ShadowControl User Guide

StorageCraft Copyright Declaration

StorageCraft ImageManager, StorageCraft ShadowProtect, StorageCraft Cloud, and StorageCraft Cloud Services, together with any associated logos, are trademarks of StorageCraft Technology Corporation in the United States and elsewhere. All other brands and product names are or may be trademarks or registered trademarks of their respective owners.

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 the ShadowControl v3.7.0 appliance and endpoint agent.

User Guide Sections

This user guide includes the following major sections:

Additional Information

- 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.

Documentation Conventions

This symbol designates **Important** information that provides details on making a selection about the configuration and/or use of ShadowControl.

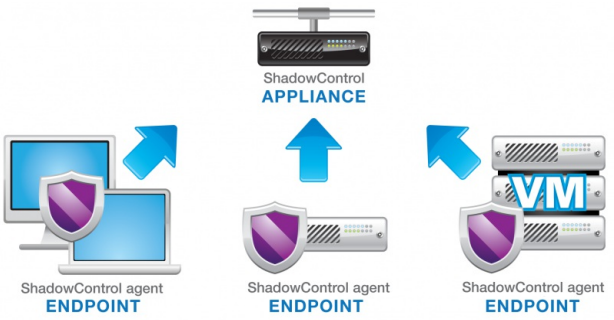
This symbol designates a **Warning** that highlights critical information affecting backup job performance or potential data loss.

1 Understanding ShadowControl

Welcome to StorageCraft® ShadowControl®—the central monitoring, management, and reporting console for the StorageCraft Recovery solution. ShadowControl has two main components:

- **ShadowControl Appliance:** A Linux-based server running as a VM or on dedicated hardware. It receives and collates status information from each agent-equipped endpoint and provides a centralized console for monitoring and managing the endpoint's ShadowProtect and ImageManager activities.
- **ShadowControl Agent:** A client installed at each endpoint. The ShadowControl agent sends status information to the ShadowControl appliance and queries the appliance regularly for tasks that it should perform.

© 2016 StorageCraft Technology Corporation



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

Administrators use the appliance's browser-based console to:

- Install and activate the ShadowControl agent and ShadowProtect software to selected endpoints
- Configure endpoint status rules and alert settings
- Configure SPX backup job policies
- Monitor ShadowProtect and ImageManager status for subscribed endpoints

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.

2 Installing the ShadowControl Appliance

The ShadowControl appliance installs on either a physical or virtual machine using a standard ISO file.

System Requirements

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

- The physical or virtual machine must support a 64-bit Ubuntu Linux v12.04 operating system. See the Ubuntu 12.04 Supported Hardware Page for detailed requirements for running Ubuntu Linux.
  Warning: While other hypervisors might work for test environments, StorageCraft has tested and approved ShadowControl for use only on Microsoft Hyper-V or VMware ESX/ESXi.
- StorageCraft recommends the following minimum requirements for a ShadowControl appliance:
  - 2GB RAM
  - 80GB disk space
  - Dual-core processor
    Important: The appliance's CPU and RAM requirements are determined primarily by the number of endpoints subscribed to the Appliance.
  - Active Internet connection for downloading appliance components during the install
  - An available IP address
  - Either Port 443 or 8443 available for appliance-to-endpoint communication
  - Port 5556 available 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 for email notifications
  - A Web browser. Use a current Web browser version for best results (Google Chrome, Firefox, Internet Explorer, etc.)

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 installing the Linux operating system.
5. On the *Initial Appliance Setup* dialog, select **Setup a new appliance**.
   Note: The Install process can take 15 minutes or more as it downloads Linux and StorageCraft packages to complete the install.
6. 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, proxy configuration, host name, and domain.
   - Specify and record the Access Code for this appliance. StorageCraft Support may later use this code to troubleshoot appliance issues.

When the ShadowControl appliance installation completes, it displays a login screen. All further configuration occurs through the

When the ShadowControl appliance installation completes, it displays a login screen. All further configuration occurs through the browser-based ShadowControl console. To access the console, open a browser to https://<*IPaddr or Host*> where <*IPaddr or Host*> is the IP address or host name of the newly installed ShadowControl appliance.

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

3 Installing the Endpoint Agent

The Endpoint Agent is a Windows- or Linux-based client installed on each monitored system. It gathers endpoint data, and performs tasks as directed by the ShadowControl appliance. You must install the endpoint agent software on each system you want to monitor and manage.

System Requirements

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

- The endpoint agent hardware and software requirements match those of ShadowProtect and ShadowProtect SPX.
- The endpoint agent supports ShadowProtect v5.0 and newer, and StorageCraft ImageManager v6.0.0 and newer.
- Endpoint agent communication with the ShadowControl appliance requires the following ports: 80, 443 or 8443, and 5556.

Note: While the endpoint agent can monitor systems without ShadowProtect or ImageManager installed, it provides only basic detail on those endpoints.

To install the ShadowControl agent on an endpoint and subscribe the endpoint to your ShadowControl appliance, use one of the following options:

- Install the endpoint agent automatically as part of a Push Install.
- Install the endpoint agent manually using the instructions available from the ShadowControl Console:
  - Browse to **ShadowControl > Appliance Settings > Endpoint Installation**.
  - From the Dashboard, click **EndPoint Installation Instructions**.

3.1 Windows Silent Install

You can install the Windows ShadowControl agent silently as part of a scripted install process or policy operation. Use the following commands to perform the silent install:

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

The last command subscribes the endpoint to the appliance. For more information, see Subscribing from the Command Line.

Important: The */restart* argument prevents the endpoint from executing an undesired reboot as part of the silent install. This can happen if the operating system or any application has previously set the *pending reboot flag*.

4 Subscribing an Endpoint

After installing the Endpoint Agent, you must subscribe the endpoint to a ShadowControl appliance in order for them to start communicating. How you subscribe an endpoint usually depends on how you installed the endpoint agent:

- Installed by Using a Push Install job: The endpoint subscribes automatically.
- (Windows or Linux) Installed by command-line (manual or scripted): Subscribe the endpoint using the ShadowControl CLI.
- (Windows only) Installed by running the .msi directly: Subscribe the endpoint using the ShadowControl Agent Settings.

Important: StorageCraft recommends using a Hostname rather than an IP address for subscribing endpoints to the appliance. This lets you change the appliance's IP address without having to resubscribe endpoints. To use a hostname, however, make sure you have properly configured DNS entries on the network so endpoints can identify the appliance by its host name.

© 2016 StorageCraft Technology Corporation

4.1 Subscribing from the Command Line

The ShadowControl agent provides the stccmd command-line utility for subscribing both Linux and Windows endpoints.

To subscribe an endpoint using the CLI:

1. Open a command shell on the endpoint that you want to subscribe to a ShadowControl appliance.
2. Run the following command to subscribe the endpoint, where *<address>* is the IP address or host name of the ShadowControl appliance.
   See CLI Subscribe Parameters below for the optional parameters supported by the command-line utility.

Windows `C:\Program Files (x86)\StorageCraft\CMD\stccmd subscribe [parameters] <address>`

Linux `/opt/StorageCraft/shadowcontrol-agent/bin/stccmd subscribe [parameters] <address>`

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

CLI Subscribe Parameters

The stccmd utility supports the following parameters for subscribe operations:

Note: All parameters are case-sensitive.

Option	Description
–U	Specifies the username of the ShadowControl appliance administrator subscribing this endpoint. Without providing valid appliance credentials, the ShadowControl appliance assigns the endpoint to the Default Organization.
–P	Specifies the password of the ShadowControl appliance administrator subscribing this endpoint. Used in conjunction with the -U option.
-T	Specifies a pre-defined subscription token that lets an endpoint subscribe without using appliance administrator credentials. For more information, see Creating Tokens.
–a	Instructs the endpoint and appliance to use the alternate port 8443 for HTTPS communications.
-f	Performs a "force" subscribe, meaning that if an endpoint it already subscribed it will unsubscribe it first, then subscribe it to the specified appliance.
-g	Specifies the endpoint's importance. Valid options include: *normal*, *semi*, or *critical*.
-h	Displays a list of the subscribe options. The stccmd utility provides Help information for each sub-command. For example, for help about the *subscribe* sub-command, type *stccmd subscribe -h.*
-m	Specifies the endpoint's System Type. Valid options include: *server*, *desktop*, *virtual*, and *laptop*.
–o	Specifies the Organization, and optionally the Site, where you want to subscribe this endpoint. To specify both an Organization and Site when subscribing and endpoint, use the syntax *Organization:Site*. For more information, see Using Organizations.
–t	Specifies a descriptive tag to associate with this endpoint. You can apply multiple tags when subscribing an endpoint by specifying the -t parameter multiple times. For more information, see Using Tags.

4.2 Subscribing with ShadowControl Agent Settings

The Windows MSI version of the endpoint agent installer includes a separate graphical utility, called ShadowControl Agent Settings, for subscribing the endpoint. You can use either this utility, or the command-line utility, to subscribe a Windows endpoint.

You can run the ShadowControl Agent Settings at any time after installing the endpoint agent. The utility is available at: *C:|Program Files (x86)|StorageCraft|CMD|ShadowControl-Gui.exe.*

To use ShadowControl Agent Settings:

1. Upon completing the installation of the endpoint agent on a Windows endpoint, select *Launch ShadowControl Subscription Application*, then click **Finish**.
2. In the ShadowControl Agent Settings dialog, provide the required information, then click **Subscribe**.

DNS Host Name/IP	Provide the hostname or IP address of the ShadowControl appliance where you want to subscribe this endpoint.
Use alternate port (8443)	(Optional) Select **Use alternate port (8443)** to have the endpoint use port 8443 for SSL communications with the appliance.
Machine Type	(Optional) 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 valid appliance administrator credentials to assign the endpoint to a specific Organization or Site as part of the subscription process. Without valid credentials, the appliance assigns the endpoint to the Default Organization **Note:** If you specify an Organization or Site that doesn't exist on the appliance, the appliance creates the specified Organization or Site automatically and assigns the endpoint to it.

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

5 Configuring the Appliance

Once installed, the ShadowControl appliance console provides access to its basic configuration settings. Some of these settings were configured during the installation process, but others must be configured post-installation.

You can access these settings from the ShadowControl Console by selecting **Configure ShadowControl** > **Appliance Settings**:

- System Info
- Network
- Security
- Mail Server
- Branding
- Product Registration

5.1 System Info

The System Info tab provides general information about the ShadowControl appliance, including:

Item	Description
Version	The software version for the ShadowControl appliance (not the version of Linux it runs on).
Release Notes	Link to the ShadowControl Readme. The readme provides granular detail about the most-recent release so you can determine if and when to update your appliance.
Access Code	The user-specified value (set during the appliance install) that StorageCraft Support can use under your direction to troubleshoot appliance issues. **Note:** The Access Code cannot be recovered, so protect it as you would a password.
RAM Usage	The amount of RAM currently in use by the ShadowControl appliance.
Disk Usage	The amount of disk space currently in use by the ShadowControl appliance.

CPU Usage	The current processor utilization on the ShadowControl appliance.
Load Average	The average processor work load over the last five minutes. For example, an average of 1.00 equates to 100% utilization of a single core; 2.00 equates to 100% utilization of two cores; etc.

Additionally, System Info lets you do the following:

Item	Description
Appliance Timezone	Sets the appliance timezone. This effectively sets the clock for the ShadowControl console. Click **Set Timezone** to accept changes.
Reboot Appliance	Reboots the appliance. For example, if an OS security update requires a reboot to complete the installation.
Shut Down Appliance	Gracefully shuts down the appliance.

Note: When a ShadowControl appliance update is available, System Info displays additional information and options so you can perform the appliance update. For more information, see Updating ShadowControl.

5.2 Network

The Network page lets you modify the following appliance configuration settings:

Warning: Modifying network configuration settings might prevent the appliance from communicating with endpoints.

Setting	Description
IP	Specifies the basic IP configuration for the ShadowControl appliance, including: IP address, net mask, default gateway, and DNS server address.
HTTP Proxy	(Optional) Specifies HTTP proxy settings for thost networks that use a proxy service. **Note:** During the appliance installation, you can configure only a single proxy configuration. Post-install, you can create separate proxy configurations for HTTP and HTTPS communications, if needed.
HTTPS Proxy	(Optional) Specifies HTTPS proxy settings for thost networks that use a proxy service.
Public Appliance Address	Specify the IP address to use when accessing the appliance from an external location. By default, ShadowControl uses the standard IP configuration for this purpose.

To modify Network settings:

From Appliance Settings > Network, modify any of the available settings as needed, then click **Save**.

5.3 Security

The Security tab lets you configure a custom SSL certificate issued by a recognized Certificate Authority (CA). If you don't have a custom SSL certificate, you can generate a Certificate Signing Request (CSR) directly from the appliance. You can then submit the CSR to the CA of your choice to request the needed certificate files.

To install a custom SSL certificate:

Browse to, and select, the files for your custom certificate, then click **Save**.

- Certificate File
- Key File
- (Optional) Intermediate Bundle File

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

Note: The certificate files generated by Microsoft IIS do not include a separate key file and will not import properly.

Important: ShadowControl cannot important certificate files that have a passphrase.

To generate a Certificate Signing Request (CSR):

Enter the required data into the fields, then click **Generate CSR**.

- Distinguished Name: The fully qualified domain name that you want to secure.
- Organization: The full, legal name of the entity requesting the certificate.
- (Optional) Organizational Unit: The department, or sub-group in the Organization that will use this certificate.
- (Optional) Country: The two-letter ISO code for the country where the Organization is located.
- (Optional) State: The full name (not abbreviation) of the State or Province where the Organization is located.
- (Optional) Locality: The full name (not abbreviation) of the city or town where the Organization is located.

ShadowControl generates the CSR using the data provided, and downloads the CSR to your local system through the Web browser.

Note: ShadowControl does not store the generated files on the appliance.

5.4 Mail Server

ShadowControl lets you configure the SMTP settings used to send email alerts and reports. By default, ShadowControl enables an internal SMTP server that is suitable for test environments. However, StorageCraft recommends using a separate SMTP server for production use of ShadowControl.

To configure mail server settings:

1. From the ShadowControl console, browse to **Appliance Settings** > **Mail Server**.
2. Select the type of SMTP support to use on the ShadowControl appliance, then click **Save**.
   Click **Send Test Email** to verify SMTP settings before saving them.

Use this appliance's built-in SMTP server: Use the default SMTP server running directly on the ShadowControl appliance.

From Address: The email address that appears in the email From field. (This does not have to be a valid address.)

Use another SMTP server: Provide the access information and credentials necessary to use an existing SMTP server.

Host Name or IP address	The external SMTP server's hostname or address.
Port	The port used for the SMTP protocol. By default, this is port 25.
Username	A valid username for the SMTP server.
Password	The user's password.
From address	The email address that appears in the email From field. (This does not have to be a valid address.)
Security	The SMTP server uses Transport Layer Security (TLS).

Don't use and SMTP server: Disables ShadowControl's email-based alerts and reports.

5.5 Branding

By default, ShadowControl displays a StorageCraft ShadowControl logo on each email alert and report. However, you can apply a custom logo to ShadowControl's email alerts and reports.

To enable custom branding:

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

5.6 Product Registration

During installation, you can register the ShadowControl appliance to enable support for the appliance. Once configured, you can modify the registration information as needed.

To modify registration information:

1. From the ShadowControl console, browse to Appliance Settings > Product Registration.
2. In the Product Registration page, provide the required information, then click **Save**.
   Note: All fields are required.

Field	Description
First name	The first name of the person responsible for the ShadowControl appliance.
Last Name	The last name of the person responsible for the ShadowControl appliance.
Company	The full name of the organization responsible for the ShadowControl appliance.
Email Address	The email address of the person responsible for the ShadowControl appliance.
Phone	The phone number of the person responsible for the ShadowControl appliance.
Street Address	The company's main office address.
City	The company's main office city.
State/Province	The company's main office state.
Postal Code	The company's main office postal code.

6 Configuring Users and Access

ShadowControl provides the following mechanisms to manage access to data and functionality:

- **User Roles:** Define specific permissions, and the scope of those permissions, to assign to users.
- **User Accounts:** Provide ShadowControl access credentials for a specific individual.
- **Tokens:** Provide access to certain administrative functions, subscribing endpoints or accessing data through the appliance REST API, without creating or sharing administrator credentials.

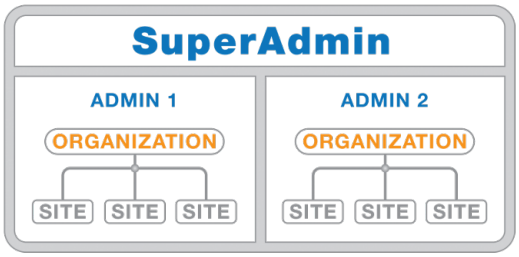
For example, Admin is a User Role in ShadowControl. You can assign the Admin role to a specific User Account, "Jane Doe", to grant Jane Doe Admin privileges in ShadowControl. However, if someone simply needs rights to subscribe endpoints to the appliance, you can create and share a Token with them, instead of granting that person full administrative access to the ShadowControl console.

- Creating User Roles
- Creating User Accounts
- Creating Tokens

6.1 Creating User Roles

ShadowControl provides the following types of user roles:

- **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.
- **Admin:** View and manage all endpoints in one or more Organizations and Sites. For more information about Organizations, see Organizing Endpoints.
- **Read-only:** View endpoint status in one or more Organizations and Sites.



To add a user role:

1. In the ShadowControl console, browse to **Configure ShadowControl** > **User Roles**.
2. From the User Roles page, click **Add Role**.
3. 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.

6.2 Creating User Accounts

A user account provides login credentials to the ShadowControl console for a specific person.

To add a user account:

1. From the ShadowControl console, browse to **Configure ShadowControl** > **User Accounts**.
2. In the User Accounts dialog, click **Add User Account**.
3. In the Add User Account dialog, provide the required information, then click Save.

Field	Description
Username	Specify a username.
Password	Specify a user password.
Confirm Password	Confirm the user password.
Email	Specify an email address for this user. ShadowControl sends this user's email notifications, including alerts and reports, to this address.
Status Notifications	Select the type of email alerts for this user to receive. Options include *All*, *Critical Only*, or *None*.
Notification Language	Select the language to use for this user's email notifications.
Assigned Roles	Select the User Role to assign to this user account. For more information, see Creating User Roles.

Once logged in, the *User Profile* menu provides the following user-related options:

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:** A user cannot change their assigned User Role.
Help	Displays the *ShadowControl User Guide*. (Requires Internet access.)
About	Displays the ShadowControl appliance version number, and provides links to the EULA, third-party licenses, and the StorageCraft feature request page.
Logout	Logs the user out of the appliance console.

6.3 Creating Tokens

ShadowControl tokens grant access to certain administrative functions, subscribing endpoints or accessing the appliance REST API, without creating or sharing administrator credentials.

To create a token:

1. From the ShadowControl console, browse to **Configure ShadowControl** > **Tokens**.
2. From the Tokens page, click **Create Token**.
3. 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 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:** Grants token access to all organizations on the ShadowControl appliance. ◦ **Restricted To:** Grants token access to only the selected organizations.

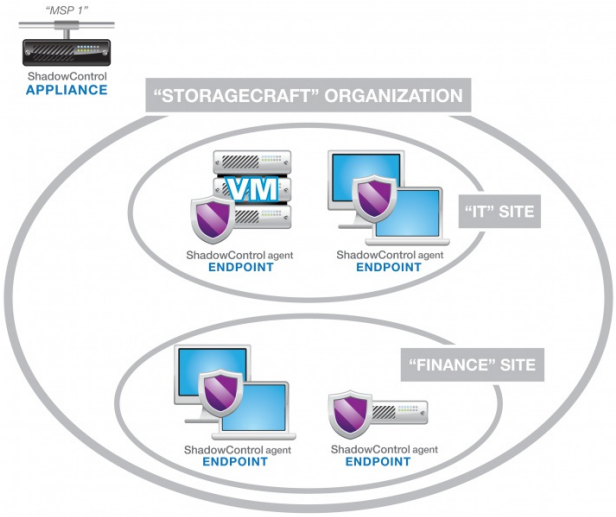
7 Organizing Endpoints

ShadowControl offers the following features for organizing ShadowControl endpoints:

- Using Organizations and Sites: The primary organizational unit on a ShadowControl appliance.
- Sites: An organizational sub-unit. Sites let administrators organize endpoints within an Organization.
- Using Tags: A descriptive word or phrase associated with a specific endpoint. Tags let administrators easily filter across Organizations and Sites to locate endpoints with a common characteristic.

7.1 Using Organizations and Sites

Administrators can create Organizations and Sites, then assign endpoints to them as needed, either during the subscription process or after. Organizations and Sites can be any logical grouping of endpoints, including geographical, organizational, and functional.



Organizations and Sites provide the following administrative advantages:

- Creates an easy way to filter the endpoint list in the ShadowControl console.
- Defines a reporting group so interested parties can receive alerts and reports for only that group of endpoints.
- Creates an administration point for SPX backup job policy, where each member endpoint automatically receive a default backup job configuration.

Organization and Site Names

When adding a new Organization or Site, select a name that identifies the shared characteristic of the endpoints in the group. For example:

Characteristic	Sample Names
Geographical	"East Campus", "Second Floor", "New York"
Organizational	"Accounting", "Development", "Sales"
Functional	"Windows 7", "Windows 2K", "Servers", "Laptops"

Default Organization

Every endpoint must be assigned to an Organization, so ShadowControl creates a single Default Organization for those endpoints not assigned to a user-defined Organization. While the Default Organization behaves like any other Organization, it is accessible only by a user with the Superadmin user role. Because of this, StorageCraft recommends assigning each endpoint to an appropriate Organization or Site rather than keep endpoints in the Default Organization.

Note: You cannot delete the Default Organization, even if you are not using it as part of your administrative structure.

Status Rule Policies

ShadowControl does not support applying status rule policies through an Organization or Site. Doing so provides more granular and flexible control over how ShadowControl monitors its subscribed endpoints. 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.

Creating Organizations and Sites

To create an organization:

1. From the ShadowControl console, browse to **Configure ShadowControl** > **Organizations**.
2. In the Organizations page, click **Add Organization**.
3. In the Add Organization page, provide the required information, then click **Save**.

Organization Name	Specify a name for the new Organization. Both Organizations and Sites support non-English characters, but they do not support HTML control characters such as "&" and "?".
Default SPX Policies	(Optional) Select a default SPX backup policy. ShadowControl assigns the default SPX backup policy to any endpoint that doesn't already have one. **Note:** To prevent the need to restart a backup image chain, ShadowControl does not automatically replace an existing backup policy when the endpoints moves from one Organization to another.
Contacts	(Optional) Provide contact information for non-administrators that you want to receive status information about the endpoints in the Organization. **Note:** This information is solely for your use. StorageCraft does not collect or use it in any way.
Send Reports	Specify if you want a contact to receive Organizational reports.
Send Alerts	Specify if you want a contact to receive email alerts for the endpoints in this Organization.
Notification Language	Specify the language used for reports and email alerts.

Creating a site:

1. From the ShadowControl console, browse to **Configure ShadowControl** > **Organizations**.
2. In the Organizations page, click **Add Site** on the Organization where you want to add a Site.
3. In the Add Site page, provide the required information, then click **Save**.
   Note: All information requested to create a Site is identical to that requested when creating an Organization (see above).

Assigning Endpoints to Organizations/Sites

Once created, you can assign an endpoint to an Organization or Site in the following ways:

- At subscribe: Automatically assign an endpoint to a specific Organization/Site when subscribing it to the ShadowControl appliance. See Subscribing an Endpoint. If you do not do this, ShadowControl automatically assigns the endpoint to the Default Organization.
- After subscribe: Manually assign an endpoint to a specific Organization/Site from the ShadowControl console.

To manually assign an endpoint:

1. From the ShadowControl console, browse to **Configure ShadowControl** > **Organizations**.
2. In the Organizations page, click **Assign Endpoints** on the Organization or Site where you want to assign the endpoint.
3. In the Assign Endpoints page, select the endpoints to assign, then click **Save**.
   Note: By default, ShadowControl displays only those endpoints assigned to the Default Organization. To assign an endpoint from another Organization, use the FIlter By dropdowns to modify the endpoint filter.

Filter	Description
Organization	Displays all endpoints currently assigned to the Organization selected from the second dropdown list. **Note:** This view includes all endpoints assigned to Sites within the selected Organization.
Tag	Displays all endpoints currently labeled with the Tag selected from the second dropdown list.
All endpoints	Displays all endpoints subscribed to this appliance.

7.2 Using Tags

Tags are second type of organization that you can apply to your endpoints. Tags consist of a key word or phrase that you can use to identify endpoints with a common characteristic. Tags create associations that span Organizations and Sites, and let you do the following:

- Search for endpoints by tag value.
- Filter endpoint lists by tag value.
- Sort the endpoint lists by tag value.

You can apply multiple tags to an endpoint for more flexible searching, filtering and sorting. For example, if you have a mail server in each of your organizations, you might assign an "Email" tag to each of those endpoints.You can then create a filtered view of just your Email servers to apply consistent status rule policies, or SPX backup policies.

Note: You can create tags that include non-English characters, but not HTML control characters such as "&" and "?".

To create a tag:

1. From the ShadowControl Console, browse to **Configure ShadowControl** > **Tags**.
2. In the Tags page, specify a tag value, then click **Create Tag**.
3. Click **Done** when finished creating tags.

Once created, click **Edit** to modify an existing tag. ShadowControl updates the name and preserves the link to all endpoints using this tag.

To assign a tag to an endpoint:

1. From the ShadowControl Console, click **Endpoints**.
2. From the Endpoint list, select an endpoint.
3. In the Endpoint Details page, click **Assign Tags**.
4. Check an existing tag and click **Done** to assign a tag.

8 Configuring Alerts

Status Rules are the heart of ShadowControl's monitoring. These rules set the thresholds that ShadowControl uses to alert administrators about a change in endpoint status. ShadowControl provides settings for:

- ShadowControl Rules
- ShadowProtect Rules
- ImageManager Rules
- ITSM Notifications

ShadowControl includes a default status rule policy with some rules active and others disabled, but ShadowControl administrators should modify the default settings to address their specific needs. For example, an administrator may create a unique status rule policy called "DB Server" that have rule thresholds appropriate for this type of endpoint. The adminstrator can then assign this policy to all database server endpoints to make sure each is monitored consistently.

Severity and State

ShadowControl alerts operate on the concept of *severity* and *state*:

- **Severity:** Defines how serious ShadowControl should consider a rule violation. Most status rules let the administrator define the severity of a given rule, either *Warning* or *Critical*. When an endpoint violates a rule, the severity determines the resulting state of the endpoint.
- **State:** Defines the current condition of the endpoint, based on the status rules, if any, it has violated. Endpoint state equals that of the most severe rule it has violated. Violating a Warning rule results in a "Warning" (Yellow) state, and violating a Critical rule results in a "Critical" (Red) state.

Important: ShadowControl automatically upgrades an endpoint's state once it passes a previously violated rule, as long as no other rule violation prevents this.

State-Based Alerts

ShadowControl bases its alerting on endpoint state, not rule violation; meaning that it sends alerts based on a change in the endpoint's state, not for each rule violation. For example, if an endpoint violates a Warning rule, it enters a Warning state and ShadowControl issues an alert. If the same endpoint then violates another Warning rule, ShadowControl does nothing. However, if the same endpoint then violates a Critical rule, it enters a Critical state and ShadowControl issues another alert.

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.

8.1 ShadowControl Rules

ShadowControl status rules include the following:

Rule	Description	Active by Default?

Endpoint Unresponsive	Triggers an alert when the endpoint agent has not recently communicated with the appliance.	Yes

8.2 ShadowProtect Rules

ShadowProtect status rules include the following:

Rule	Description	Active by default?	Rule Options
Failed Backup Job	Triggers an alert if the backup job remains in a failed state for the specified time period.	Yes	Minutes, Hours, Days
Backup Failure Rate	Triggers an alert if the endpoint exceeds the specified ratio of backup failures to backup attempts. This rule notifies the administrator when repeated, but not necessarily consecutive, backup failures occur.	No	Number of backup failures, Number of total backups
Last VSS Backup*	Triggers an alert if the backup occurs without using Microsoft's Volume Shadowcopy Service (VSS). VSS helps provide optimal backups for server applications such as SQL or Exchange. If a problem occurs with VSS, ShadowProtect falls back to a "crash-consistent" non-VSS backup, which might require additional recovery effort.	No	Minutes, Hours, Days
Paused Backup Job	Triggers an alert whenever a backup job remains paused for the set period of time.	Yes	Minutes, Hours, Days
Destination Disk Usage	Triggers an alert whenever the amount of used space in the image file destination drive exceeds the specified threshold.	Yes	Warning %, Critical %
License Status	Triggers a Warning alert when a system using a ShadowProtect MSP license is 5 days from expiration, and a Critical alert when the MSP license expires.	Yes	None
Service Status	Triggers an alert if the ShadowProtect service stops responding.	Yes	None

*Some endpoints might not support successful VSS backups. In this case, using the optional Last VSS Backup results in a continuous flow of alerts for non-VSS backups. To avoid this, make sure all endpoints of this type use a separate status rule policy with **Last VSS Backup** disabled.

8.3 ImageManager Rules

ImageManager status rules include the following:

Rule	Description	Active by default?	Rule Options
Managed Folder Disk Usage	Triggers an alert if the used space on the drive with the managed folders exceeds the set threshold.	Yes	Percent of disk space used
Verification Status	Triggers an alert if an image file fails its verification test. (This test confirms the fidelity of the file for restoration.)	Yes	Severity level
	Triggers an alert if an ImageManager consolidation job fails.	Yes	

Replication Queue Status	Triggers 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	Maximum number of files in the queue
License Status	Triggers a Warning alert when an ImageManager MSP subscription is 5 days from the license expiration, and a Critical alert when the MSP license expires.	Yes	N/A
Service Status	Triggers an alert if the ImageManager service stops responding.	Yes	Severity level

8.4 ITSM Notifications

IT Service Managment (ITSM) lets you specify an email address to send specialized alert messages designed for better integration with external ticketing systems or Remote Monitoring and Management (RMM) systems. Normally, ShadowControl sends alerts in a consolidated digest every ten minutes. ITSM notifications send each alert as a separate email with a fixed subject line so they can be easily parsed by an external system.

To enable ITSM notifications:

1. In the ShadowControl console, browse to **Appliance Settings** > **ITSM Notifications**.
2. Select **Enable IT service management notifications**.
3. Provide the required configuration details, then click **Save**.

Email Address:	The ITSM email address. **Note:** This should be an email address used exclusively by the external system.
Notification Language:	The desired language for the ITSM notifications.
Notification Type:	The type and frequency of ITSM notifications: **Send on endpoint status change:** Sends an alert only when a rule violation causes the endpoint status to change. For example, from Good to Warning, or Good to Critical. **Send separate notifications for each status rule violation:** Sends an alert for every rule violation, regardless of current endpoint status. This option results in more ITSM notifications.

9 Configuring Backup Job 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.

Before implementing SPX backup policies, consider the following:

- Once installed, you can manage policy-based backup jobs only through the ShadowControl appliance. Users cannot modify or control the backup job locally.
- You can assign only one SPX backup policy to an endpoint. For example, if you create one SPX backup policy for system volumes, and another for data volumes, you cannot assign both policies to the same endpoint.
  Note: If desired, you could create a local backup job to backup volumes not protected by an SPX backup policy job.
- When assigning SPX policies, ShadowControl never changes or replaces an existing backup job. This is true whether the existing job is locally managed, or 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.
- ShadowControl does not guarantee that a policy gets applied to a particular endpoint, but it will regularly retry any failed

policy assignments. Also, ShadowControl regularly checks the job configuration to make sure it matches current policy settings, and will automatically update the policy-based backup job as needed.

- Once configured on each endpoint, policy-based backup jobs run independently, so even the endpoint loses communication with the ShadowControl appliance, backup jobs continue to run.

Using an SPX Backup Policy involves the following tasks:

- Creating a Backup Store
- Creating an SPX Backup Policy
- Assigning an SPX Backup Policy
- Managing Policy-Based Jobs

9.1 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 a backup store path might be valid from the endpoint but not from the ShadowControl appliance.

To add a Backup Store:

1. From the ShadowControl Console, browse to **Manage Endpoints > Backup Stores**.
2. In the Backup Stores page, click **Add Backup Store**.
3. In the Add Backup Store page, provide the requested data, then click **Save**.
   Note: Both Windows and Linux can use the same backup store if you 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.

9.2 Creating an SPX Backup 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.

Note: ShadowControl can assign only one SPX backup policy to each SPX endpoint.

To add a new backup policy:

1. From the ShadowControl Console, 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, enter the desired backup job configuration, then click **Save**. ShadowControl organizes the backup job configuration into three tabs:
    - SPX Policy Settings
    - SPX Policy Schedule
    - SPX Policy Advanced Settings

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*.)

SPX Policy Settings

In the Settings tab, provide general information about the policy-based backup job.

Field	Description
Policy Name	Enter a descriptive name for the policy.
Protection Scheme	Select the type of volumes to back up: • All volumes (Default) • System Volumes only (volumes with an OS or a boot loader) • Data Volumes only (volumes without an OS or a boot loader)
Backup Store	Select a backup store to use with this SPX policy. For more information, see Creating a Backup Store.
Compression	Select the type of data compression to use: • *None*: Use no compression. • *Standard*: (Default) Typically compresses data by about 40%. • *Best*: Typically compresses data by about 50%. **Note:** Most contemporary processors can provide the *Best* compression level without impacting performance.
Encryption	Select the type of data encryption to use: • None • AES 128-bit • AES 256-bit (Default) **Note:** StorageCraft strongly recommends encrypting all backup files.

Password	(Conditional) Provide a password for encrypting the backup image files. **Warning:** Guard this encryption password carefully. StorageCraft cannot replace or recover a lost password.

SPX Policy Schedule

SPX backup scheduling is extremely flexible, supporting backup schedules of almost any configuration. For example, a single backup schedule could do all of the following:

- Backup every 30 minutes during business hours Monday-Friday.
- Backup every hour from 6PM to 12AM to protect online transactions.
- Backup every 15 minutes from 6PM to 10PM on first Friday of each month to make sure monthly sales data is protected.

In the Schedule tab, specify the type of backup schedule and the schedule specifics to use in the policy-based backup job.

Field	Description
Schedule Type	Select the type of backup schedule to use: **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. This schedule type requires ImageManager for image file chain management. **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/Month:** Select one or more days of the week or month that you want to run Full backups. **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/Month:** Select one or more days of the week or month that you want to run Incremental backups. **From** or **All Day:** Select the time span during the day to create Incremental backups. "All Day" specifies that SPX create Incremental backups 24 hours/day. **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.

SPX Policy Advanced Settings

The *Advanced* tab options provides granular control over SPX backup job operations. In most cases, the default settings are suitable. However, if you think you might need to adjust some of the Advanced Settings, see Advanced Tab, in the *ShadowProtect SPX User Guide*.

9.3 Assigning an SPX Backup Policy

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

- Directly, from **Manage endpoints > ShadowProtect SPX Policies**.
- Indirectly by applying a default SPX policy to a ShadowControl Organization.

To assign endpoints directly:

1. From the ShadowControl Console, browse to **Manage Endpoints** > **ShadowProtect SPX Policies**.
2. In the ShadowControl SPX Policies page, click **Manage Endpoints** for the policy where you want to assign endpoints.
3. In the Manage Endpoints page, select the endpoints to add to the policy.
   You can filter the endpoint list or search for specific endpoints.
   For information about the various icons in the endpoint list, see SPX Policy Endpoint List.
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**.
   This displays all endpoints with changing SPX policy assignments.
6. Click **Save**.

To assign endpoints through a default policy:

1. From the ShadowControl Console, browse to **Configure ShadowControl** > **Organizations**.
2. In the Organizations page, click **Edit** on the Organization or Site where you want to add a default SPX policy.
3. In the *Default SPX Policies* section, provide the required information, then click **Save**.

ShadowProtect SPX Backup Policy	Select the desired SPX backup policy from the dropdown list.
Start the first full backup of this job	Select the start time and interval during which the each endpoint begins its first full backup. **Note:** Randomized start times help prevents overwhelming the Backup Store with multiple full backups simultaneously.

Important: 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.

SPX Policy Endpoint List

The SPX Policy Endpoint list provides the following:

- 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.

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.

9.4 Managing Policy-based Jobs

When using SPX backup policy to automatically apply backup job configurations to endpoints, 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.

Removing an SPX Policy

When removing an SPX backup policy from an endpoint, you must decide what to do with the SPX backup job on the endpoint. You have two options:

- Convert the SPX policy backup job into a locally-managed one. Doing this preserves the existing backup chain, and returns full job management and control to the SPX console.
- Delete the job from the endpoint.
  Note: Deleting the job leaves the endpoint unprotected and ends the current backup chain. However, the existing backup image files remain in the Backup Store.

Changing the Assigned SPX Backup Policy

You can change the SPX backup policy assigned to an endpoint. Doing so ends the current backup chain and starts a new one with the new backup job. To do this:

1. Remove the current policy from the endpoint. When doing this, choose to delete the backup job from the endpoint.
2. Assign the endpoint to a new policy.

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

Deleting an SPX Backup Policy

Before deleting an SPX policy from the ShadowControl appliance, do the following:

- Remove the SPX backup policy as the default policy for all Organizations and Sites.
- Remove the SPX backup policy assignment from all endpoints. When you do this, you must either:
  - Convert the policy-based backup job into a locally-managed job.
  - Delete the policy-based backup job from the endpoint.

Unsubscribing an Endpoint

Unsubscribing and endpoint with an assigned SPX backup policy, whether from the appliance or from the endpoint, converts the policy-based backup job to a locally managed job.

Note: If the ShadowControl appliance crashes, either temporarily or permanently, a policy-based backup job will not spontaneously convert to a locally managed job. If necessary, you can force this conversion by unsubscribing the endpoint from the Command Line, or using the ShadowControl Agent Settings.

10 Using Push Install

ShadowControl Push Install lets you manage the installation and update of the following components of the StorageCraft Recovery Solution:

- ShadowProtect SPX or ShadowProtect 5
- ShadowControl Agent

Before configuring a Push Install job, be aware of the following:

- The ShadowControl agent is a prerequisite for all other component installations, so ShadowControl automatically installs the ShadowControl agent and subscribes the endpoint if needed.
  Note: ShadowControl installs the endpoint agent directly from the ShadowControl appliance.
- ShadowControl always installs the latest version of ShadowProtect or ShadowProtect SPX, downladed to the endpoint from StorageCraft's public download URL. Because of this, endpoints require internet access when using Push Install.
- ShadowControl requires that you activate all ShadowProtect installations using licenses stored in the License Pool, or generated through the MSP Portal.
- To protect limited appliance and network resources, Push Install is a linear operation; meaning that a push install job involving multiple endpoints proceeds one endpoint at a time.

ShadowControl Sources

The first step in a push install is to identify the candidate machines where you want to install or update StorageCraft software. To do this, ShadowControl uses Sources. A *Source* helps ShadowControl "discover" candidate machines and include them in a push install job. ShadowControl supports discovering endpoints through the following Sources:

ShadowControl Endpoint List: ShadowControl automatically creates a Source from the Endpoint List, which includes all currently subscribed endpoints. This Source is suitable for updating the ShadowControl endpoint agent, and installing or updating ShadowProtect.

Discovery by CSV: Create a new Source by importing a Comma Separated Value (CSV) file with information about endpoints that are not yet subscribed to ShadowControl. This Source is suitable for installing or updating the ShadowControl endpoint agent and ShadowProtect.

Discovery by System Center plugin: Create a new Source by linking the ShadowControl appliance to a Hyper-V hypervisor and importing information about virtual machines running on that hypervisor. This Source is suitable for installing or updating the ShadowControl endpoint agent and ShadowProtect.

Discovery by vCenter plugin: Create a new Source by linking the ShadowControl appliance to a VMware hypervisor and importing information about virtual machines running on that hypervisor. This Source is suitable for installing or updating the ShadowControl endpoint agent and ShadowProtect.

ShadowControl Push Install includes the following:

10.1 Using the License Pool

The ShadowControl License Pool verifies and stores non-MSP product keys for use in ShadowControl Push Install jobs. The License Pool validates any StorageCraft product key, even for products not currently available for push install. The License Pool however ignores any MSP product keys it encounters.

Note: ShadowControl provides direct integration to the MSP Portal for those partners that want to use MSP licenses for ShadowControl push install jobs.

To add product keys to the license pool:

1. Obtain one or more ShadowProtect product keys, including perpetual, OEM, and socket-based keys.
2. From the ShadowControl Console, browse to **Manage Endpoints** > **License Pool**.
3. Copy and paste the product keys into the validation pane, then click **Import Product Keys**.

ShadowControl validates the product keys, then updates the *License Pool* list with the following details:

Field	Description

Product Key	Displays the alphanumeric product key.
Product	Identifies what StorageCraft product the key supports (Server, Desktop, VM).
Assigned Organization	Displays the product key's assigned Organization. See Managing Product Keys below.
Language	Identifies the product key's language. (StorageCraft licensing uses distinct keys for different languages.)
Remaining Activations	Displays the remaining (unused) activations remain for this product key.
Total Activations	Displays the total number of activations available for this product key.

Managing Product Keys

The License Pool provides the following management features for product keys, once they have been imported:

- **Assign Keys to Organizations:** Select one or more keys, then click **Change Assigned Organization** to restrict the use of the keys to a specific Organization. Keys assigned to an Organization can be used to activate only endpoints assigned to the same organization, so administrators reserve product keys for use by specific customers or groups.
- **Remove Product Keys:** Select one or more keys, then click **Remove From Pool** to delete that product key from the ShadowControl License Pool.

10.2 Discovery with CSV

Using Plugins

To use either plugin for endpoint discovery, click **Discovery with vCenter Plug-in** or **Discovery with System Center Plug-In** on the *Push Install* page. If the selected plugin is not installed, ShadowControl begins the install process for that plugin. (Refer to the Discovery with the System Center Plug-in or Discovery with the vCenter Plug-in install instructions for details). With one or both plugins installed, either plugin can then report on installed VMs to ShadowControl.

To perform a push install to one or more endpoints from the plugins:

1. Select the relevant Source list on the *Push Install* page.
2. Select All or individual endpoitns from the list.
3. Click **Push Install**.

Refer to Using Push Install to continue.

Using a CSV Listing

ShadowControl can import a comma-separated value (CSV) file listing endpoints. The file should list each endpoint with three elements:

- Machine Name
- IP Address
- Platform (Linux or Windows)

For example:

```
Server-Win2012  192.168.1.101  windows
Server-CentOS6  192.168.1.102  linux
```

To import a CSV file:

1. Specify a source name. This simplifies keeping track of different CSV files.
2. Browse to the file's location.
3. Click **Create Source**.

ShadowControl imports the contents of the CSV file. To perform a push install of endpoints from this Source file:

1. Select the listed CSV Source on the *Push Install* page.

2. Select All or individual endpoitns from the list.
3. Click **Push Install**.

Refer to Using Push Install to continue.

Warning: Do not click *Discovery with CSV File* after scheduling any Push Install jobs for endpoints on that Source list. Doing so cancels any pending Push Install jobs for those endpoints. (This does not affect completed jobs or any currently in progress.

10.3 Discovery with the 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 System Center
- Perform Push Installs
- Using the Summary Dashboard

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 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.

System Center Requirements

Installing the ShadowControl plug-in on VMM requires:

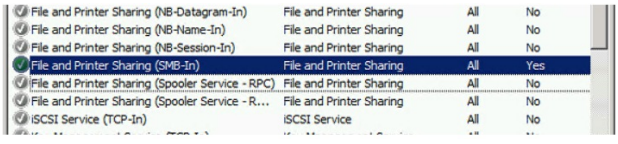
- Microsoft System Center 2012 R2
- Virtual Machine Manager active on System Center
- Administrator access to Microsoft System Center Virtual Machine Manager
- Virtual Guest Services installed on each client VM
- Active ShadowControl v2.5.0 or newer appliance

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

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:



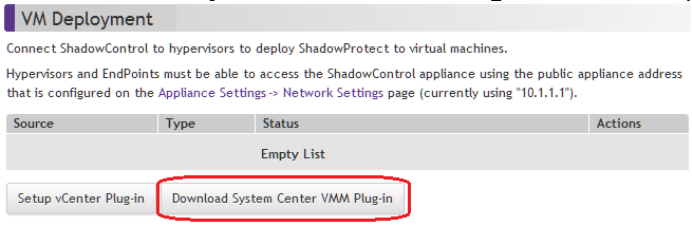
Otherwise, these endpoints will not appear in the VMM list.

Virtual Guest Services Requirement

Each VM client must have a *Virtual Guest Services* module installed to report basic information such as its computer name and IP addresses. These properties come from the operating system and not hardware, therefore System Center Virtual Machine Manager cannot determine these properties without this module. Administrators often require this basic information for VMs in VMM. The ShadowControl integration with System Center also requires the computer name and IP addresses. Refer to the Updating Integration Services with SCVMM MSDN article for details on installing this module.

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**.

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 Perform Push Installs section to perform these installs.

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:

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.

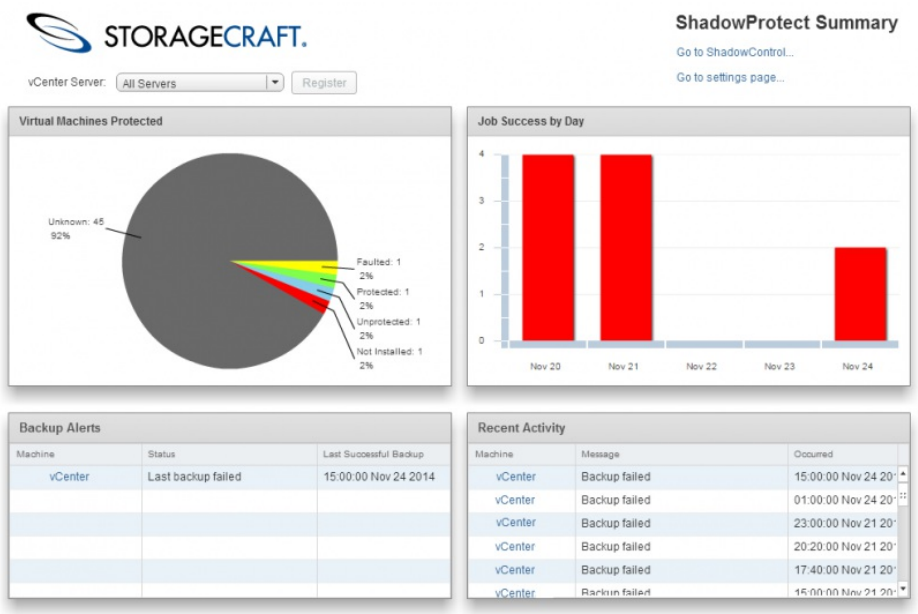
Select the *Licensing* tab to specify the product key(s) for the endpoint(s):

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.

Using the Summary Dashboard

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



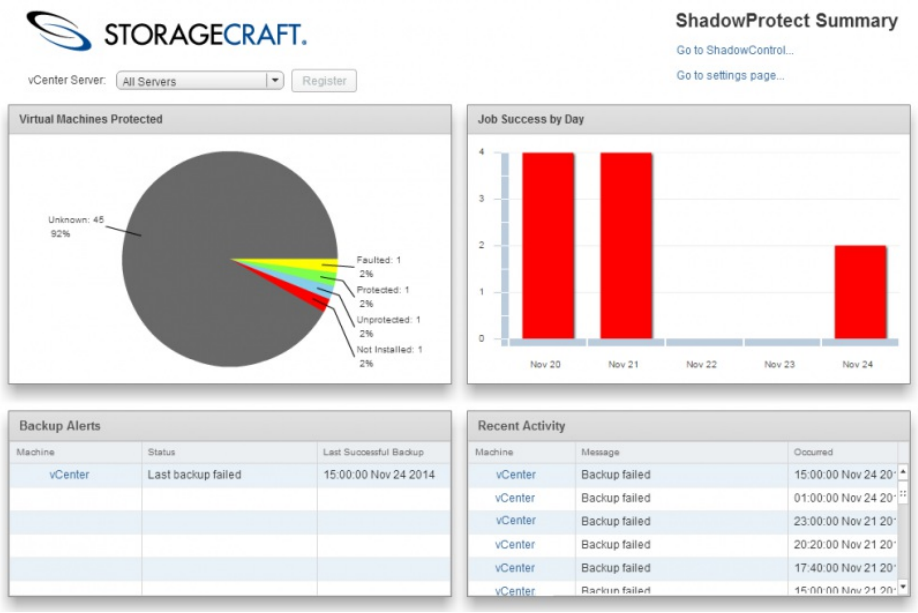
The dashboard includes five elements:

- 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:

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

- 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

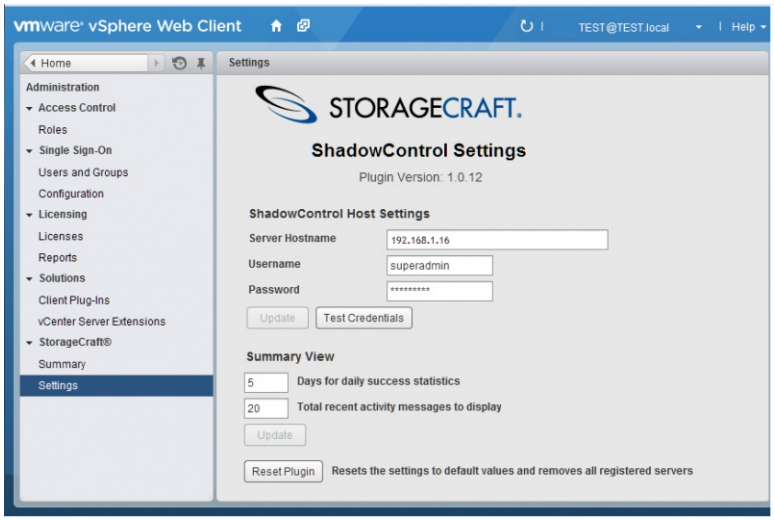
Use the **Resync** button to update information from the selected hosts.

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

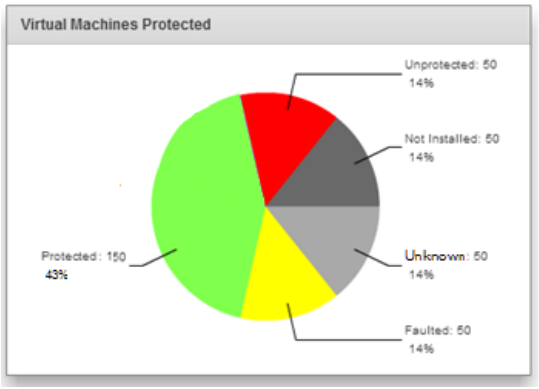
The Virtual Machines Protected chart by detault provides:

- 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:



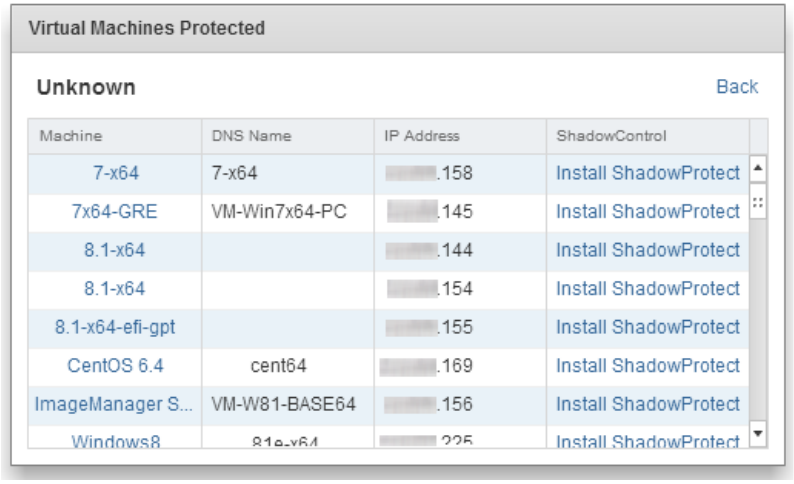
These include:

- **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:



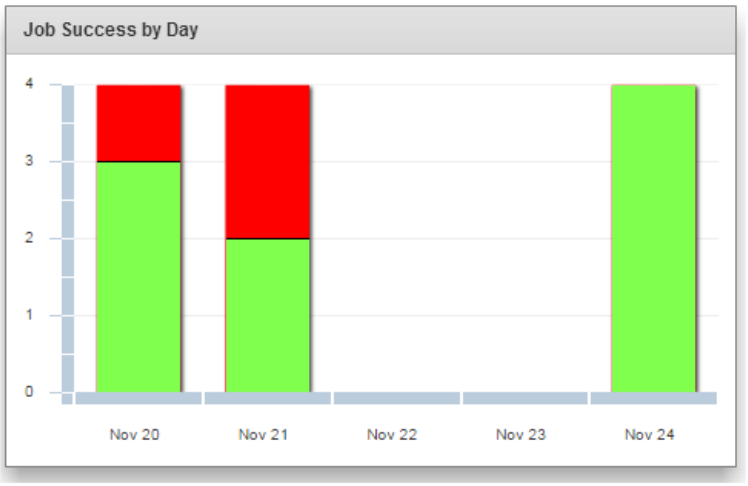
The list also shows whether ShadowProtect is installed (and with it, the ShadowControl agent).

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.

10.4 Discovery with the 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

⚠ **Important:** Discovery requires that hypervisors and endpoints have access to the ShadowControl appliance using the IP address configured in the appliance on the *Appliance Settings -> Network Settings* page.

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

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.

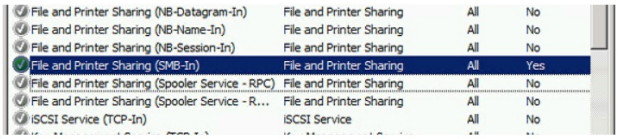
Note: If this deleted server returns, re-register the server via the plug-in. Otherwise, ShadowControl will not monitor that host server's virtual machines.

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:



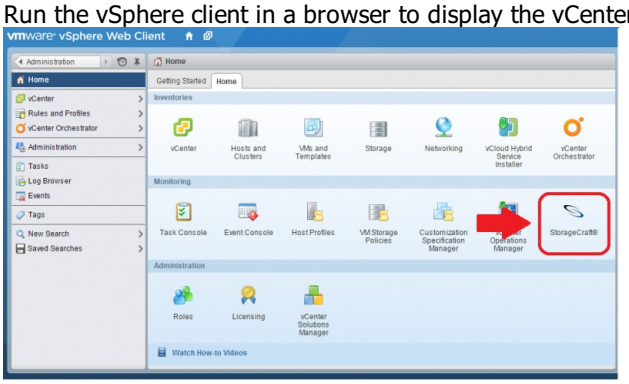
VMware Tools Requirement

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.

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.

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 Perform Push Installs section to perform these operations.

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:

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

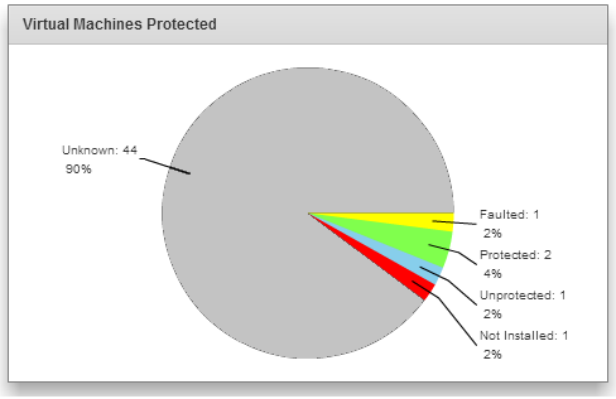
To perform a push install, first determine if the install is for:

- 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.

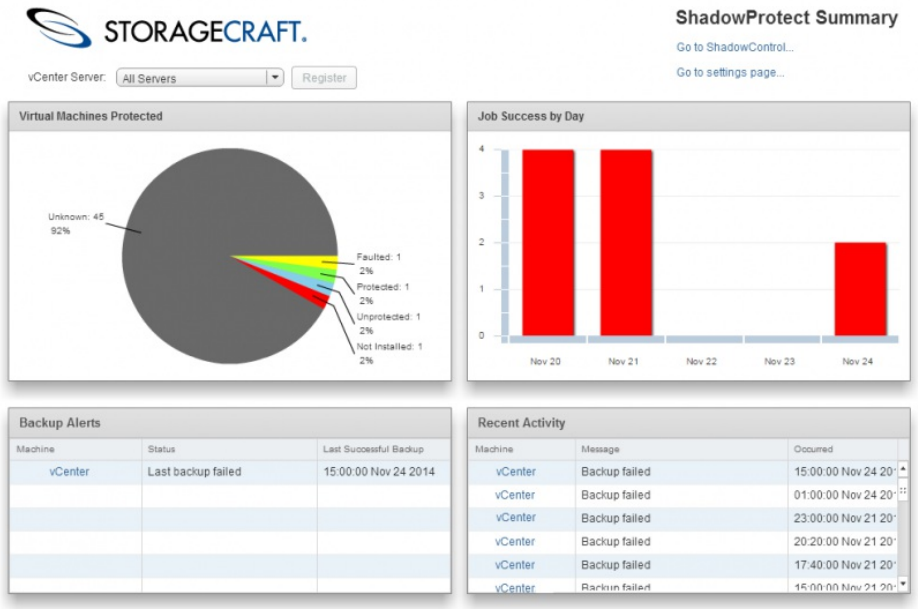
Select the *Licensing* tab to specify the product key(s) for the endpoint(s):

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.

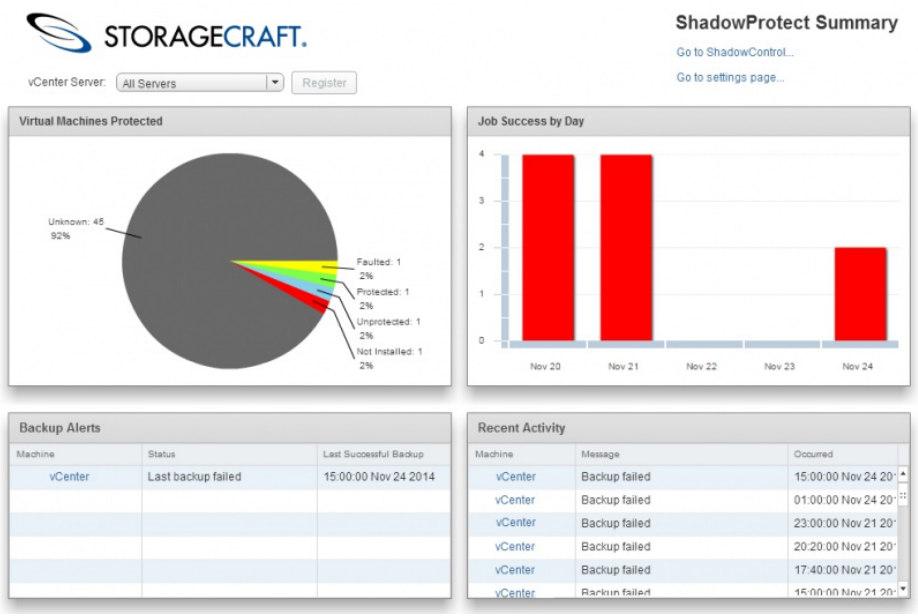
Using the Summary Dashboard

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



The dashboard includes five elements:

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.

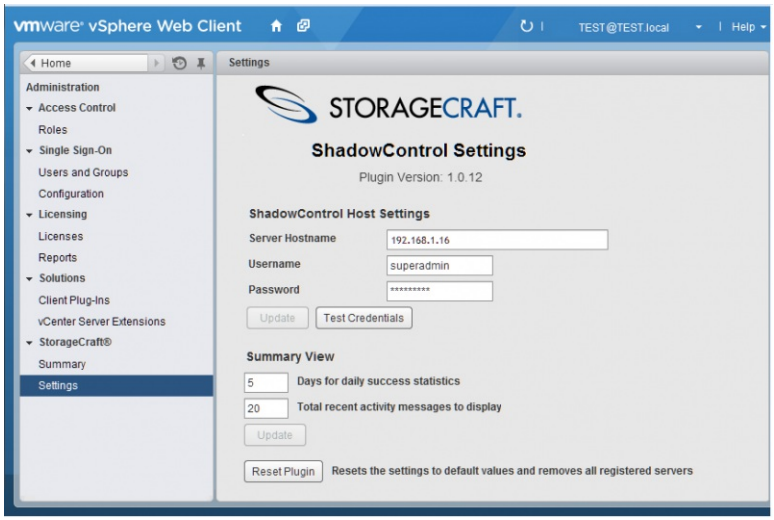
Go to ShadowControl

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.

© 2016 StorageCraft Technology Corporation



Virtual Machines Protected Chart

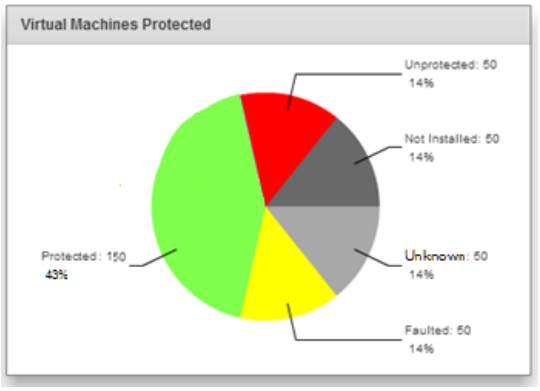
The Virtual Machines Protected chart by detault provides:

- 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:



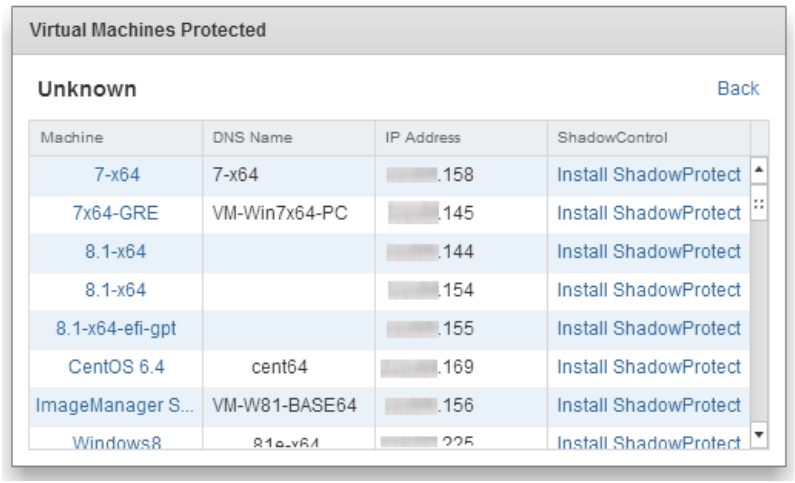
These include:

- **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:



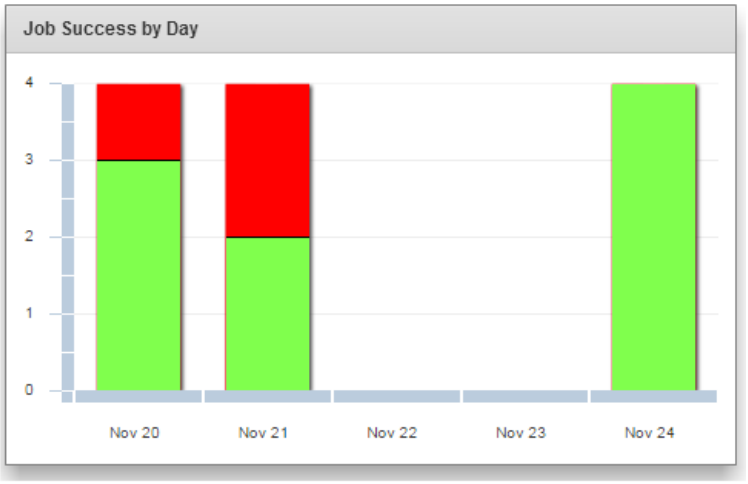
The list also shows whether ShadowProtect is installed (and with it, the ShadowControl agent).

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.

10.5 Configuring a Push Install Job

Once you have identified candidate machines and know how you will handle licensing for a push install job, you are ready to configure a Push Install job.

To perform a push install:

1. From the ShadowControl Console, browse to **Manage Endpoints** > **Push Install**.
2. From the Push Install page, click **Push Install** for the Source that you want to use for the push install.
   For more information about Sources, see Discovery with CSV, Discovery with the System Center Plug-in, and Discovery with the vCenter Plug-in.
3. From the **Select Action** dropdown list, select the type of push install job to perform.

Install ShadowProtect SPX	Installs the latest version of ShadowProtect SPX.
Install ShadowProtect	Installs the latest version of ShadowProtect SPX.
Install ShadowControl Agent	Installs the ShadowControl appliance's version of the endpoint agent.
Upgrade ShadowProtect SPX	Upgrades the endpoint to the latest version of ShadowProtect SPX.
Upgrade ShadowProtect	Upgrades the endpoint to the latest version of ShadowProtect.
Upgrade ShadowControl Agent	Upgrades the endpoint to the ShadowControl appliance's version of the endpoint agent.

4. Select the candidate machines to include in this push install job, then click **Push Install**.
   ShadowControl automatically filters the candidate list based on your choice in the Select Sction dropdown. Select **Filter Active Installations** to remove candidates included in another push install job that is already underway.
5. Continue with the Push Install based on the type of push install job you selected:
   - Finalizing an Install Job
   - Finalizing an Upgrade Job

Once you finalize the Push Install job, ShadowControl schedules the install or upgrade, and the Push Install page displays the status of the various job tasks on each candidate machine involved in the push install job. If an error occurs, the Push Install page identifies the error and provides a link to the push install log for troubleshooting purposes.

Finalizing an Install Job

When using Push Install, if you chose to install a new component on the candidate machines, you must provide the following information to finalize the install job:

Install Schedule: When to start the push install.
Machine Credentials: ShadowControl requires administrative credentials to be able to install new software on the candidate machines.
Licensing: ShadowControl must know where to get product keys to activate the newly installed component software.
ShadowControl-specific: Provide specific configuration related to Endpoint Agent installation.
SPX-specific: Provide specific configuration related to ShadowProtect SPX installation.
ShadowProtect-specific: Provide specific configuration related to ShadowProtect installation.

To finalize an install job:

In the Installing Component page, provide the required information, then click **Push Install**.

Install Schedule (Used for SPX or ShadowProtect installations)	
Start Delay	From the dropdown list, select a time delay before starting the push install job.
Windows Machine Credentials (Used for all component installations) **Note:** Required if candidate is not subscribed to the appliance.	
Domain	Specify the candidate machine's Windows domain.
Username	Specify an Administrator user on the candidate.
Password/Confirm	Provide and confirm the user's password.
Linux Machine Credentials (Used for SPX or ShadowControl installations) **Note:** Required if candidate is not subscribed to the appliance.	

SSH Port	Specify the port used to open a secure shell (SSH) session to the candidate.
Username	Specify an Administrator user on the candidate.
Password/Confirm	Provide and confirm the user's password.
ShadowControl	
Organization	Select a backup policy to apply to the endpoints from the dropdown list.
Licensing (Used for SPX or ShadowProtect installations) **Note:** Push Install uses the same licensing information for all endpoints.	
Product Keys	Select the source of the product keys to use from the dropdown list. By default, Push Install gets product keys from the License Pool. Select **Activate using StorageCraft MSP Portal product keys** to use MSP product keys.
Customer Name	(Conditional) Specify a Customer name to use when activating with the License Pool.
Organization	(Conditional) Specify an Organization (Company) name to use when activating with the License Pool.
MSP Portal	(Conditional) Select the MSP Portal, either North America or European, where you normally log in.
MSP Portal Username	(Conditional) Specify your MSP Portal login username.
MSP Portal Password	(Conditional) Provide your MSP Portal login password.
Account	(Conditional) Select the MSP Portal account where you want to generate the MSP product keys for this push install job.
Site	(Conditional) Select the MSP Portal site where you want to generate the MSP product keys for this push install job.
ShadowProtect SPX	
Backup Policy	From the dropdown list, select the SPX Backup Policy to assign to these endpoints.
ShadowProtect	
Installer Language	From the dropdown list, select the ShadowProtect install language to use for this push install job.
Job Type	From the dropdown list, select the backup job configuration to apply during this push install job.
End User License Agreement (Used for all component installations)	
EULA	Check the box to indicate agreement with the product EULA. Use the link to view the agreement.

Finalizing an Upgrade Job

When using Push Install, if you chose to upgrade an existing component on the endpoint, you must provide the following information to finalize the job:

Install Schedule: When to start the push install.
SPX-specific: Provide specific configuration related to ShadowProtect SPX installation.
ShadowProtect-specific: Provide specific configuration related to ShadowProtect installation.

To finalize an upgrade job:

In the Installing Component page, provide the required information, then click **Upgrade**.

Install Schedule (Used for SPX or ShadowProtect upgrades)	
Start Delay	From the dropdown list, select a time delay before starting the push install job.
End User License Agreement (Used for all component upgrades)	
EULA	Check the box to indicate agreement with the product EULA. Use the link to view the agreement.

11 Reporting

An important part of what the ShadowControl appliance does is create informative reports for both internal and external parties interested in the status of the StorageCraft Recovery Solution. ShadowControl offers the following reports:

- ShadowControl Standard Report: A standard report, generated nightly, that ShadowControl can email to those interested in receiving it.
- ShadowProtect Backups Report: An on-demand report that displays
- ShadowProtect Licensing Report: An on-demand report that lists all ShadowProtect licenses currently in use, by Organization.

Additionally, ShadowControl offers a REST API that provides programmatic access to its endpoint status and report data:

- The ShadowControl Report API

11.1 ShadowControl Standard Report

The standard ShadowControl report is the typical report that administrators and users view to get a snapshot of the health of their StorageCraft Recovery Solution. ShadowControl offers variations of the Standard report based on the following:

Audience: ShadowControl varies the scope of the Standard report based on the report recipient:

- Superadmin: Includes data all Organizations and all endpoints on this appliance, and sends the report to each Superadmin user on this appliance.
  Note: Superadmins can generate a current report on-demand by browsing to **Configure ShadowControl** > **Reports**, then clicking **View Report**.
- Administrator: Includes data for those endpoints in Organizations assigned to each administrator, and sends the report to each Admin user on this appliance.
- Organization (Contact): Includes data only for those endpoints in each organization, and sends the report to each Organization contact designated to receive reports.

The Standard report can have up to four sections, depending on on the options selected when the report was scheduled (see Scheduling the Standard Report):

Endpoint Summary	Always included in the report, the Summary includes the following detail similar to that in the appliance Dashboard: • A chart of endpoint status (Critical, Warning, Good or Offline) by product (ShadowProtect, ImageManager, ShadowControl). • A list of recent notifications by product (ShadowProtect, ImageManager, ShadowControl).
ShadowProtect Endpoint Details	(Optional) Displays, by Organization, a list of ShadowProtect endpoints with the following ShadowProtect information: • Backup Job Summary: Last backup time and status (success/fail), backup success rate for the report time period, and when their last backup occurred. • Storage Summary: Last backup size, Average space used / day for the report time. • Status: Current state of the endpoint, based upon ShadowControl alerts (Green=Good, Yellow=Warning, Red=Critical, Gray=Unresponsive).

ImageManager Endpoint Details	(Optional) Displays, by Organization, a list of ImageManager endpoints with the following ImageManager information: • Job Summary: List of Replication and HSR jobs running on this endpoint. • Folder Summary: Number of managed folders, total number of image files, Total storage used by image files. • Status: Current state of the endpoint, based upon ShadowControl alerts (Green=Good, Yellow=Warning, Red=Critical, Gray=Unresponsive).
Storage Statistics	Displays a set of daily averages for the amount of disk space used by backup image files. ShadowControl 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.

Scheduling the Standard Report

ShadowControl supports automatically sending its standard report to the desired recipients. Once scheduled, the ShadowControl appliance automatically generates its standard report at 12:30am (0030 hours), based on the appliance clock, and distributes it to those selected to receive it.

To schedule reports:

1. From the ShadowControl Console, browse to **Configure ShadowControl** > **Reports**.
2. In the Reports page, click **Schedule Reports**.
3. In the Report Scheduling page, make your desired selections, then click **Save Schedule**.

Send Reports	Select when to send a report to this recipient. Options include: *Never*, *Daily*, *Weekly*, and *Monthly*.
ShadowProtect Details	Includes information about each ShadowProtect endpoint in the report for this recipient.
ImageManager Details	Includes information about each ImageManager endpoint in the report for this recipient.
Storage	Includes information about storage utilization and projected growth related to ShadowProtect backup image files. **Note:** ShadowControl bases estimates solely on backup image file size, and does not account for ImageManager consolidation over time, if applicable.

11.2 ShadowProtect Backups Report

The ShadowProtect Backups report is an on-demand report that displays a daily "backup success" ratio for each endpoint subscribed to this appliance, grouped by Organization. Specifically, it includes the following data:

Endpoint Name	The first column of the report contains the names of each endpoint subscribed to this endpoint. They are organized alphabetically, first by Organization, then by Machine Name.
Date	The first row of the report contains the dates contained in the report, in the format *mmm dd*. You can configure the number of days in the report.
Date Status	The Backups report represents each day with a color, representing the status of backups for that day. Green = Good, Yellow = Warning, Red = Critical.
Successful Backups	The successful backups for the day, represented as a percentage of the attempted backups, or as an absolute value.

Attempted Backups	(Optional) The total backups attempted each day.

To generate the ShadowProtect Backups report:

1. From the ShadowControl Console, browse to Configure **ShadowControl** > **Reports**.
2. In the Reports page, click **ShadowProtect Backups**.
3. In the ShadowProtect Backups page, click **Edit report settings**.
4. In the Backups Report Settings page, configure the report view, then click **Save**.
   The following settings let you configure how the report displays its data:

Number of days to display	(Default: 30) Specify the number of days to display in the report. Supported values: 1-90.
Threshold for warning	(Default: 66) Specify a percentage of successful daily backups below which the report displays the day in a Warning (yellow) state. Supported values: 1-99.
Threshold for critical	(Default: 33) Specify a percentage of successful daily backups below which the report displays the day in a Critical (red) state. Supported values: 1-99.
Format successful backups as	(Default: a percentage of attempts) Select how you want the report to represent the number of successful backups for each day. Supported values include: *a percentage of attempts*, or *the number of successes*.
Show total backup attempts for each day	(Default: selected) Displays the total attempted backups for each day in addition to the number of successful backups.

11.3 ShadowProtect Licensing Report

The ShadowProtect License report is an on-demand report that displays details about ShadowProtect product key usage for the endpoints subscribed to this ShadowControl appliance. Specifically, it includes the following details:

Organization	The report groups ShadowProtect endpoints by Organization.
License	The ShadowProtect product key assigned to this endpoint.
Endpoint	The endpoint's machine name. Within each Organization, ShadowControl sorts the endpoint list alphabetically, by machine name.

To generate the ShadowProtect Licensing report:

1. From the ShadowControl Console, browse to Configure **ShadowControl** > **Reports**.
2. In the Reports page, click **ShadowProtect Licensing**.

11.4 ShadowControl Report API

Using the ShadowControl Report API requires experience with the following:

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

Important: StorageCraft does not support any of these processes and provides this content solely on an AS-IS basis.

The ShadowControl Report API lets third-parties request endpoint report data from the ShadowControl appliance for external use. Report data is available in two ways:

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

When ShadowControl receives a request, it then:

- Filters the data based on the access credentials provided in the request.
- Sorts these results by *organization* then by each *site* in that organization.

Note: StorageCraft recommends using Tokens to provide access to the ShadowControl Report API. For more information, see Creating Tokens. For example, a curl request for a status report data might look like the following:

```
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: 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)
}
```

Element	Explanation
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"
}
}
```


12 Protecting Appliance Data

To protect its data and configuration, and simplify recovery in the event of an appliance failure, ShadowControl provides a backup mechanism that preserves the following types of data: appliance configuration, endpoint subscriptions, custom SSL certificates, custom branding, and endpoint backup history.

Note: The Appliance time zone and network settings must be reconfigured manually when recovering the appliance.

This backup provides a recovery path in the event of 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. Because of this, StorageCraft recommends the following best practices for appliance backup:

- Schedule a recurring backup at least weekly.
- Run a manual backup before and after updating the ShadowControl appliance.

Note: ShadowControl keeps only the most-recent backup. When creating a new backup, the appliance overwrites the previous backup, if any.

To schedule a recurring appliance backup:

1. From the ShadowControl Console, browse to **Configure ShadowControl** > **Applicance Settings** > **Appliance Backup**.
2. In the Appliance Backup page, specify, and confirm, a password for encrypting the backup archive file, then click **Save**.
   ⚠ **Warning:** This password cannot be recovered if lost. Make sure to guard it carefully.
3. In the Backup Schedule and Export section, provide the required information, then click **Schedule Backup**.

Backup Store	Select where you want to store the backup archive file. You can store the archive locally on the appliance (not recommended), or have the appliance automatically copy the archive file out to a configured Backup Store.
Backup Frequency	Select how often to save the backup. Options include: *Daily*, *Once a week*, *Once every two weeks*, or *Once a month*.
Backup Day	(Conditional) Select a day to perform the backup if you select any backup frequency other than *Daily*.
Backup Time of Day	Select the time of day to create the backup archive file.

⚠ **Caution**: The backup process might take a few minutes. Do not refresh the screen (press <F5>) during the export progress. Doing so restarts the export.

To run a manual backup:

1. From the ShadowControl Console, browse to **Configure ShadowControl** > **Applicance Settings** > **Appliance Backup**.
2. In the Appliance Backup page, click **Export Database File**.
   ShadowControl creates the file and does the following:
   - Saves a copy locally on the appliance.
   - Sends a copy to the requesting web browser.
   - Exports the file to the defined Backup Store (if there is one).

Caution: ShadowControl erases any other existing appliance backup file created on the same day as the manual one.

12.1 Restoring an Appliance

With a backup archive file, you can quickly recover a ShadowControl appliance to its state at the time the backup was taken.

Note: You cannot restore an appliance archive file to an existing appliance. The restore process is available only as part of a new appliance install.

To restore an appliance database:

1. Install a new ShadowControl appliance, as described in Installing the ShadowControl Appliance.
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. Enter the encryption password, then click **Save**.
   The setup program restores the appliance's configuration.
5. Follow the remaining steps in the setup wizard to complete the restore.

13 Updating ShadowControl

The ShadowControl appliance automatically detects when StorageCraft releases a ShadowControl update. When this happens, the Dashboard displays a banner notification that an update is available. A similar notice also appears on the *Appliance Settings* page, along with information necessary to update the appliance and endpoints. There are two types of ShadowControl updates:

- **Appliance-only:** Denoted by a change to the third number in the product version; for example, 2.5.0 to 2.5.1. These updates do not require a change to the endpoint.
- **Full update:** 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 update to both the appliance and the endpoint agent.

Important: StorageCraft strongly recommends exporting a copy of the appliance database before starting an update. For more information, see Protecting Appliance Data.

To update an appliance:

1. In the System Info page, click **Update Appliance**.
2. From the Schedule Appliance Update dialog, select the size of the delay before the appliance upgrade starts, then click **Schedule Update**.
   Options range from *Start Immediately* to *Delay 12 hours*.

Following an appliance update, if the new appliance requires an updated endpoint agent, the Dashboard displays the following message, where *n* is the number of endpoints eligible for udpate:

```
Endpoint Updates Available: ShadowControl Agent update required for n endpoints.
```

To update endpoint agents:

1. From the ShadowControl Console, open the Dashboard view.
2. Click the link in the Endpoint Updates Available message.
3. In the Push Install page, select one or more of the eligible endpoints to update.
   You can update all endpoints, or perform the update in multiple batches, depending upon your needs.
4. Click **Push Install**.

13.1 Additional Update Options

There are a few other ShadowControl update options that you should be aware of:

Appliance OS Update

The ShadowControl appliance regularly checks for, and applies, security updates to the underlying Linux operating system. At times, those updates require the operating system to restart to complete the update. When this occurs, the Dashboard displays the following message:

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

When you see this message, you should reboot the appliance as soon as practical. To do so, browse to **Configure ShadowControl** > **Appliance Settings**, then click **Reboot Appliance** to complete the install.

Note: For your convenience, the Appliance Reboot Required message includes a link that takes you straight to the Appliance Settings page.

Manual Endpoint Updates

If necessary, you can manually update the ShadowControl endpoint agent. As with an automated update, the manual endpoint update retains the appliance subscription and settings.

To manually update Windows endpoints:

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.

To manually update Red Hat/CentOS Linux endpoints:

1. Update the contents of your Linux product repositories.
2. When prompted
3. sudo yum update

ubuntu: sudo apt-get update