Assigned endpoints	Shows only those endpoints assigned to a ShadowControl SPX policy.
Organization	Opens a second dropdown list to select which Organization's endpoints to show.
Tag	Opens a second dropdown list to select which user-defined Tag to use to filter the list.

8.7 Managing Policy-based Jobs

Although a user can monitor backup jobs on the endpoint using the SPX console, the user cannot modify or control (start, stop, or pause the backup) a policy-based job with SPX. ShadowControl instead provides these controls on the *Endpoint Details* page. ShadowControl also manages SPX Policies.

Unassigning an SPX Policy

An administrator can unassign an endpoint from a policy in ShadowControl. ShadowControl then presents two options to the user:

- Convert the SPX policy backup job into a locally-managed one or
- Delete the job from the endpoint

Converting to a local job preserves the existing backup chain. It also returns control of the job to the SPX console. The Pause, Play, and Stop controls become active as does editing the job's configuration.

⚠ **Caution:** Deleting the job leaves the endpoint unprotected and ends the current backup chain. However, the existing backup image files remain in the Backup Store.

Reassigning an endpoint

An administrator can also reassign an endpoint to another SPX Policy. Reassignment ends the current backup chain and starts a new one under the new policy. To do this:

1. Unassign the endpoint from its current policy.
2. Choose to delete the backup job from the endpoint.
3. Assign the endpoint to a new policy.

Note: The endpoint's existing backup files remain at the Backup Store.

Deleting an SPX Policy

ShadowControl supports deleting an SPX policy. However, an administrator must first remove all assigned endpoints from the policy before the deletion. As the administrator does so, ShadowControl again asks to:

- Convert the SPX policy backup job into a locally-managed one or
- Delete the job from the endpoint

Converting to a local job preserves the existing backup chain. It also returns control of the job to the SPX console. The Pause, Play, and Stop controls become active as does editing the job's configuration.

⚠ **Caution:** Again, deleting the job leaves the endpoint unprotected and ends the current backup chain. However, the existing backup image files remain in the Backup Store.

Scheduling an SPX policy backup

The SPX Policy dialog's *Schedule* tab includes a start time setting which randomizes when the first backup begins. This prevents overwhelming available network bandwidth and storage resources if an SPX policy runs a backup job on multiple endpoints simultaneously.

Note: Each endpoint randomizes its start time using its own local clock and not the ShadowControl appliance's time clock. If the selected start time has passed on the endpoint, the job runs at that time the next day.

Lost communication between and endpoint and ShadowControl

The endpoint's response to a loss of communication with the ShadowControl appliance depends on the cause:

Cause	Endpoint Response
The administrator unsubscribes the endpoint from the ShadowControl appliance.	This ends communication with the appliance. At that point, the ShadowControl agent automatically converts the policy-based job into a local job on the endpoint.
The administrator subscribes the endpoint to a new appliance.	The new appliance may have a new policy which the administrator could assign to the endpoint. The administrator ends the previous local job and its chain and initiates a new chain with the new policy.

The ShadowControl appliance halts temporarily or permanently.	The endpoint continues to run the configured backup job. However, users cannot access the local SPX job controls or edit the configuration of the SPX Policy-based job. At the endpoint, the administrator must run an unsubscribe from the old appliance to transfer control of it to the local SPX console and keep the current backup chain.

8.8 SPX Policy Assignments

Assigning an SPX policy to a new endpoint

When the administrator assigns an SPX Policy to an endpoint, ShadowControl distributes a backup job based on the policy configuration to that endpoint. SPX then installs the new job and SPX starts creating backups of the specified volumes on that endpoint, according to the schedule defined by the backup job. Although SPX runs the policy-based job, the endpoint user cannot use SPX to edit or control the job.

Assigning only one policy to an endpoint

An administrator can assign an endpoint to only one SPX policy. For example, if the assigned SPX policy applies to one type of volume (such as a system volume) on the endpoint, ShadowControl does not allow assigning a second policy for another volume type (such as a data volume) to the same endpoint.

Assigning an SPX Policy to an existing endpoint

As mentioned, a critical rule in the SPX Policy feature is to maintain any existing backup chain on the endpoint. When applying an SPX policy, ShadowControl detects if the endpoint already has a backup job. If it does, ShadowControl does not install the policy. ShadowControl logs a failed policy assignment in the Dashboard and in the Endpoint Details page if it cannot apply the policy to that endpoint.

ShadowControl does not guarantee that a policy gets applied to a particular endpoint. A variety of conditions can prevent ShadowControl from applying a policy to an endpoint. However, ShadowControl will continue to retry if it fails to apply the policy.

A user can allow ShadowControl to apply the SPX policy on an endpoint with an existing local backup job. The user must first select to stop and remove the local job from the endpoint then retry the SPX Policy assignment.

Note: Before migrating an endpoint to an SPX Policy, evaluate the existing local backup job. Determine if maintaining the job and its chain is preferable to applying a new policy-based job which would start a new chain for the volumes on the endpoint.

9 Updating ShadowControl

ShadowControl includes an automated system to upgrade the appliance and EndPoints as newer software versions are released. The ShadowControl Dashboard displays a notice when it detects an update is available. A similar notice also appears on the *Appliance Settings* dialog, along with an **Update Appliance** button in the *System Info* section.

ShadowControl supports two types of updates from StorageCraft:

ShadowControl includes an automated system to upgrade the appliance and endpoints as newer software versions are released. The ShadowControl Dashboard displays a notice when it detects an update is available. A similar notice also appears on the *Appliance Settings* dialog, along with an **Update Appliance** button in the *System Info* section.

ShadowControl supports two types of updates from StorageCraft:

- **Appliance-only update:** Denoted with a change to the third number in the product version. For example, 2.5.0 to 2.5.1. These updates do not require an endpoint update and do not display the endpoint update option as part of the appliance update.

- **Full upgrade:** Denoted with a change to the first or second number in the product version. For example, 2.5.0 to 2.6.0 or 2.6 to 3.0. These updates require an endpoint update along with the appliance update.

Note: StorageCraft strongly recommends exporting a copy of the appliance database before starting an update. For more information, see Appliance Backup and Restore.

To perform an appliance upgrade:

1. Note in the *Appliance Settings* dialog if the link **Update Appliance** appears.
2. If the link appears, click **Update Appliance**.
3. Specify the details of the upgrade, then click **Schedule Update**.
4. Click **OK** when prompted about the appliance being unavailable during the upgrade process.

Option	Description
Schedule Appliance Update	From the dropdown, select the size of the delay before the appliance upgrade should start. Increments go from *Start Immediately* to *Delay 12 hours*.
Endpoint Update Window	From the dropdown, select a time period within which ShadowControl should execute the updates to all subscribed endpoints. Increments go from *15 minutes* to *6 hours*. The appliance randomly assigns each endpoint an update time within this window to help reduce the impact on the network during the endpoint update process. The *Manual* option bypasses the automated endpoint update process for those who want to handle the endpoint upgrade process using other means such as Group Policy, RMM, or other scripted means. **Note:** Automatic endpoint updates require endpoint agent v2.0.0 or newer installed. **Important:** Port 5556 is a required second port for endpoint-to-appliance communication. If this port is not open, ShadowControl cannot perform endpoint updates or other bi-directional services.

Appliance OS Update

The ShadowControl Dashboard may show a message:

Appliance reboot required: *Appliance system updates have been installed. A server reboot is required to finish installing the updates.*

This indicates that the ShadowControl appliance has OS updates to install. Go to **Configure ShadowControl** > **Appliance Settings** and click **Reboot Appliance** to complete the install.

Automated Endpoint Updates

Endpoint update notices appear in either of two places:

- *Appliance Settings* page--Indicates when a system-wide agent release is included with an appliance update.
- *Endpoints* List--Indicates which endpoints need to update their agent.

With a system-wide update, click on **Update Endpoints** to schedule the process. With an individual endpoint, click on its name in the EndPoints list. Click on **Update Endpoint** to initiate the update.

Manual Endpoint Updates

To perform a manual update:

1. Download the endpoint agent from the ShadowControl product page, or directly from the ShadowControl appliance at: *https://<appliance address>/static/downloads/ShadowControl_Installer.msi*.
2. Run the endpoint installer MSI and follow the prompts in the Install Wizard.

The endpoint update retains the previous version's appliance subscription and settings.

10 Appliance Backup and Restore

The ShadowControl appliance maintains a database of subscribed endpoints and their backup history. StorageCraft recommends making a copy of this database at least weekly (and especially before and after an update) as a precaution against a system failure. While rebuilding a failed appliance is not difficult, reconfiguring the appliance and resubscribing all endpoints can take a long time, especially if the appliance has a large number of endpoints.

To backup the appliance database:

The ShadowControl appliance maintains a database of subscribed endpoints and their backup history. StorageCraft recommends making a copy of this database at least weekly (and especially before and after an update) as a precaution against a system failure. While rebuilding a failed appliance is not difficult, reconfiguring the appliance and resubscribing all endpoints can take a long time, especially if the appliance has a large number of endpoints.

To backup the appliance database:

1. In ShadowControl, select **Configure ShadowControl** > **Applicance Settings** > **Appliance Backup** > **Export Backup File**.

   Caution: The export process may take a few minutes. Do not press <F5> to refresh the screen and view the current progress of the export. Pressing <F5> causes ShadowControl to abandon the first export and initiate a new one. This prolongs the export process.

2. Select the backup file and save it to a secure location off the ShadowControl appliance.

Once the export completes, ShadowControl displays the location and date/time stamp of the exported database file.

The appliance database does not include the following, so you should keep a copy of these in a safe place as well:

- Custom branding graphics.
- Network settings.
- Custom SSL certificates.

To restore an appliance database:

1. Rerun the ShadowControl install program.
2. On the Initial Appliance Setup dialog, select **Restore this appliance from a ShadowControl database backup file**.
3. Click **Browse** to locate and select the database backup file.
4. Click **Save**. The setup program restores the appliance's configuration.
5. When the appliance install completes, manually reconfigure the appliance time zone, network settings, custom SSL certificates, and custom branding graphics.
6. Follow the remaining steps in the setup wizard to complete the restore.

Note: ShadowControl does not support restoring the database to an existing appliance. The restore process is available only during a new appliance install.

11 VMware vCenter Plug-in

The StorageCraft Plug-in for VMware vCenter integrates reporting and management functions from ShadowControl into vCenter. This provides single pane monitoring of ShadowProtect operations on VMware VMs. In vCenter, this plug-in can:

- Display all registered VMs running on a VMware host.
- Push install ShadowProtect and the ShadowControl agent to a VM (without having to login to the VM)
- Display current metrics on backup jobs. (This includes name, status, last successful time and next run time.)
- Display system metrics. (This includes the number of virtual machines deployed on a particular host server.)
- Display recent log file entries
- Display any recent errors on backup jobs. (For example, backup failed, not activated, or if no backup job is configured.)
- Launch the ShadowControl console when required

To install and use the plug-in, review the sections on:

11.1 Integration Concepts

The process of integrating vCenter with ShadowControl and ShadowProtect backup jobs involves:

- Registering Host Servers
- Associating endpoints with Virtual Machines
- Resyncing Endpoint Information

Registering Host Servers

ShadowControl needs to know the host servers managed by vCenter. It can then match up the ShadowProtect endpoints with the corrrect virtual machines on VMware. This process, called Registration, creates a link between ShadowControl and the vCenter plug-in for each host server.

The plug-in then uses this link to query statistics on all monitored endpoints on each host. In turn, ShadowControl uses this link to categorize its endpoints under the correct host severs.

Note: Use the VM Deployment tab in ShadowControl to view the vCenter host server records registered with ShadowControl.

Associating Endpoints with Virtual Machines

Once ShadowControl registers a host server on VMware, it automatically:

- Retrieves relevant information and metrics about all of the server's virtual machines.
- Link its ShadowControl endpoints to the correct virtual machines using this information.

To view the list of registered virtual machinesfor each host server, click on the binoculars icon for the desired host server in ShadowControl's *VM Deployment* tab.
Note: The plug-in uses the Compuer Name and IP address to match virtual machines with ShadowControl clients. This is why the VM needs the Tools module. Otherwise, the endpoint can't be included in the registration or resync process.

Resyncing Endpoint Information

The plug-in cannot automatically refresh the list of registered virtual machines on VMware. To refresh (resync) the list, click **Resync** in the VM Deployment tab for each host server. ShadowControl then:

- Updates the list of virtual machines
- Matches the ShadowProtect endpoints to new entries
- Deletes any virtual machines that no longer exist on VMware.

Refer to the VM Deployment tab to view the current list of registered virtual machines.

To remove an server entry from ShadowControl, click the trashcan icon for the desired entry.

Note: If this deleted server returns, re-register the server via the plug-in. Otherwise, ShadowControl will not monitor that host server's virtual machines.

11.2 vCenter System Requirements

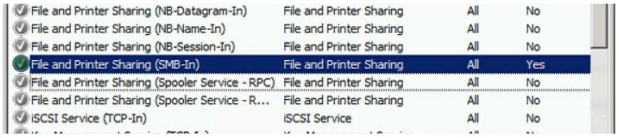
The StorageCraft vCenter Plug-in requires:

- VMware vCenter v5.1 or v5.5 (vCenter requirements)
  ⚠ **Note:** The plug-in does not support the *vCenter Server Appliance*.
- WMware vSphere 5.5
- Workstation with vSphere Web Client and Administrator access to vCenter
- VMware Tools module installed on each VM client (Refer to Installing VMware Tools on the VMware website for details.)

Note: Without the Tools module, endpoints won't appear in the ShadowControl plug-in list.

- Active ShadowControl v2.5.0 or newer appliance

Potential endpoints also require Share access configured in the client firewall:

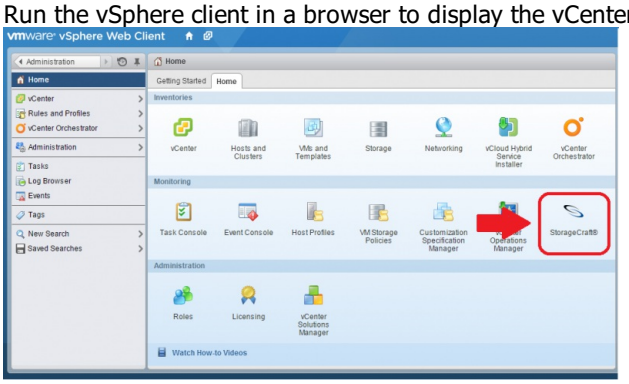


VMware Tools Requirement

Each VM client requires a Tools module installed into its operating system to report basic information such as its Computer Name and IP addresses. As these properties come from the operating system and not hardware, vCenter cannot determine these properties without this Tools module. Administrators often require basic information about the operating system when looking at the VMs in vCenter. In addition, the ShadowControl integration with vCenter also requires the Computer Name and IP addresses. Refer to the VMware online guide for details on installing this module.

11.3 Installing the vCenter Plug-in

To install the vCenter plug-in:

1. Open ShadowControl.
2. Open the *Manage Endpoints* dropdown menu from the menu bar:
   
3. Select **VM Deployment.** ShadowControl displays the VM Deployment dialog.
   Note: The VM Deployment option only appears for users with Administrator rights. It does not appear for Read-Only users.
4. Click **Setup vCenter Plug-in** at the lower left of the dialog.
5. In the *vCenter Plug-in Setup* dialog, enter the:
   - IP Address or Hostname for the vCenter system
   - Valid credentials to log into vCenter.
   - Alternate port if the default Port 443 is in use by another process.
   Note: The plug-in does not support the *vCenter Server Appliance*.
6. Click **Install Plugin**.
7. Log out of vSphere, then log back in.
8. Run the vSphere client in a browser to display the vCenter home page and open a session with the vCenter host.
   

   Note the addition of the StorageCraft icon in the Monitoring section. This indicates that the plug-in successfully installed.
9. Proceed to the *Configure the vCenter Plug-in* section.

11.4 Configure the vCenter Plug-in

After installing the StorageCraft vCenter plug-in, select Settings in the left-side menu to configure the plug-in:

Setting	Description

Server Hostname	Specify either the host name or the IP address of the ShadowControl appliance. **Note:** The hostname field can include a port but does not need a prefix. For example, enter "cmd.mydomain.com:9090" or "127.0.0.1:8080". Do *not* enter "https://cmd.mydomain.com".
Username	Specify a valid user to log into the appliance.
Password	Provide the user's valid password.
Test Credentials	Click **Test Credentials** to confirm the user login.
Update	Click **Update** to save the settings.

To continue the configuration:

1. Click **Administration** in the left-hand navigation pane on the vCenter home page..
2. Click **StorageCraft** > **Summary** to display the Summary dialog.
   Note: The dialog displays a message to register a vCenter server with the plug-in. Until a successful server registration, the log and metric panes remain blank.
3. Click on the *vCenter Server* dropdown in the upper-left of the pane to show a list of active vCenter hosts.
4. Select a vCenter host from the iist.
5. Click **Register**. ShadowControl completes the connection between vCenter and itself using the plug-in.
   The system matches the VMs with the ShadowControl clients, then populates the charts and information panes with available data for that host's VMs.
6. Repeat these last three steps for each vCenter server.
7. Click **Summary** in the left navigation pane to display the ShadowProtect Summary.

The Dashboard now populates with information from endpoints from all of the hosts.

In common practice, one or more of the vCenter client VMs will need the ShadowControl agent or ShadowProtect installed. Use the instructions in the Push Install section to perform these operations.

11.5 Perform Push Installs

The vCenter plug-in supports push installs to one or more selected endpoints for:

- ShadowProtect (including software and license activation)
- ShadowControl agent (incuding subscribing and organization assignment)

A push install can also assign one of several default backup job configurations to these endpoints.

Push Install Requirements

To perform correctly, the Push Install feature requires:

The vCenter plug-in supports push installs to one or more selected endpoints for:

- ShadowProtect (including software and license activation)
- ShadowControl agent (incuding subscribing and organization assignment)

A push install can also assign one of several default backup job configurations to these endpoints.

Push Install Requirements

To perform correctly, the Push Install feature requires:

- The UTC time of the appliance and the endpoint system must be within five minutes of each other. So if the ShadowControl appliance time is 12:00 and the endpoint time is 12:15, the push install fails. Time zone is not relevant.
- Destination endpoints require access to the c$ share.

- Push Install requires *Classic* security access to operate. On systems that do not have c$ share access, most likely Windows operates in a so-called "simple file sharing" mode. In this simple mode, Windows will only provide *guest level access* and not *Classic* access to the requester when:

- Trying to access the endpoint over the network
- Using credentials that are local to that destination server or client

To fix this:

1. Go to **Start** > **Run** > **secpol.msc** > **Local Policies** > **Security Options**.
2. Change "*Network Access: Sharing and security model for local accounts*" to "*Classic - local users authenticate as themselves*".

- Push Install may also fail when blocked by Windows Remote User Account Control. The *LocalAccountTokenFilterPolicy* setting affects how administrator credentials are applied to remotely administer the computer. Before performing a push install with a Windows Vista or Windows 7 machine, configure a registry setting at a command prompt:

```
reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\system"
 /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

Note: The above command should be entered as one line with a space before the "/v".

Performing a Push Install

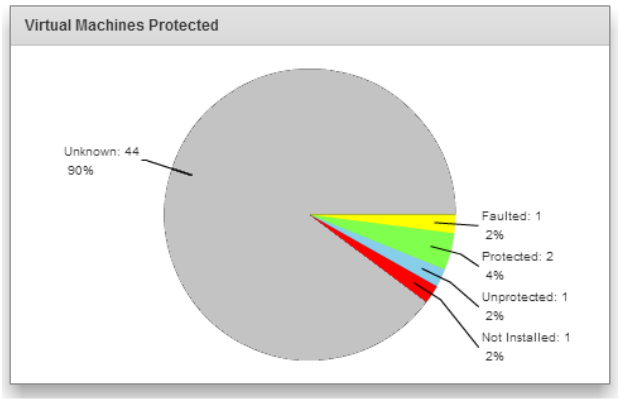
To perform a push install, first determine if the install is for:

- One endpoint
- Multiple Endpoints

One Endpoint Push Install

To perform a push install for one endpoint::

1. Click **Summary** in the vSphere dialog.
2. In the *Virtual Machines Protected* pane of the ShadowProtect Summary page, click on either of these sections of the chart:
   Unknown--This indicates that neither ShadowProtect nor the ShadowControl agent are installed.
   Not Installed--This indicates that the ShadowControl agent is installed but not ShadowProtect.



   The plug-in displays a list of the VMs that match that status (no ShadowProtect or no ShadowControl agent).

3. Click **Install ShadowProtect** in the right-hand column of the endpoint. The plug-in displays the *Push Install ShadowProtect* dialog (see below).

Multiple endpoints Push Install

To perform a push install to multiple endpoints:

1. Select **Manage Endpoints** > **VM Deployment**.
2. Select the host with the endpoints that need ShadowProtect or ShadowControl in the VM Deployment dialog.
3. Select the desired endpoints from the list in the *Manage Clients* dialog.
4. Click **Push Install ShadowProtect**.

The plug-in displays the *Push Install ShadowProtect* dialog (see below).

Push Install ShadowProtect Dialog

Use this dialog to:

- Configure the push install

- Define a backup job
- Specify licenses and activate them

Configure the push install

The dialog provides three tabs to configure the install:

- *Configuration*--covers options for the software install.
- *Backup Job*--(Optional) Specifies a backup job for the selected endpoint(s).
- *Licensing*--Specifies and activates a ShadowProtect license for the selected endpoint(s).

Select the *Configuration* tab to specify:

Section	Option	Details
ShadowControl		
	Subscribe to organization	Mark this option and specify which organization to subscribe the endpoint to. (Use ShadowControl to specify the site if required.)
ShadowProtect		
	ShadowProtect Installer	Use the dropdown list to select which version of ShadowProtect to install.
	Installer Language	Use the dropdown list to select which language the installer uses. (Note: The language must match the license.)
Endpoint Credentials		Provide the login credentials for each endpoint listed. If all of the listed endpoints have the same administrator credentials, use the **Down** arrow button to fill in those fields automatically.
	Domain	Specify the domain the endpoint is part of (if required).
	User Name	Specify a user name which has administrator rights to the endpoint.
	Password	Provide a valid password for the user.
License Agreement		Mark the EULA acceptance to continue.

Select the *Backup Job* tab to specify the default backup job for the selected endpoint(s):

Option	Details
Job Type	Select a default backup job type from the dropdown list. The types are: every 30 minutes (24-7), every hour (8-6) M-F, every two hours (8-6) M-F with a full backup on Sunday, or twice a day with a full backup once a month, **Note:** For more options, use ShadowProtect to create a backup job for the specific endpoint(s).
Job Name	Specify a name for the backup job.
Encryption Password	Specify a password to encrypt the backup files.
Source Volumes Types	Select the type(s) of volume(s) to backup from the dropdown list--all, only boot volumes, or only data volumes.
Destination Name	Specify the name of the destination (as defined in ShadowProtect.
Destination Path	Specify the path to the backup destination.
Credentials	Provide the domain, username, and password to log into the backup destination.

EULA Agreement	Mark the agreement to continue the install.

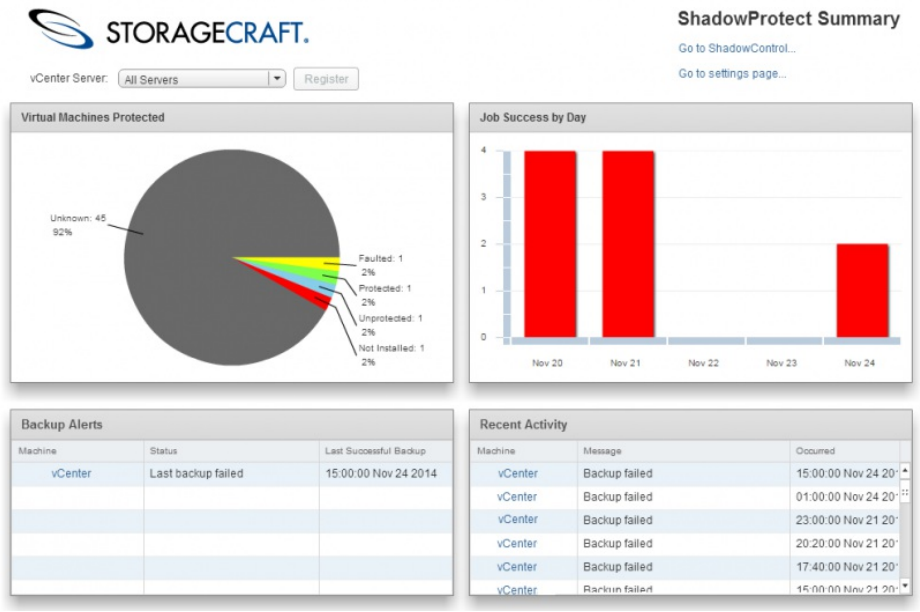
Select the *Licensing* tab to specify the product key(s) for the endpoint(s):

Option	Details
Product Keys	Enter the ShadowProtect license key(s), one per line. Include enough keys for the number of selected endpoints. **Note:** This feature works for remotely activating ShadowProtect v5.1.0 or later. Use ShadowProtect to activate licenses for older versions.
License Information	These are optional. Specify a customer name and their organization. Best Practice is the name of an administrator who manages ShadowProtect.
EULA Agreement	Mark the agreement to continue the install.

Once the options in the three tabs are selected, click **Push Install ShadowProtect** in the *Licensing* tab. This starts the install process. When the process completes, reboot the endpoint(s) as needed.

11.6 Using the Summary Dashboard

The StorageCraft plug-in displays a Summary Dashboard once it runs with registered hosts and endpoints:



The dashboard includes five elements:

- Menu Pane
- Virtual Machines Chart
- Job Success Pane
- Backup Alerts Pane
- Recent Activity Pane

Menu Pane

The top of the Summary Dashboard offers three options:

- vCenter Server
- Go to ShadowControl
- Got to settings page

vCenter Server

Use this dropdown to select:

- **All Servers**--Displays backup status information from all regsistered hosts
- **A particular listed host**--Displays the backup status of vMs from the selected host

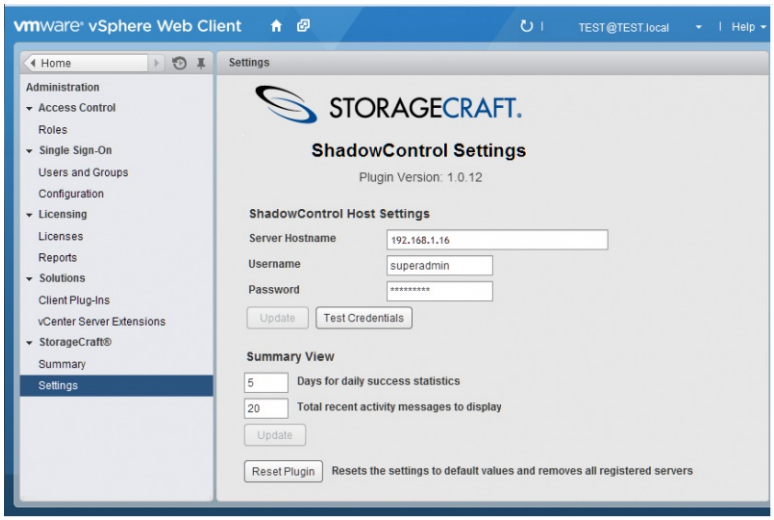
Use the **Resync** button to update information from the selected hosts.

Go to ShadowControl

Click this option to open the ShadowControl console. This does not require a separate login.

Go to settings page

This option opens the StorageCraft plug-in's Settings page in vCenter. The Settings page manages the ShadowControl host's login credentials. It also sets the metrics for the Summary Dashboard: the number of days to display the daily success statistics and the tolal number of revent activity messages to display.



Virtual Machines Protected Chart

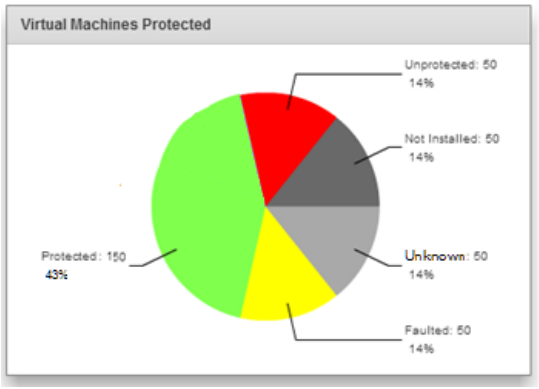
The Virtual Machines Protected chart by detault provides:

- Current status of the endpoints on all hosts
- Drill-down feature to display a list of the endpoints in the selected category

Note: Selecting a specific host in the vCenter Server dropdown list changes the chart to display the status of only those endpoints in the selected host.

Current Status of the endpoints

Each segment of the chart indicates the current status of endpoints:



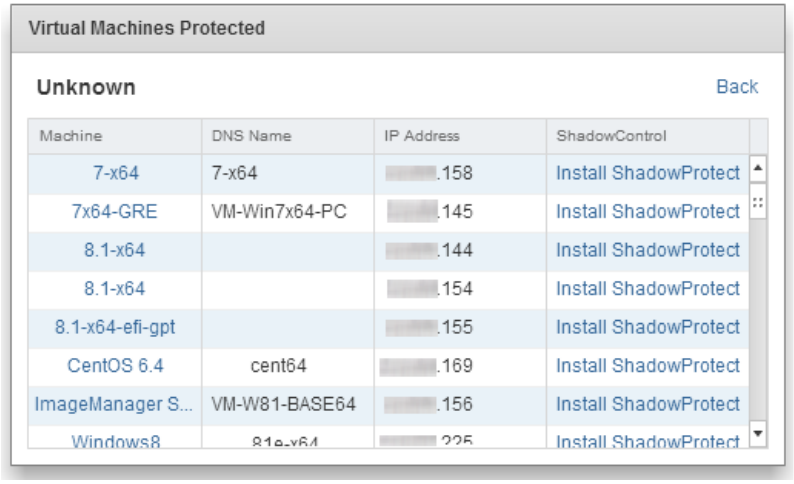
These include:

- **Unknown**--The plug-in cannot communicate with the endpoint. Most likely the endpoints require the ShadowControl agent installed. It may also indicate a neetworking issue.
- **Faulted**--One or more errors exist with ShadowProtect performing backups.
- **Protected**--These endpoints have ShadowProtect installed and have had successful backups run.
- **Unprotected**--These endpoints may or may not have ShadowProtect installed or the first backup job has not yet run.
- **Not Installed**--These endpoints have the ShadowControl agent installed but not ShadowProtect.

Note: Click on a segment to view a drill-down list of endpoints with that status.

Drill-down List

The drill-down list shows the endpoints with the selected status:



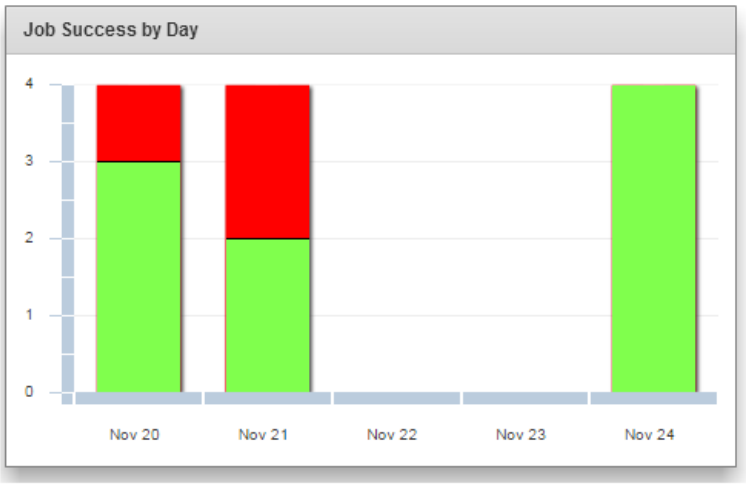
The list also shows whether ShadowProtect is installed (and with it, the ShadowControl agent).

Note: The Unknown list comes from vCenter since the ShadowControl agent or ShadowProtect may not be installed. Since it comes from vCenter, it may list VMs with operating systems not supported by ShadowProtect. (Note the CentOS 6.4 VM in the listing.)

- Click **Install** in the ShadowControl column to open ShadowControl's *Manage Clients* dialog. In that dialog, select one or more unprotected endpoints to push install ShadowProtect or the ShadowControl agent. (See Push Insatall for details.)
- Click on the name of a VM in the *Machine* column to display vCenter's Summary page for that VM:

Job Success Pane

The Job Success by Day pane shows the number of attempts made to complete that day's backup jobs:



The colors in the bar varies--green for success, red for a failed attempt.

Note: The height of the bar may vary from day-to-day depending on the number of backup jobs scheduled for that day.

Backup Alerts Pane

This pane displays a list of any ShadowProtect alerts issued. It also shows the last successful backup for the VM where backups fail.

Note: This list is a sub-set of the messages listed in the Recent Activity pane.

Recent Activity Pane

This pane shows a list of any ShadowProtect-issued messages for the monitored VMs.

12 Microsoft System Center Plug-In

Users of the *Microsoft System Center Virtual Machine Manager* (VMM) can now view ShadowControl metrics and log files via an optional plug-in. The StorageCraft Plug-in for System Center VMM provides single pane monitoring of ShadowProtect operations on System Center VMs. This plug-in connects the running ShadowControl appliance with an existing instance of VMM to:

- Display all registered VMs running on a VMM server.
- Push install ShadowProtect and the ShadowControl agent to a VM (without having to login to the VM)
- Display current metrics on backup jobs. (This includes name, status, last successful time and next run time.)
- Display system metrics. (This includes the number of virtual machines deployed on a particular host server.)
- Display recent log file entries
- Display any recent errors on backup jobs. (For example, backup failed, not activated, or if no backup job is configured.)
- Launch the ShadowControl console when required

To install and use the plug-in, review the:

- Integration Concepts
- System Center Requirements
- Install the System Center Plug-in
- Configure the Plug-in
- Perform Push Installs
- Using the Summary Dashboard

12.1 Integration Concepts

The process of integrating VMM with ShadowControl and ShadowProtect backup jobs involves:

- Registering Host Servers
- Associating Endpoints with Virtual Machines
- Resyncing Endpoint Information

Registering Host Servers

ShadowControl needs to know the host servers manageed by System Center VMM. It can then match up the ShadowProtect endpoints with the corrrect virtual machines on VMM. This process, called Registration, creates a link between ShadowControl and the System Center plug-in for each host server.

The plug-in then uses this link to query statistics on all monitored endpoints on each host. In turn, ShadowControl uses this link to categorize its endpoints under the correct host severs.

Note: Use the VM Deployment tab in ShadowControl to view the System Center host server records registered with ShadowControl.

Associating Endpoints with Virtual Machines

Once ShadowControl registers a host server on VMM, it automatically:

- Retrieves relevant information and metrics about all of the server's virtual machines.
- Link its ShadowControl endpoints to the correct virtual machines using this information.

To view the list of registered virtual machinesfor each host server, click on the binoculars icon for the desired host server in ShadowControl's *VM Deployment* tab.

Note: The plug-in uses the Compuer Name and IP address to match virtual machines with ShadowControl clients. This is why the VM needs the Tools module. Otherwise, the endpoint can't be included in the registration or resync process.

Resyncing Endpoint Information

The plug-in cannot automatically refresh the list of registered virtual machines on VMM. To refresh (resync) the list, click **Resync** in the VM Deployment tab for each host server. ShadowControl then:

- Updates the list of virtual machines
- Matches the ShadowProtect endpoints to new entries
- Deletes any virtual machines that no longer exist on VMM.

Refer to the VM Deployment tab to view the current list of registered virtual machines.

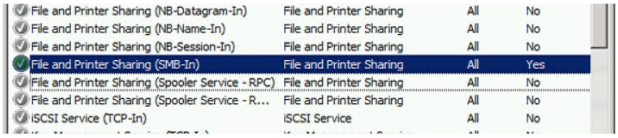
To remove an server entry from ShadowControl, click the trashcan icon for the desired entry. Note: If this deleted server returns, re-register the server via the plug-in. Otherwise, ShadowControl will not monitor that host server's virtual machines.

12.2 System Center Requirements

Installing the ShadowControl plug-in on VMM requires:

- Microsoft System Center 2012 R2
- Virtual Machine Manager active on System Center
- Administrator access to Microsoft System Center Virtual Machine Manager
- Virtual Guest Services installed on each client VM
- Active ShadowControl v2.5.0 or newer appliance

Potential endpoints also require Share access configured in the client firewall:



Otherwise, these endpoints will not appear in the VMM list.

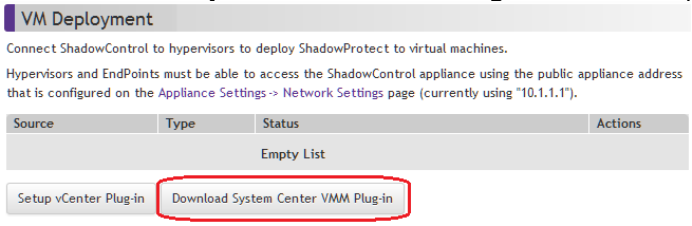
Virtual Guest Services Requirement

Each VM client requires a Virtual Guest Services module installed to report basic information such as its Computer Name and IP addresses. As these properties come from the operating system and not hardware, System Center VMM cannot determine these properties without this module. (Administrators often require this basic information on VMs in VMM. In addition, the ShadowControl integration with System Center also requires the Computer Name and IP addresses.) Refer to the MSDN article for details on installing this module.

12.3 Install the System Center Plug-in

To install the ShadowControl VMM plug-in:

1. Run ShadowControl.
2. Open the *Manage Endpoints* dropdown menu from the menu bar:

3. Click **VM Deployment**.
   Note: The VM Deployment option only appears with Admnistrator rights. It does not appear for Read-Only users.
4. Click **Download System Center VMM Plug-in** in the VM Deployment dialog.


   ShadowControl displays a download dialog.
5. Download the zipped file to a folder accessible from the VMM system.
6. Run as Administrator the System Center Virtual Machine Manager.
7. Login as an administrator to VMM.
8. Click **Settings** at the lower left of the main dialog.
9. Click **Import Console Add-in** from the ribbon menu at the top of the dialog.
10. Follow the steps in the *Import Add-in* wizard to select and install the downloaded zipped file containing the plug-in. System Center adds the ShadowProtect menu icon to the list of installed add-ins.
11. Go to **Settings** > **Console Add-ins**.
12. Click the ShadowControl plug-in icon in the VMM menu bar to display the ShadowControl dashboard.

Use this dashboard to monitor and manage endpoints from within VMM.

Uninstall the ShadowProtect Plug-in

To uninstall the plug-in:

1. Run System Center VMM.
2. Click **Settings** at the lower left of the main dialog.
3. Click **Console Add-ins** from the navigation pane.
4. Highlight the ShadowProtect Add-in icon in the grid.
5. Click **Remove**.

12.4 Configure System Center

Now that the ShadowControl plug-in is installed in VMM and the ShadowControl icon appears in the Console Add-ins menu, create a connection to ShadowControl.

To connect to ShadowControl and begin monitoring servers:

1. Run VMM.
2. Open the VMs and Services menu.
3. Select one of the host servers from the menu.
4. Click **ShadowProtect** in the Home ribbon menu. VMM displays the ShadowProtect summary dialog for the selected server with a notice to configure the ShadowControl hostname in the Settings dialog.
5. Click on the *Settings...* link in the upper-right of the dialog. VMM opens the Settings dialog.
6. Enter the hostname for the ShadowControl appliance then appropriate credentials to log into the appliance.
7. Click **Test Credentials** to confirm the login process works.
8. Click **Save**. VMM returns to the ShadowControl summary dialog.
9. Click **Register**. VMM sends the required information on each virtual machine from the selected host to ShadowControl.
   Note: When the registration process completes, VMM populates the summary dialog panes with metrics for the selected

host's virtual machines.
10. Repeat Steps 2-10 for each host server in VMM.

Now that VMM has registered each host server with ShadowControl, both monitoring services now display current information on backup jobs and protection status for the virtual machines. In common practice, one or more of the endpoints will require installing ShadowProtect or the ShadowControl agent. Use the Push Install section to perform these installs.

12.5 Perform Push Installs

The System Center VMM plug-in supports push installs to one or more selected endpoints for:

- ShadowProtect (including software and license activation)
- ShadowControl agent (incuding subscribing and organization assignment)

A push install can also assign one of several default backup job configurations to these endpoints.

Push Install Requirements

To perform correctly, the Push Install feature requires:

The System Center VMM plug-in supports push installs to one or more selected endpoints for:

- ShadowProtect (including software and license activation)
- ShadowControl agent (incuding subscribing and organization assignment)

A push install can also assign one of several default backup job configurations to these endpoints.

Push Install Requirements

To perform correctly, the Push Install feature requires:

- The UTC time of the appliance and the endpoint system must be within five minutes of each other. So if the ShadowControl appliance time is 12:00 and the endpoint time is 12:15, the push install fails. Time zone is not relevant.
- Destination endpoints require access to the c$ share.

- Push Install requires *Classic* security access to operate. On systems that do not have c$ share access, most likely Windows operates in a so-called "simple file sharing" mode. In this simple mode, Windows will only provide *guest level access* and not *Classic* access to the requester when:

    - Trying to access the endpoint over the network
    - Using credentials that are local to that destination server or client

  To fix this:

1. Go to **Start** > **Run** > **secpol.msc** > **Local Policies** > **Security Options**.
2. Change "*Network Access: Sharing and security model for local accounts*" to "*Classic - local users authenticate as themselves*".

- Push Install may also fail when blocked by Windows Remote User Account Control. The *LocalAccountTokenFilterPolicy* setting affects how administrator credentials are applied to remotely administer the computer. Before performing a push install with a Windows Vista or Windows 7 machine, configure a registry setting at a command prompt:

```
reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\system"
 /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

Note: The above command should be entered as one line with a space before the "/ v".

Performing a Push Install

To perform a push install, determine if the install is for:

- One endpoint
- Multiple Endpoints

One Endpoint Push Install

To perform a push install for one endpoint::

1. In System Center VMM, select VMs and Services from the left-side menu.
2. In the ribbon menu, seelct *StorageCraft*.
3. In the *Virtual Machines Protected* panef of the *ShadowProtect Summary* page, click on either of these sections of the chart:
   Unknown--This indicates that neither ShadowProtect nor the ShadowControl agent are installed.
   Not Installed--This indicates that the ShadowControl agent is installed but not ShadowProtect.

   The plug-in displays a list of the VMs that match that status (endpoints that have no ShadowProtect or no ShadowControl agent).

4. Click **Install ShadowProtect** in the right-hand column of the endpoint. The plug-in displays the *Push Install ShadowProtect* dialog (see below).

Multiple endpoints Push Install

To perform a push install to multiple endpoints:

1. In ShadowControl, select **Manage Endpoints** > **VM Deployment**. ShadowControl displays
2. Select the host with the endpoints that need ShadowProtect or ShadowControl from the *VM Deployment* dialog. The program opens the *Manage Clients* dialog. This
3. Select the desired endpoints from the list of all of the endpoints hosted by the selected hypevisor.
4. Click **Push Install ShadowProtect**.

The plug-in displays the *Push Install ShadowProtect*dialog (see below).

Push Install ShadowProtect Dialog

Use this dialog to:

- Configure the push install
- Define a backup job
- Specify licenses and activate them

Configure the push install

The dialog provides three tabs to configure the install:

- *Configuration*--covers options for the software install.
- *Backup Job*--Specifies a backup job for the selected endpoint(s). This is optional.
- *Licensing*--Specifies and activates a ShadowProtect license for the selected endpoint(s).

Select the *Configuration* tab to specify:

Section	Option	Details
ShadowControl		
	Subscribe to organization	Mark this option and specify which organization to subscribe the endpoint to. (Use ShadowControl to specify the site if required.)
ShadowProtect		
	ShadowProtect Installer	Use the dropdown list to select which version of ShadowProtect to install.
	Installer Language	Use the dropdown list to select which language the installer uses. ⚠ **Note:** The language must match the license.
Endpoint Credentials		Provide the login credentials for each endpoint listed. If all of the listed endpoints have the same administrator credentials, use the **Down** arrow button to fill in those fields automatically.

	Domain	Specify the domain the endpoint is part of (if required).
	User Name	Specify a user name which has administrator rights to the endpoint.
	Password	Provide a valid password for the user.
License Agreement		Mark the EULA acceptance to continue.

Select the *Backup Job* tab to specify the default backup job for the selected endpoint(s):

Option	Details
Job Type	Select a default backup job type from the dropdown list. The types are: every 30 minutes (24-7), every hour (8-6) M-F, every two hours (8-6) M-F with a full backup on Sunday, or twice a day with a full backup once a month, ⚠ **Note:** For more options, use ShadowProtect to create a backup job for the specific endpoint(s).
Job Name	Specify a name for the backup job.
Encryption Password	Specify a password to encrypt the backup files.
Source Volumes Types	Select the type(s) of volume(s) to backup from the dropdown list--All, only boot volumes or only data volumes.
Destination Name	Specify the name of the destination (as defined in ShadowProtect.
Destination Path	Specify the path to the backup destination.
Credentials	Provide the domain, username, and password to log into the backup destination.
EULA Agreement	Mark the agreement to continue the install.

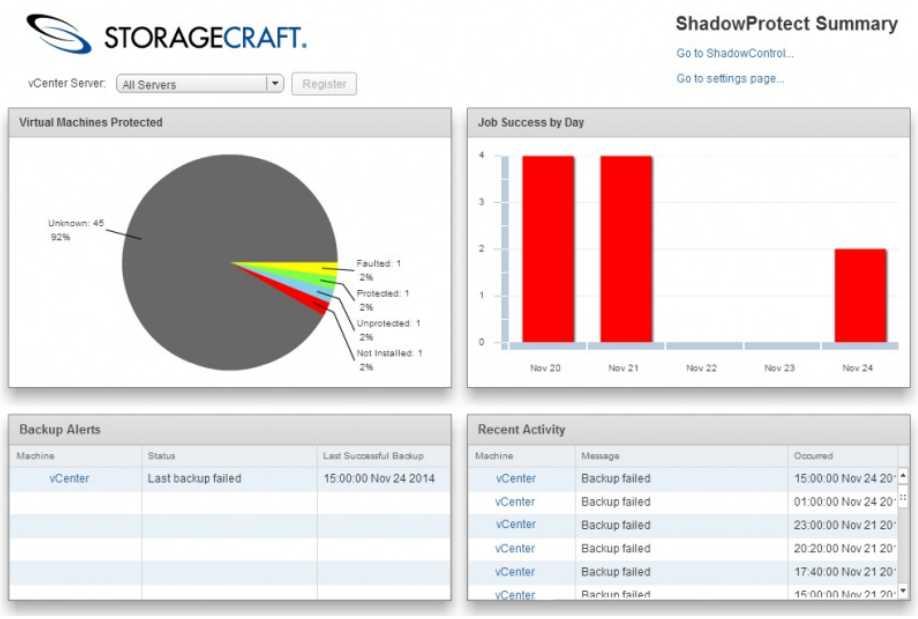
Select the *Licensing* tab to specify the product key(s) for the endpoint(s):

Option	Details
Product Keys	Enter the ShadowProtect license key(s), one per line. Include enough keys for the number of selected endpoints. ⚠ **Note:** This feature works for remotely activating ShadowProtect v5.1.0 or later. Use ShadowProtect to activate licenses for older versions.
License Information	These are optional. Specify a customer name and their organization. Best Practice is the name of an administrator who manages ShadowProtect.
EULA Agreement	Mark the agreement to continue the install.

Once the options in the three tabs are selected, click **Push Install ShadowProtect** in the *Licensing* tab. This starts the install process. When the process completes, reboot the endpoint(s) as needed.

12.6 Using the Summary Dashboard

The StorageCraft plug-in displays a Summary Dashboard once it runs with registered hosts and endpoints:



The dashboard includes five elements:

- Menu Pane
- Virtual Machines Chart
- Job Success Pane
- Backup Alerts Pane
- Recent Activity Pane

Menu Pane

The top of the Summary Dashboard offers three options:

- vCenter Server
- Go to ShadowControl
- Got to settings page

vCenter Server

Use this dropdown to select:

- **All Servers**--Displays backup status information from all regsistered hosts
- **A particular listed host**--Displays the backup status of vMs from the selected host

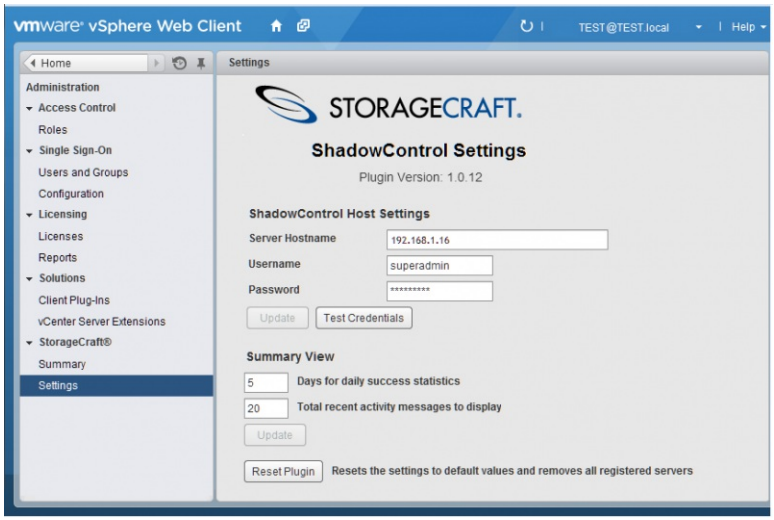
Use the **Resync** button to update information from the selected hosts.

Go to ShadowControl

Click this option to open the ShadowControl console. This does not require a separate login.

Go to settings page

This option opens the StorageCraft plug-in's Settings page in vCenter. The Settings page manages the ShadowControl host's login credentials. It also sets the metrics for the Summary Dashboard: the number of days to display the daily success statistics and the tolal number of revent activity messages to display.



Virtual Machines Protected Chart

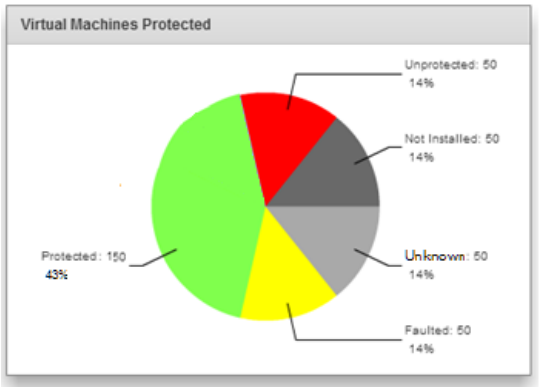
The Virtual Machines Protected chart by detault provides:

- Current status of the endpoints on all hosts
- Drill-down feature to display a list of the endpoints in the selected category

Note: Selecting a specific host in the vCenter Server dropdown list changes the chart to display the status of only those endpoints in the selected host.

Current Status of the endpoints

Each segment of the chart indicates the current status of endpoints:



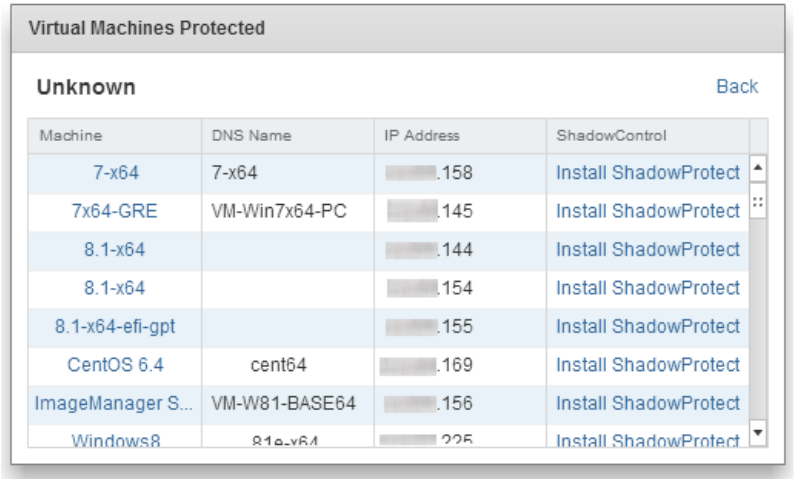
These include:

- **Unknown**--The plug-in cannot communicate with the endpoint. Most likely the endpoints require the ShadowControl agent installed. It may also indicate a neetworking issue.
- **Faulted**--One or more errors exist with ShadowProtect performing backups.
- **Protected**--These endpoints have ShadowProtect installed and have had successful backups run.
- **Unprotected**--These endpoints may or may not have ShadowProtect installed or the first backup job has not yet run.
- **Not Installed**--These endpoints have the ShadowControl agent installed but not ShadowProtect.

Note: Click on a segment to view a drill-down list of endpoints with that status.

Drill-down List

The drill-down list shows the endpoints with the selected status:



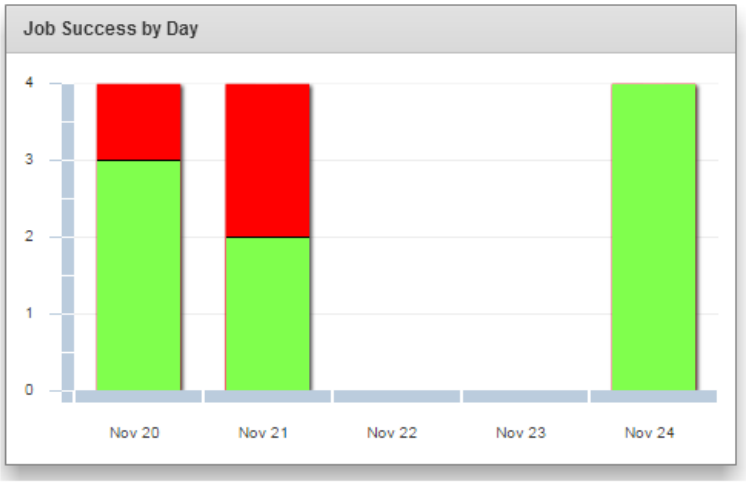
The list also shows whether ShadowProtect is installed (and with it, the ShadowControl agent).

Note: The Unknown list comes from vCenter since the ShadowControl agent or ShadowProtect may not be installed. Since it comes from vCenter, it may list VMs with operating systems not supported by ShadowProtect. (Note the CentOS 6.4 VM in the listing.)

- Click **Install** in the ShadowControl column to open ShadowControl's *Manage Clients* dialog. In that dialog, select one or more unprotected endpoints to push install ShadowProtect or the ShadowControl agent. (See Push Insatall for details.)
- Click on the name of a VM in the *Machine* column to display vCenter's Summary page for that VM:

Job Success Pane

The Job Success by Day pane shows the number of attempts made to complete that day's backup jobs:



The colors in the bar varies--green for success, red for a failed attempt.

Note: The height of the bar may vary from day-to-day depending on the number of backup jobs scheduled for that day.

Backup Alerts Pane

This pane displays a list of any ShadowProtect alerts issued. It also shows the last successful backup for the VM where backups fail.

Note: This list is a sub-set of the messages listed in the Recent Activity pane.

Recent Activity Pane

This pane shows a list of any ShadowProtect-issued messages for the monitored VMs.

13 Appendix: ShadowControl Report API

These instructions require experience in:

- Making HTTP requests in a RESTful environment
- Programming or scripting skills and text parsing
- JSON-formatted output

StorageCraft does not support any of these processes and provides this content only on an AS IS basis.

ShadowControl has one reporting API. This API allows a Get Request to retrieve endpoint report information for use in an external reporting system. This information can be:

- Historical Endpoint Data - /api/reports/history/
- Endpoint Current Status - /api/reports/status/

Once ShadowControl receives a request, it then:

- Filters the data based on the access token included in the request. For example, using an unrestricted token delivers data on all endpoints on the appliance. Entering a restricted token delivers data for only those endpoints that are members of a particular organization or site (as specified in the token's configuration)..
- Sorts these results by *organization* then by each *site* in that organization.

Tokens

ShadowControl includes a feature to create credential tokens. Using a token allows limited access to ShadowControl without exposing credentials (username/password) in scripts.

Note: A Report API token only allows access to the specified historical or status endpoint data. It does not provide access to any other features of ShadowControl or other data.

To create a token for this request:

- Select a *Report API Access* token Type.
- Specify the expiration date (if desired) for the token.
- Specity the organization data the token has access to: unrestricted (all) or the selected organization/site

Example

An example of a reports status request using curl would be:

```
curl -v -k -H "CMD_TOKEN:<Token>" https://<appliance>/api/reports/status/<UUID of endpoint>/
```

where:

- -v is an option to show verbose errors,
- -k is an option to allow a connection to an appliance that does not have a trusted cert.
- -H CMD_TOKEN <*token*> is a required argument which adds the access token to the request header. Note that the quote marks are optional, as the marks are only required when there's a space in the string.
- <UUID of endpoint> is an option to indicate which endpoint data to return. Without this option, ShadowControl responses with data on all endpoints subscribed to the appliance.

Here are two examples of the format for the resulting JSON responses for a History request or for a Status request:

Historical Data Reporting: /api/reports/history/[<endpt uuid>/]

```
{ "<endpt uuid>":
  { "name" : "<endpt name>",
    "org" : "current org <org>[:<site>]",
    "timezone" : <endpoint's timezone given as seconds offset from UTC - only given if available>,
    "summary": [
      {
        "ts": "<date of info for day 1>",
        "jobs_successful": <number of successful jobs completed on this day>,
```

```
        "jobs_aborted": <number of aborted jobs>,
        "jobs_failed": <number of failed jobs>,
        "img_total": <number of backup images saved during the day>,
        "total_size": <total size of all backup images in Bytes>,
      },
      "{...for day 2},
           ...
    ]
  },
  ... (one entry for every endpt if the request does not inlcude the <endpt uuid> parameter)
}
```

Field	Explanation of content displayed in the report
name	Displays the name of the endpoint in the report. **Note:** Each endpoint requires a unique call to include it in the report.
org	Displays the organization and optionally the site of the selected endpoint.
timezone	Displays the endpoint's timezone if available. The timezone appears as seconds offset from UTC.
ts	Displays the date of info for day 1.
jobs_successful	Displays the number of successful backup jobs completed for this endpoint on this day.
jobs_aborted	Displays the number of backup jobs aborted.
jobs_failed	Displays the number of failed backup jobs.
img_total	Displays the number of backup images saved during the day.
total_size	Displays the total space used by all backup images in bytes.

Current Endpoint Status Reporting: /api/reports/status/[<endpt uuid>/]

```
{ "<endpt uuid>":
  { "name" : "<endpt name>",
    "org" : "<org>[:<site>]",
    "tags" : [<list of tag strings>],
    "timezone" : <endpoint's timezone given as seconds offset from UTC - only given if available>,
    "status" : <current endpoint status: ok, warning (yellow), critical (red), offline(=endpoint not responding)>,
    "lost_contact": <minutes since appliance's last contact with the endpt, 0 if endpt is currently responding>,
    "machine_details" : {
        "last_start" : "<last boot time>",
        "ram" : <total MB>,
        "volumes" : [
            {
                "device" : "<device>",
                "label" : "<label>",
```

```
            "mountpoint" : "<mountpoint>",
            "size" : <bytes as MB>,
            "used" : "<bytes as MB>",
            "boot" : <true if the boot/system volume, false otherwise>
        },
        ...
    ]
},
"shadowprotect" : {
    "version" :
        {
            "name" : "<application name as installed>",
            "version" : "<version string>",
            "lang" : "<licensed language code>",
            "is_installed" : <true if installed>,
            "is_running" : <true if is currently running>,
            "serial" : "<license serial number>",
            < may contain the following fields depending on availability and license type >
            "is_msp" : <true if an MSP license>,
            "is_trial" : <true is a trial license>,
            "company" : "<name associated with license>",
            "days_to_expire" : <days left until license expires>,
            "expire_date" : "<date that license will expire>",
            "is_expired" : <true if license has expired>
        },
    "jobs" : [
      {
        "name: "<name of job1>",
        "policy: "<name of ShadowControl policy used to create the job, omitted if no policy>
        "status": "<current job status; queued, pauses, etc.>",
        "next_run": "<datetime of next scheduled backup>",
        "last_run": "<datetime of last backup>",
        "last_mode": "<type of last backup; full, incremental>"
        "last_result": "<result of last backup; success, failure>"
        "last_success": "<datetime of last successful backup>",
        "destination": "<path to destination>",
        "schedule": [
            {
                "time_range": [<start_time>, <end_time, if defined>],
                "interval": 1,
                "frequency": <"weekly" or "monthly">,
                "mode": <"full" or "incremental">,
                "offsets": [
                    <list of days: 0-7 if weekly, 1-31 if monthly, -1=last day of month>
                ],
```

```
            },
            ...
          ]
        },
        {
          "name: "<name of job2>",
          ...
        },
        ...
      ],
  },
  "imagemanager" : {
      "version" :
          {
              "name" : "<application name as installed>",
              "version" : "<version string>",
              "lang" : "<licensed language code>",
              "is_installed" : <true if installed>,
              "is_running" : <true if is currently running>,
              "serial" : "<license serial number>",
          },
      "folders" : [
        {
          "path": "<path to folder1>",
          "state": "<current state: active = 10, syncing = 20, offline = 30, failure = 40>",
          "file_count": <number of files in folder>,
          "folder_used_mb": <total folder size in MB>,
          "vol_total_mb": <filesystem total size in MB>,
          "vol_free_mb": <filesystem free space in MB>,
          "consolidation_errors": [
            {
              "code": "<error code, reserved for future use. currently empty>",
              "details": "<error as produced for display in IM>",
              "ts": "<datetime of failure>",
              "filename": "<name of the file that failed during consolidation>",
              "volume": "<volume name>",
            },
            ...
          ],
          "verify_errors": [
            {
              "code": "<error code, reserved for future use. currently empty>",
              "details": "<error as produced for display in IM>",
              "ts": "<datetime of failure>",
```

```
                "last_success": "<datetime fo last successful verification>",
                "volume": "<volume name>",
                "collapse": <type of collapse attempted>,
                "snap_ts": "<datetime of snapshot>",
                "chain": "<UUID of chain (can be used in IM Rest API to access more chain info)>",
                "file_size": <file size (in MB)>
              },
              ...
            ],
            "replication": [
              {
                name: "<replication job name>",
                status: <IM's description of current status>
                queued_files: <number of file waiting to be replicated>
              }
            ],
            "hsr": [
              {
                "uuid": "<uuid of hsr job>",
                "name": "<hsr name>",
                "state": "<summary state>",
                "jobs": [
                  {
                    "uuid": "<uuid of hsr target>",
                    "path": "<path of hsr target>",
                    "state": <target state>,
                    "status": "<string displayed by IM describing target's current status>",
                    "last_update": "<datetime of last HSR update for this target>",
                  },
                  ...
                ]
              }
            ]
          },
          ...
        ],
    },
  },
  ... (one entry for every endpt if the request does not inlcude the <endpt uuid> parameter)
}
"""
```

Field	Explanation of content displayed in the report

name	The name of the endpoint in the report. **Note:** Each endpoint requires a unique call to include it in the report.
org	The organization and optionally the site of the selected endpoint.
timezone	The endpoint's timezone if available. The timezone appears as seconds offset from UTC.
ts	The date of info for day 1.
jobs_successful	The number of successful backup jobs completed for this endpoint on this day.
jobs_aborted	The number of backup jobs aborted.
jobs_failed	The number of failed backup jobs.
img_total	The number of backup images saved during the day.
total_size	The total space used by all backup images in bytes.

ENDPOINT UUID SECTION

name	The endpoint's name
org	The name of the organzation and site (if assigned) for this endpoint
tags	Lists the tags defined for this endpoint
timezone	The endpoint's timezone given as seconds offset from UTC (if available)
status	The endpoint's current status (OK, Warning (yellow), Critical (red), or Offline (if the endpoint is not responding. Also called "Unknown".)
lost_contact	The minutes since the appliance's last contact with this endpoint. Shows "0" if the endpoint is currently responding.

MACHINE DETAILS SECTION

last_start	The last boot time for the endpoint
ram	The total memory on the endpoint in MB

VOLUMES SECTION

device	Device name
label	Volume label
mountpoint	The volume's mount point on the endpoint
size	Size of the volume in megabytes
used	The used space on the volume in megabytes
boot	Identifies if this is a boot volume (True if it is a boot volume, False if not).

SHADOWPROTECT VERSION SECTION

name	The application name as installed
version	The version string of the application
lang	The license's language code
is_installed	Indicates True if the application is installed

is_running	Indicates True if the application is currently running
serial	The license serial number
is_msp	Indicates True if the license is an MSP license
is_trial	Indicates True if the license is a trial license
company	The name associated with the license
days_to_expire	Number of days left until the license expires
expire_date	The date when that license will expire
is_expired	Inidcates True if the license has expired

JOBS SECTION

name	The name of job1
policy	The name of the ShadowControl policy used to create the job. (This is, omitted if there is no policy.)
status	The current job status: queued, paused, etc,
next_run	The date and time of the next scheduled backup.
last_run	The date and time of the last backup.
last_mode	The type of the last backup: Full or Incremental
last_result	The result of the last backup: Success or Failed
last_success	The date and time of the last successful backup
destination	The path to the job's destination

SCHEDULE SECTION

time_range	Gives the start and end time, if defined
interval	1 (Indicates every week or every month)
frequency	Weekly or monthly
mode	Full or Incremental
offsets	Provides a list of days: 0-7 if weekly, 1-31 if monthly, -1=last day of month

IMAGEMANAGER VERSION SECTION

name	The application name as installed
version	The application's version string
lang	The language code of the license
is_installed	Indicates True if installed
is_running	Indicates True if the application is currently running
serial	Gives the license's serial number

IMAGEMANAGER FOLDERS SECTION

path	Shows the path to folder1

state	Shows the current state: active = 10, syncing = 20, offline = 30, failure = 40
file_count	The number of files in the folder
folder_used_mb	The total size of the contents of the folder in megabytes
vol_total_mb	The volume's total size in megabytes
vol_free_mb	The volume's freespace in megabytes

IMAGEMANAGER CONSOLIDATION ERRORS SECTION

code	Reserved for future error code use (currently empty)
details	The error as shown in ImageManager
ts	THe date and time of the consolidation failure
filename	The name of the file that failed during consolidation
volume	The volume name where the failed file came from

VERIFY ERRORS SECTION

code	The would be an error code, however, it is currently reserved for future use and therefore is empty.
details	Shows the error as produced for display in ImageManager
ts	The data and time of the last failure
last_success	The date and time of the last successful verification
volume	The name of the source volume
collapse	The type of collapse attempted
snap_ts	The date and time of the snapshot
chain	The UUID of the backup chain (can be used in the IM Rest API to access more chain info).
file_size	The failed file's size in MB

REPLICATION SECTION

name	The replication job's name
status	ImageManager's description of the current status for replication.
queued_files	Shows the number of files waiting in the replication queue

HSR JOB SECTION

uuid	The uuid of the HSR job
name	The name of the HSR
state	The summary state
uuid	The uuid of the HSR target
path	The path to the HSR target
state	The current state of the target
status	The string shown by ImageManager describing the target's current status.

last_update	The date and time of the last HSR update to this target.

Report Formats

There are three different data sets available through the report API:

/api/reports/status	Description of endpoint client and the current status of its StorageCraft application
/api/reports/history	Detailed daily backup information: backup success/failures and backup image sizes
/api/reports/backups	Daily backup success rates for each endpoint (condensed subset of /reports/history)

Parameters

All three report APIs allow for the following parameters:

Parameter	Will Match
name=<string>	Any endpoint that starts with the given string (case insensitive)
org=<org>[:<site>]	Any endpoint in the given org/site

For /api/reports/history, ShadowControl also supports the following parameter:

days=<1..90>	Will return the last # of days (instead of all available, e.g. the default of 90)

For /api/reports/backups, ShadowControl supports these optional parameters:

csv=<any value>	Returns a CSV-formatted table (mime type 'text/csv') of the same information (Example with details shown below.) **Note:** "Any value" includes no value.
days=<1..90>	Will return the last # of days (instead of all available, e.g. the default of 90)
percent=<any value>	Will change the success ratios to percentages in the output i.e. "33%" instead of "1/3"

For example:

```
/api/reports/backups/?csv=&days=3
```

Backup Success Data Reporting: /api/reports/backups/[<endpt uuid>/]

Note: Unlike /reports/history, all dates for /reports/backups are in appliance local time.

JSON formatted data:

```
{
   "date" : "<current date>",
   "days" : <days in report>
```

```
  "rates" : [
   { "name" : "<endpt name>",
     "org" : "current org <org>[:<site>]",
     "success_rates": {
        "<date>": <success rate>,
          ... (one entry for each date with a backup attempt)
     },
   },
   ... (one entry for every endpt in the request)
  ]
}
```

CSV formatted data:

Endpoint, Organization, <latest date>, <previous day's date>, ... <earliest date>

<endpt name>, <org name>, <success rate>, <success rate>, ... <success rate>

... (one entry for each endpt, success rates are give as a numeric percentage or "--" if no backups were attempted)

Sample Output

	A	B	C	D	E	F	G	H	I	J	K	L
1	EndPoint	Organization	7/10/2015	7/9/2015	7/8/2015	7/7/2015	7/6/2015	7/5/2015	7/4/2015	7/3/2015	7/2/2015	7/1/2015
2												
3	DocTest-CentOS6	Desktops	5(5)	6(6)	4(4)	--	3(3)	6(6)	6(6)	6(6)	6(6)	4(4)
4												
5	doctest-ubuntu1204	Desktops	10(10)	10(10)	10(10)	1(1)	--	10(10)	10(10)	10(10)	10(10)	10(10)
6												
7	DocTest-Win08R2	Servers	11(11)	11(11)	11(11)	--	--	11(11)	11(11)	11(11)	11(11)	1(1)

Historical Data Reporting: /api/reports/history/[<endpt uuid>/]

Same as documented earlier.

Backup Success Data Reporting: /api/reports/backups/[<endpt uuid>/]

Note: Unlike /reports/history, with /reports/backups all dates will be in appliance local time

---

JSON formatted data:

```
{
   "date" : "<current date>",
   "days" : <days in report>
   "rates" : [
    { "name" : "<endpt name>",
      "org" : "current org <org>[:<site>]",
      "success_rates": {
          "<date>": <success rate as a numeric percentage>,
             ... (one entry for each date with a backup attempt)
      },
    },
    ... (one entry for every endpt in the request)
   ]
}
```

Sample Output


```
{
 "date": "2015-07-22",
 "rates": [
  {
   "success_rates": {
    "2015-07-18": "3(3)",
    "2015-07-20": "4(4)",
    "2015-07-23": "--",
    "2015-07-22": "5(5)",
    "2015-07-21": "6(6)",
    "2015-07-19": "--",
    "2015-07-16": "6(6)",
    "2015-07-17": "6(6)",
    "2015-07-14": "6(6)",
    "2015-07-15": "6(6)",
    "2015-07-12": "--",
    "2015-07-13": "4(4)"
   },
   "org": "Desktops",
   "name": "DocTest-CentOS6"
  },
  {
   "success_rates": {},
   "org": "BDR",
   "name": "DocTest-Host"
  },
  {
   "success_rates": {
    "2015-07-18": "--",
    "2015-07-20": "10(10)",
    "2015-07-22": "10(10)",
    "2015-07-21": "10(10)",
    "2015-07-19": "1(1)",
    "2015-07-16": "10(10)",
    "2015-07-17": "10(10)",
    "2015-07-14": "10(10)",
    "2015-07-15": "10(10)",
    "2015-07-12": "1(1)",
    "2015-07-13": "10(10)",
    "2015-07-11": "--"
   },
   "org": "Desktops",
   "name": "doctest-ubuntu1204"
  },
 ],
 "days": 10
}
```

Current Endpoint Status Reporting: /api/reports/status/[<endpt uuid>/]

Same as documented earlier.

Sample Output


```
{
  "fda01d6a59f545db98a8266ec4669293": {
    "status": "ok",
    "name": "DocTest-Win08R2",
    "tags": [],
    "machine_details": {
      "ram": 2047,
      "last_boot": "2015-07-22T00:15:48.860000",
      "volumes": [
        {
          "used": 27251,
          "os_vol": true,
          "boot": false,
          "label": "Srvr08R2",
          "readonly": false,
          "removable": false,
          "device": "\\\\?\\Volume{8cdffa3c-8a65-11e2-90b3-806e6f6e6963}\\",
          "mountpoint": "C:\\",
          "size": 81817
        },
        {
          "used": 28,
          "os_vol": false,
          "boot": false,
          "label": "System Reserved",
          "readonly": false,
          "removable": false,
          "device": "\\\\?\\Volume{8cdffa3b-8a65-11e2-90b3-806e6f6e6963}\\",
          "mountpoint": null,
          "size": 99
        }
      ]
    },
    "imagemanager": {
      "folders": []
    },
    "lost_contact": 0,
    "shadowprotect": {
      "version": {
        "lang": "en",
        "name": "ShadowProtect",
        "is_msp": true,
        "company": "Srvr08R2",
        "expire_date": "2015-08-13T00:00:00.000000",
        "is_running": true,
        "version": "5.2.3.37285",
        "days_to_expire": 23,
        "is_installed": true,
        "is_expired": false
      },
      "jobs": [
        {
          "status": "queued",
          "next_run": "2015-07-23T05:00:00.000000",
          "destination": "\\\\DocTest-Host\\BackupStore\\Srvr08R2",
          "name": "Srvr08R2",
          "failed_time": null,
          "schedule": [
            {
              "offsets": [
                1,
                2,
                3,
                4,
                5
              ],
```

```
          "interval": 1,
          "time_range": [
            "T08:00:00",
            "T18:00:00"
          ],
          "frequency": "continuous_vss",
          "mode": "incremental",
          "repeats": 60
        }
      ],
      "last_mode": "incremental",
      "last_run": "2015-07-22T15:00:00.000000",
      "last_result": "success",
      "last_success": "2015-07-22T15:00:00.000000",
      "last_size": 337408
    }
  ]
 },
 "timezone": 10800,
 "org": "Servers"
}
}
```