Symantec™ Protection Center 2.0 Security Guide

Symantec™ Protection Center Security Guide

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Contents

Chapter 1

Introducing Protection Center security

This chapter includes the following topics:

About this document

This document provides a high-level description of the security features that are built in to Symantec Protection Center. It is intended to help you evaluate and implement Protection Center by answering general questions that you may have regarding the security of Protection Center and its suitability for use in your organization. This document does not provide detailed information about the design and implementation of Protection Center features, nor does it describe how Protection Center functions in any particular scenario.

Symantec Protection Center security

Protection Center is the hub of security information and infrastructure in your organization. It performs actions and remediation, reports on important security issues within your organization and allows access to all other integrated products.

Protecting the integrity of the Protection Center infrastructure, its communications, and all its data is critical. Protection Center is designed to be highly secure and resistant to attack, and consequently includes many features that safeguard your working environment.

Protection Center is shipped as an appliance. Protection Center runs on the Windows Server 2008 R2 Core Server operating system, which is a stripped down version of Windows 2008 that has no Windows Explorer shell installed. This operating system has a reduced set of features installed to trim the memory footprint and increase the performance of the server. To keep the attack surface small, only the minimum set of applications and processes are running, and the minimum number of ports are used.

Table 1-1 describes the Protection Center security features.

Table 1-1 Protection Center security features

Category	Description
Protection Center infrastructure security	The Protection Center infrastructure is locked down to make it highly resistant to attack and is constantly monitored for any changes in security. See "About Protection Center infrastructure security" on page 7.
Product integration security	All products that integrate with Protection Center must be registered. Every product is authenticated to ensure that only legitimate products are integrated with Protection Center. Registration is the mechanism by which Protection Center establishes a trust relationship with an integrated product and secures communication channels. Protection Center also supports single sign-on (SSO) which enables the Protection Center console to display pages from an integrated product's user interface without requiring the user to sign in to each individual product. See "About Protection Center product integration security" on page 14.
Communications security	All communications between Protection Center and integrated products are authenticated and encrypted for security. Product registration uses basic authentication, but all other Protection Center web services use SSL with mutual certificate authentication (two-way SSL). See "Protection Center communications security" on page 18.
User security	Protection Center has a permission-based security mechanism that it uses to secure access to its data, reports, and console pages. See "Protection Center user security" on page 25.

About Protection Center infrastructure security

Protection Center runs in a secure, dedicated environment as a "zero maintenance" appliance. To achieve this, the Protection Center infrastructure is locked down and monitored.

Locking down the Protection Center infrastructure provides the following benefits:

- Simplified management
  Protection Center takes care of operating system updates, software updates, and security management in your environment.
- Enhanced security
  Protection Center maintains policy and controls configuration of all your products. Its locked-down infrastructure prevents changes that may compromise the security of the system.
- Reliable performance and upgrades
  Protection Center has dedicated access to all of its resources, such as web server, database, memory, hard disks, and CPU. Only the essential services run on Protection Center and no unnecessary functions are available. Unauthorized users cannot change, move, or install software that could negatively impact Protection Center performance or the ability to upgrade it.

Security events such as authentication failures, lockouts, account creation/deletion, permission modifications, and group membership changes are logged in the Protection Center system log and shown in the System Logs report. The Protection Center administrator is notified of each event.

Protection Center infrastructure lockdown framework

The Protection Center infrastructure is locked down, which minimizes its attack surface and makes it highly resistant to attack. The lockdown framework checks the Protection Center infrastructure every 30 minutes to identify any changes in security. The framework also provides detection and correction of lockdown breaches throughout the Protection Center life cycle. In addition, it provides comprehensive logging for all lockdown items.

Table 1-2 describes the main features of the Protection Center infrastructure lockdown framework.

Table 1-2 Protection Center infrastructure lockdown framework

Lockdown feature	Description
Prevention	The Protection Center infrastructure is locked down to minimize its attack surface. The system is actively monitored to ensure that it remains locked down. Any non-compliant changes are prevented or reverted.
Detection	Protection Center is actively monitored: each lockdown item, or configuration aspect, is checked to detect any possible non-compliance with the lockdown state. For example, if a port is opened that should not be opened, Protection Center will lock down the system by closing the port. The lockdown state of each item is either: ■ The system complies with the lockdown requirement. ■ The system is in breach of the lockdown requirement. The detection process is independent for each lockdown item: there are no dependencies on other lockdown items.
Correction	Actions are taken to bring Protection Center from a non-compliant state into the locked-down state. This is maintained through the entire life cycle of Protection Center, including installation, upgrades, Windows updates and patching, and administrative changes made as part of normal Protection Center operations. Correction is necessary whenever anything alters the state of Protection Center. In some cases the correction may require a disruption to normal Protection Center operations, such as a restart of services (such as IIS) or a system reboot. Any such disruption remains under the control of the Protection Center administrator to allow grouping of disruptions or administrator input. A disruptive operation cannot occur without the approval of the Protection Center administrator.

Protection Center infrastructure lockdown items

The items that are locked down in the Protection Center infrastructure (lockdown items) can be organized into logical groups. Each lockdown item also has a category that identifies the major Protection Center functionality component that the item relates to:

Operating system
: Protection Center runs on the Windows Server 2008 R2 Core Server operating system. This is a stripped down version of Windows 2008 that has no Windows Explorer shell installed.

Database
: Protection Center uses SQL Server 2008 R2 Express.

Web server
: Protection Center uses Internet Information Server 7.0.

The logical groups of lockdown items are as follows:

- Accounts and authentication
  See "Accounts and authentication" on page 9.
- Components
  See "Protection Center components" on page 10.
- Ports and protocols
  See "Ports and protocols" on page 11.
- Security updates
  See "Security updates" on page 11.
- SQL Server
  See "SQL Server" on page 11.
- Windows Server
  See "Windows Server" on page 13.

Note: Although many lockdown items are identified above, it is possible that future releases of Protection Center may include new lockdown items.

Accounts and authentication

Table 1-3 describes the lockdown items that relate to accounts and authentication.

Table 1-3 Accounts and authentication lockdown items

Lockdown Item	Category	Description
Dedicated administrator account	OS	Protection Center has a non-deletable dedicated administrator account. The Protection Center administrator must set a cryptographically strong password during the installation process. The password must contain at least eight characters and include at least three of the following: ■ Uppercase alphabetic characters (A through Z) ■ Alphabetic Unicode characters that are not categorized as uppercase (A through Z) or lowercase (a through z) ■ Numeric characters (0 through 9) ■ Non-alphanumeric characters (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Table 1-3 Accounts and authentication lockdown items *(continued)*

Lockdown Item	Category	Description
Default Windows accounts	OS	The default Windows Administrator account and the Guest account have been disabled. SQL Server authentication logging is enabled. Log information goes to the SQL Server Log, which also goes to the Windows Application Event Log. To view the log information, the administrator can open CRTTools from the Protection Center control panel (this requires a signed powershell script). The administrator can then read, search, and parse the Windows Event Log for SQL authentication information.
Passwords	OS	Passwords for user accounts that are created on Protection Center must have a minimum password length of eight characters. This minimum length does not apply to passwords for LDAP or Microsoft Active Directory accounts. LAN Manager hash values are not stored. The security option **Network Security: Do not store LAN Manager hash value on next password change** is enabled. For more information, see *Network Security: Do not store LAN Manager hash value on next password change*, updated January 21, 2005, on the Microsoft Web site at the following URL: http://technet.microsoft.com/en-us/library/cc757582(WS.10).aspx
Windows authentication	SQL	The SQL Server is configured for Mixed-mode authentication. However, Protection Center uses Windows authentication only. The database can only be accessed by the local host. It is not externally available.
Guest connections	SQL	Database guest connections have been revoked: the Guest account has been dropped from all databases except “master” and “tempdb”.

Protection Center components

Table 1-4 describes the lockdown items that relate to Protection Center components.

Table 1-4 Components lockdown items

Lockdown Item	Category	Description
Windows services whitelist	OS/SQL/IIS	Protection Center uses a whitelist to start only the required Windows services. See “Windows services whitelist” on page 29.

Table 1-4 Components lockdown items *(continued)*

Lockdown Item	Category	Description
Restrict service log on	SQL/IIS	The SQL Server services and IIS run as the Network Service account. The Network Service account is unchanged from the default. For more information, refer to the Windows Server 2008 help.
Web applications	IIS	All non-Protection Center web applications have restricted access controlled by the IP filtering feature of IIS. Whitelisted web pages and files are available from any IP address; all other Web pages and files are available only to Protection Center IP addresses.

Ports and protocols

Table 1-5 describes the lockdown items that relate to ports and protocols.

Table 1-5 Ports and protocols lockdown items

Lockdown Item	Category	Description
Port whitelist	OS/SQL/IIS	The only open ports in Protection Center are port 80 and port 443. See "Firewall settings required to support Protection Center" on page 35.

Security updates

Table 1-6 describes the lockdown items that relate to security updates.

Table 1-6 Security updates lockdown items

Lockdown Item	Category	Description
Windows updates	OS/SQL/IIS	All necessary security updates and patches are applied to Protection Center. Symantec LiveUpdate is used to download, distribute, and schedule the most up-to-date patches. The downloads occur automatically at midnight, but the administrator manually schedules the Windows updates. See "Windows components whitelist" on page 32.

SQL Server

Table 1-7 describes the lockdown items that relate to SQL Server.

Table 1-7 SQL Server lockdown items

Lockdown Item	Category	Description
Sp_configure options	SQL	The SQL Server options that can only be enabled and disabled using sp_configure have been secured. The following sp_configure options have been set to the specified values: ■ Ad Hoc Distributed Queries=0; ■ Agent XPs=0 ■ clr enabled=0 ■ cross db ownership chaining=0 ■ Database Mail XPs=0 ■ max server memory (MB)=2147483647 ■ Ole Automation Procedures=0 ■ remote access=0 ■ remote admin connections=0 ■ Replication XPs=0 ■ xp_cmdshell=0 ■ SQL Mail XPs=0 For more information on the sp_configure options, see *Setting Server Configuration Options* on the Microsoft Web site at the following URL: http://msdn.microsoft.com/en-us/library/ms189631.aspx
Extended stored procedures	SQL	Extended stored procedures are locked down so that a non-administrator user cannot execute any of them. The lockdown framework monitors them (checking at 30-minute intervals) and disables anything new.
DB enumeration	SQL	DB enumeration is disabled to prevent a Public user from issuing a command to enumerate the names of all of the databases that exist on the SQL Server.

Table 1-7 SQL Server lockdown items *(continued)*

Lockdown Item	Category	Description
Database	SQL	The Protection Center database is locked down as follows: ■ All permissions are moved from the Public role to a new role to prevent automatic assignment. ■ All permissions are revoked from the Public database role for each database. All permissions from the Public role are assigned to the newly created FormerPublic role. This enables the Protection Center administrator to add a user to the FormerPublic role if the administrator wants the user to have all of these permissions. The Protection Center administrator has full control of the assignment.
SQL service permissions	SQL	SQL Server service permissions are restricted. The MSSQLSERVER service runs as Network Service.

Windows Server

Table 1-8 describes the lockdown items that relate to Windows Server.

Table 1-8 Windows Server lockdown items

Lockdown Item	Category	Description
Domain membership	OS	Protection Center is designed to be used as an appliance and is managed internally, rather than being designed to be managed through group policy.
File sharing	OS	The default network file shares are disabled on all drives. This includes the ADMIN$ share.
Execute permissions	OS	Execution of Server Manager commands (and other system modifying tools) is restricted to the Protection Center administrator account. The administrator account is the only Windows account in Protection Center. In addition, the system lockdown feature checks the system every 30 minutes, and compares the state of the system to the whitelist. If the state of Protection Center is inconsistent with what the whitelist allows, the situation is rectified immediately.
Unused services	OS	Unused services (browser, agent, and full-text filtering) are disabled. See "Windows services whitelist" on page 29.

About Protection Center product integration security

To help ensure a secure environment, Protection Center forms trust relationships with integrated products. Registration is the mechanism by which Protection Center establishes a trust relationship with an integrated product and secures communication channels.

All products that integrate with Protection Center must be registered. Every product is authenticated to ensure that only legitimate products are integrated with Protection Center.

See "About supported product detection and selection" on page 14.

See "About Protection Center integrated product registration" on page 15.

See "Registering a product with Protection Center" on page 15.

See "About registration web service security" on page 17.

About supported product detection and selection

When Protection Center deployment is complete, the Protection Center administrator can start the registration process for all supported products.

To start registering a product with Protection Center, the Protection Center administrator can do either of the following:

Manually specify the product to register.	The Protection Center administrator needs to manually enter the fully qualified domain name (FQDN) or IP address of the product server that they want to register. If the product uses a non-default port for registration, the administrator also needs to specify the appropriate port number.
Run a network discovery scan.	The Protection Center administrator can run a network discovery scan to detect all supported products on a specified range of IP addresses. Protection Center retrieves the appropriate product information from each supported product instance that it discovers. The Protection Center administrator can then pick the product instance to register.

In order for a supported product to be discoverable by a network discovery scan, the product must be listening on the appropriate registration port. Firewalls need to be configured accordingly so that the registration port on the product is accessible from Protection Center.

See "Protection Center data security" on page 26.

For Symantec Endpoint Protection, a Symantec Endpoint Protection domain is counted as a separate product installation. A Symantec Endpoint Protection

domain becomes a Protection Center tenant. For multi-domain Symantec Endpoint Protection deployments, all of the domains can be connected to the same Protection Center installation, and each domain is a separate Protection Center tenant.

About Protection Center integrated product registration

When the Protection Center administrator has selected the product to register, the administrator needs to specify the appropriate product credentials. The administrator performs this task in the Protection Center console. All communication between Protection Center and the product is encrypted and mutually authenticated.

Each supported product includes credentials that can be used for authentication with Protection Center. The account used has rights to register the product with Protection Center. The appropriate product credentials must be obtained by the Protection Center administrator to use when registering the product with Protection Center.

The Protection Center registration process verifies the supplied credentials. The registration process fails if the credentials cannot be verified. Note that for some products, only certain credentials are suitable. For example, Symantec Endpoint Protection requires System Administrator credentials.

Protection Center calls the appropriate web service on the supported product and passes on the Protection Center certificate. Registration credentials are passed using basic authentication over SSL. The supported product returns a certificate which is stored in the Protection Center certificate store. This registers an instance of an integrated product with Protection Center.

See "About registration web service security" on page 17.

Each tenant hosted by the integrated product must be registered as a unique instance. The integrated product certificate is stored by Protection Center and used for all subsequent communication with this instance.

The integrated product verifies the credentials and then stores the Protection Center certificates securely.

Registering a product with Protection Center

The registration process involves the exchange of certificates that are then used to establish trust communications between Protection Center and the supported product. Both Symantec and non-Symantec products can be integrated with Protection Center.

When Protection Center is initially installed, it generates a new certificate (called the Protection Center certificate). This is an X.509 certificate that is self-signed.

It contains within its subject the FQDN of the server upon which Protection Center has been installed. Protection Center stores this certificate. When a supported product is registered, the Protection Center certificate is passed as part of the registration process and is stored by the integrated product.

Table 1-9 describes the process of integrating a product with Protection Center.

Table 1-9 Process for registering a product

Phase	Description
Get the product registration credentials.	Each supported product must have a set of credentials (an account) that Protection Center can use to authenticate with the product. The Protection Center administrator must obtain the appropriate product credentials to use when registering the product with Protection Center. See "About Protection Center integrated product registration" on page 15.
Select the product to register.	When Protection Center deployment is complete, the Protection Center administrator can start the registration process for all supported products. Protection Center refers to the product Protection Application Component file (PAC) that is preinstalled on Protection Center. The product PAC provides the integration information that is required by Protection Center, such as the default registration port and details of the data feeds that the product supports. See "About supported product detection and selection" on page 14.
Enter the product credentials.	For each supported product that the administrator wants to register, the administrator must enter the appropriate product credentials. The administrator performs this task in the Protection Center console. All communication between Protection Center and the product is encrypted and mutually authenticated. See "About Protection Center integrated product registration" on page 15.
Protection Center registers the product instance.	Protection Center calls the appropriate web service on the supported product and passes on the Protection Center certificate. The supported product returns a certificate which is stored in Protection Center. See "About Protection Center integrated product registration" on page 15.
The product registers Protection Center.	The supported product verifies the credentials and then stores the Protection Center certificate securely. It also returns the supported product's certificate to Protection Center. See "About Protection Center integrated product registration" on page 15.

Table 1-9 Process for registering a product *(continued)*

Phase	Description
Protection Center registers product users.	The Protection Center administrator associates Protection Center users with product users that have rights to administer the integrated product. When the Protection Center administrator sets up Protection Center user accounts, the administrator can match each product account with the appropriate Protection Center user. The intended scenario is that each Protection Center user account is matched to a unique product account. However, this 1:1 correspondence is not enforced in Protection Center. See "Protection Center user security" on page 25.
Protection Center imports product data.	Protection Center refers to the product PAC for details of the data feeds that the product supports. The PAC may also provide custom permissions and UI components to Protection Center. Immediately after registration, Protection Center pulls all users, computers, incidents, and events from the product's data feeds into Protection Center. The integrated product provides the requested data to Protection Center. At scheduled intervals, data synchronization occurs to pick up any changes to the data since the last time the data feed was queried. The returned data is processed and stored in Protection Center, with summary data in the database and detailed data in the archive files. See "Protection Center communications security" on page 18.

About registration web service security

Unlike other web service calls made by Protection Center to products, the registration web service call uses basic authentication over SSL. The username and password used for these calls is not stored by Protection Center and is used only for the current registration session.

All subsequent calls between Protection Center and the integrated product use mutual certificate authentication via SSL. The client certificate supplied by Protection Center contains the user name in the subject field. Cryptographically, this provides a much stronger authentication mechanism than user names and passwords and does not require the periodic changing of passwords in accordance with most organizations' password policies.

Protection Center communications security

Protection Center provides secure communications with integrated products. Protection Center authenticates any interaction with integrated products, and all communication between Protection Center and integrated products is encrypted.

See "About integrated product authentication" on page 19.

See "About Protection Center action security" on page 20.

See "Protection Center communications security features" on page 20.

See "About Protection Center web service security" on page 22.

See "Firewall settings required to support Protection Center" on page 35.

Table 1-10 Protection Center communications security

Component	Protocols and ports used
LiveUpdate	The LiveUpdate client uses HTTP (port 80) and/or FTP (port 21) to query for update list and download updates.
DeepSight	Protection Center uses HTTPS to connect to the Symantec IT-hosted server. The SSL Certificate subject is also validated. The Protection Center DeepSight server can be accessed at spc-deepsight.symantec.com:7891. The DeepSight server provides additional information about viruses and other security threats. This information is shown on the Protection Center dashboard and included in the Specific Malware report.
Windows updates	The Windows Update service uses HTTP (port 80) and HTTPS (port 443) to connect to the Microsoft Web Site.
Web services	The Discovery, Registration and Data Feed web services use HTTPS (client SSL). Port 443 is used by default, but integrated products can specify custom ports.
Workflow	Protection Center calls the integrated product web services through HTTPS. The Workflow URLs are exposed through HTTP, but require a Protection Center signed SSO ticket.
Telemetry data	Protection Center uses HTTP to connect to the Symantec IT server.

About integrated product authentication

Protection Center authenticates with integrated products by mutual certificate authentication. As a general rule, Protection Center calls integrated product web services, but not vice-versa. Protection Center provides the Protection Center certificate or the appropriate user certificate. (Each Protection Center user is issued a certificate by the Protection Center certificate authority. The common name of the certificate is issued to the name of the user.) Integrated products use their server authentication certificates, either self-signed or customer-supplied.

See "Protection Center certificates" on page 22.

When Protection Center calls an integrated product using a web service, both parties ensure the following:

Encryption	The call must be encrypted (using TLS/SSL/HTTPS). Any unencrypted calls are rejected.
Certificate validation	The certificate that is provided by the other party must be valid. For example, its hash must verify correctly and the current date and time must be after the certificate issue date and before the certificate expiry date. If Protection Center or any integrated product receives a call that includes expired or invalid certificates, it rejects the call with an access denied error.
Recognized product	The call must be signed using a certificate of a known product. If Protection Center or any integrated product receives a call that includes unrecognized certificates, it rejects the call with an access denied error.

Protection Center uses a "double gate" mechanism to secure actions, which is an approach that combines both the Protection Center security layer and the integrated product's security layer.

If a web service is provided by an integrated product and can be called in the context of a user (such as from a report row context menu) rather than only by Protection Center (such as a data feed) the product also ensures the following:

- If the caller's certificate is issued by the Protection Center certificate, the integrated product extracts the user name from the subject.
- If the user name is that of a product user, the product accepts it as identification and authentication. If not, the product returns an access denied error to the caller.

  As part of the product integration process, the Protection Center administrator associates Protection Center users with product users who have rights to administer the integrated product.

See "Protection Center user security" on page 25.

About Protection Center action security

An integrated product may allow Protection Center to perform actions on it. For each action, the product exposes the appropriate web service and supplies a workflow component that calls the web service. The workflow component is registered with Protection Center as part of the product registration process. The actions are performed on the product with user context.

Protection Center performs actions on an integrated product by calling the appropriate web service. Actions can be tied together using the Workflow feature of Protection Center. This allows the administrator to create customized workflow processes to enhance security management.

Protection Center action security is implemented as follows:

- Protection Center security controls the ability to view an action. If the user has no visibility to an action, then the action is not shown.
- Protection Center security controls the ability to execute an action. If the user does not have execute permissions, the action appears inactive.
- When the action is executed, a per-user certificate is used to pass user context information to the integrated product's action web service.
  See "Integrated product user certificates" on page 24.
- The integrated product uses the context information and checks whether that user has permissions to perform the action.
- If permissions are not sufficient, the appropriate faults/error codes are returned by the integrated product.

Protection Center communications security features

Protection Center includes mechanisms to prevent eavesdropping on data traffic, tampering (modification of traffic in transit) and spoofing (faking information) while authenticating the calling product/user and called product for auditing, authentication and non-repudiation (proving the communication comes from the other party).

These security features apply to all communications between Protection Center and integrated products: data feeds, actions, and drill-down reports. They also apply to all communications between Protection Center and the console browser. The Protection Center interface is a remote console: Protection Center is a "headless" appliance, and users do not access the Protection Center console directly from it.

Table 1-11 outlines the security features that are built into the communications between Protection Center and integrated products, and Protection Center and the Protection Center console browser.

Table 1-11 Protection Center communications security features

Feature	Description
Eavesdropping prevention	All communications between Protection Center and the integrated product server, and between Protection Center and the console are encrypted.
Replay prevention	If a third party manages to obtain access to the network traffic between Protection Center and an integrated product or the Protection Center console and inserts traffic into the data flow, the data inserted is detected by Protection Center, the integrated product, or the Protection Center console and is dropped. Protection Center relies on Transport Layer Security (TLS) and Secure Sockets Layer (SSL) for replay prevention.
Mutual authentication	If a third party attempts to communicate with Protection Center claiming to be a legitimately integrated product or the Protection Center console, the attempt is detected and prevented. If a third party attempts to communicate with an integrated product or the Protection Center console claiming to be Protection Center, the attempt is detected and prevented. The communications protocol enforces that both ends of the link are authenticated mutually. If a failed authentication attempt is detected, the invalid traffic is dropped and a system event is logged by Protection Center.
Tamper protection	It may be possible for a third party to obtain access to network traffic between Protection Center and an integrated product or the Protection Center console. The traffic is encrypted so the third party is not able to analyze the contents, but the data may be modified and sent to its destination in a modified form. Protection Center, the integrated product, or the Protection Center console detect that the data has been modified (or fail to decode the tampered data) and drop the invalid data. Protection Center relies on Transport Layer Security (TLS) or Secure Sockets Layer (SSL) for tamper protection.
Overload prevention	If an integrated product or the Protection Center console sends a large volume of data to Protection Center, it intelligently throttles the data to ensure that system thresholds are not exceeded. The throttling action causes a system event to be logged, but any failure or misbehavior of an integrated product does not cause an outage on Protection Center. For example, if there is a large number of newly registered product servers, Protection Center may receive large volumes of data and events.

About Protection Center web service security

Web service calls between Protection Center and integrated products (and vice versa, although this is rare) are encrypted to ensure that the data transmitted is visible only to authorized callers. Any calls to these methods over an unencrypted transport, such as raw HTTP, are rejected by both Protection Center and integrated products. All communications between Protection Center and integrated products uses SSL (version 3.0 or later) or TLS with 128-bit AES encryption.

All calls to non-registration web services require identification, authentication and authorization. Protection Center and each associated product provide an SSL certificate and both parties verify each other's certificate. This provides a much stronger authentication mechanism than user names and passwords and does not require the continual changing of passwords once configured.

All non-registration web methods use a per-user certificate that contains the username as the certificate subject. This certificate is issued by the Protection Center certificate so the integrated product can verify that the call is from Protection Center but can still identify the user for authentication and auditing. Because the Protection Center is trusted by the integrated product, the integrated product accepts the per-user certificate as valid (as the Protection Center certificate is the "issuer"). This per-user certificate is used typically for workflow or other actions to call web services exposed by the integrated product, but it may be used in any case where user context is part of the web service call. Data feed web services use the user that is defined in the registration process.

Any web services that are not called in the context of a user pass a certificate containing the username that was used during the product registration. The integrated product executes the web service in the context of the username retrieved from the certificate. The integrated product trusts the user is already authenticated by Protection Center.

See "Integrated product user certificates" on page 24.

The per-user certificate is generated for each product instance to which a particular user has access. Protection Center provides the ability to generate the certificate for a particular user for a particular integrated product instance (that is, one certificate per user per product instance).

Protection Center certificates

Protection Center authenticates with integrated products by mutual certificate authentication. Protection Center provides the Protection Center certificate or the appropriate user certificate. Each Protection Center user is issued a certificate by the Protection Center certificate authority. The common name of the certificate is issued to the name of the user.

Table 1-12 describes the main features of Protection Center certificates.

Table 1-12 Protection Center certificate features

Feature	Description
Key management	All certificates are stored in the machine certificate store. For all certificates, the private key of the public/private key pair is never transmitted over a network.
Certificate expiry and reissue	Protection Center does not provide an automated mechanism for reissuing certificates. Certificate lifetime is intentionally set for a long time (20 years) to prevent the need for doing so. If a key is compromised or if the administrator wants to cycle a key, the process is to unregister the integrated products, regenerate the certificate and key pair, and then re-register the products.
Self-signed certificates	During installation, each supported product generates a self-signed X.509 certificate and corresponding public/private key pair that can be used for signing TLS/SSL/HTTPS communications. See "Self-signed certificates" on page 23.
Customer-provided certificates	A supported product may allow the administrator to provide a different X.509 certificate and public/private key pair for server authentication. See "Customer-provided certificates" on page 24.
Integrated product user certificates	When Protection Center calls an integrated product web service in the context of a user (such as when a report row context menu item is selected) rather than Protection Center itself (such as a data feed), Protection Center creates an X.509 certificate and associated public/private key pair. This certificate identifies the user and is used in place of the Protection Center authentication certificate. See "Integrated product user certificates" on page 24.

Self-signed certificates

Each supported product provides a certificate and corresponding public/private key pair that can be used for signing TLS/SSL/HTTPS communications. The product can generate a self-signed X.509 certificate.

This certificate has the following properties:

- Uses SHA1 as its hashing algorithm.
- Uses RSA for its public/private key pair.
  The key size is 1024 bits.
- The certificate has a maximum validity (that is, a lifetime) of 20 years.

Customer-provided certificates

A supported product may allow the administrator to provide a different X.509 certificate and public/private key pair for server authentication. If the administrator changes the certificate and key pair of either Protection Center or an integrated product, the administrator needs to re-register the product with Protection Center.

A customer-provided certificate must have the following properties:

- If the Extended Key Usage (EKU) field is present, it must contain the Server Authentication (1.3.6.1.5.5.7.3.1) OID.
- The certificate should use SHA1 or better (e.g. SHA-256) as its hashing algorithm.
- The certificate must use RSA for its public/private key pair. It should have a key size of at least 1024 bits.

Note: The administrator can supply a certificate that does not meet recommendations given above. However, if the administrator does so, a warning message is displayed stating which recommendations were not met and explaining the associated security implications. The administrator will be prompted to confirm that they want to use the certificate before they can continue.

Integrated product user certificates

When Protection Center calls an integrated product web service in the context of a user (such as when a report row context menu item is selected) rather than Protection Center itself (such as a data feed), Protection Center creates an X.509 certificate and associated public/private key pair. This certificate identifies the user and is used in place of Protection Center's authentication certificate. The certificate is issued by the Protection Center authentication certificate.

Protection Center manages user certificates, including their issuing and reissuing when needed.

An integrated product user certificate has the following properties:

- The EKU field is present and contains the Client Authentication (1.3.6.1.5.5.7.3.2) OID.
- Uses SHA1 as its hashing algorithm.
- Uses RSA for its public/private key pair.
  The key size is 1024 bits.

Protection Center user security

Protection Center provides security controls on the data a user is able to access and view in Protection Center, and the tasks that a user can perform via the Protection Center console.

Protection Center has a non-deletable dedicated administrator account. The Protection Center administrator must set a cryptographically strong password during the installation process.

The password must contain at least eight characters and include at least three of the following:

- Uppercase alphabetic characters (A through Z)
- Alphabetic Unicode characters that are not categorized as uppercase (A through Z) or lowercase (a through z)
- Numeric characters (0 through 9)
- Non-alphanumeric characters (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

The Protection Center administrator is responsible for creating and managing Protection Center user accounts.

Note: The Protection Center administrator maps the Protection Center user accounts to the corresponding user accounts that exist on each integrated product. Protection Center cannot create a new user account on an integrated product.

Table 1-13 describes the Protection Center user security features.

Table 1-13 Protection Center user security features

Feature	Description
Permission-based security	Each Protection Center user account is assigned the appropriate set of Protection Center permissions. These permissions control user access to Protection Center features and functionality, such as console pages, folders, reports and so forth. See "Protection Center data security" on page 26.
Single sign-on	The Protection Center console supports single sign on (SSO) which enables it to display pages from an integrated product's user interface without requiring the user to sign in to each individual product. When the user is logged in to Protection Center, they have seamless access to all of the integrated products that they have permission to manage. When the user opens an integrated product console they are automatically authenticated on the product host. See "About SSO" on page 27.

Protection Center data security

Securing access to data in Protection Center involves the following:

- Controlling general access to functionality within the Protection Center console (data and reports).
- Controlling access to specific data and reports.
- Controlling access to specific resources (assets) when running reports or running tasks.

Protection Center essentially “owns” all of the data in Protection Center, either in the database as part of summary data or in the event archive. The Event Archiver component of Protection Center collects, archives and summarizes events without regard to security. All data security is applied according to the permissions of the user account that is accessing the data.

Table 1-14 describes the main components of the Protection Center data security mechanism.

Table 1-14 Protection Center data security mechanism components

Component	Description
Local permissions	Local permissions control user access to Protection Center entities such as console pages, folders, and reports. The Protection Center administrator can assign the appropriate local permissions to individual users. Local permissions can be applied to control access to specific reports. Specific reports are provided to control access to field-level data. For example, a report may contain two views: one that shows personally identifiable information (PII) and another that hides these fields. When the report is run, the user's local permissions on the report determine whether the user can see these fields.
Global permissions	Global permissions identify broad rights to perform an action (for example, Run Report). The Protection Center administrator can assign the appropriate global permissions to individual users. Global permissions for a given user apply across all integrated product data. For instance, if a user does not have the global permission to run reports, they will be unable to access any report or its associated data.

About Protection Center user interface security

The Protection Center user interface (the Protection Center console) is a web-based administration console that Protection Center users can access from remote computers. The Protection Center console cannot be accessed directly from the Protection Center appliance. Protection Center is designed for a relatively small

number of concurrent users (up to five). To ensure robust security, all communication between Protection Center and the Protection Center console is encrypted and authenticated.

The Protection Center console lets the administrator manage all of your integrated products from a single place. The Protection Center administrator can add new products as they are deployed in your environment, and remove any that are no longer required. The Protection Center administrator can set up and manage Protection Center user accounts, view summary data, generate reports, and perform any necessary Protection Center configuration and management tasks.

The Protection Center permission-based security system ensures that each user sees only the data to which he or she has appropriate access. The information that is displayed in the Protection Center console is filtered according to the permissions that are assigned to the user. For example, the administrator of a particular integrated product (or group of related products) may see only the data that is related to their product, and cannot see data from other integrated products. The administrator does not have access to dashboards or console features that are not relevant to any of their products.

The Protection Center console supports single sign-on (SSO), which enables it to display pages from an integrated product's user interface in the Protection Center console without requiring the user to sign in to each individual product server. When users are logged in to Protection Center, they have seamless access to all of the integrated products that they have permission to manage. When users open an integrated product console, they are automatically authenticated on the product host. When they sign out of the Protection Center console, they are automatically signed out of any integrated product servers to which they were signed into through SSO.

The SSO mechanism passes username context information when navigating to integrated product pages. This lets the integrated product apply the appropriate access control over page elements based on the user context. It also allows appropriate auditing and logging of user activity.

About SSO

When a product integrates with Protection Center, as part of the registration process it provides Protection Center with appropriate product-specific objects such as console pages and reports. These are treated as native Protection Center objects and can be accessed by a Protection Center user account with the appropriate permissions.

However, many products have objects, such as user interface pages or drill-down reports, that are not provided to Protection Center but remain part of the product.

Access to these objects requires a product-specific user account on the product server with the required level of access defined by the product.

To allow a Protection Center user to access these objects from the Protection Center console, the Protection Center user account must be mapped to the corresponding product user account. This mapping is performed by the Protection Center administrator as part of the Protection Center user account configuration process after the product is registered.

When these objects are accessed (pages are loaded or reports are run), the Protection Center user is authenticated and authorized against the product server. This authentication and authorization is transparent to the user.

When the Protection Center console needs to display a page from an integrated product, the Protection Center console first checks that the page is from a server that supports SSO. It then connects to a web service on Protection Center to obtain an authentication ticket. The Protection Center console redirects to the application authentication handler on the product server, and includes the authentication ticket as part of the query string.

If the authentication handler page successfully validates the authentication ticket, it grants the user access and redirects to the target page. The successful authentication is usually stored in a cookie, which is deleted when the user logs out of Protection Center.

Appendix A

Protection Center reference

This appendix includes the following topics:

Windows services whitelist

Protection Center uses a whitelist to start all required Windows services and stop all others.

Table A-1 shows the Windows services whitelist for Protection Center.

Table A-1 Windows services whitelist

Service	Service Display Name
AltirisClientMsgDispatcher	Altiris Client Message Dispatcher
ctdataloader	Altiris Client Task Data Loader
EventEngine	Altiris Event Engine
EventReceiver	Altiris Event Receiver
AltirisReceiverService	Altiris File Receiver
MetricProvider	Altiris Monitor Agent
atrshost	Altiris Object Host Service
AeXSvc	Altiris Service

Table A-1 Windows services whitelist *(continued)*

Service	Service Display Name
AeXAgentSrvHost	AeXAgentSrvHost
AltirisSupportService	Altiris Support Service
Tomcat6	Apache Tomcat Tomcat6
AeLookupSvc	Application Experience
AppHostSvc	Application Host Helper Service
Backup Exec System Recovery	Backup Exec System Recovery
BFE	Base Filtering Engine
CertPropSvc	Certificate Propagation
EventSystem	COM+ Event System
COMSysApp	COM+ System Application
Browser	Computer Browser
CryptSvc	Cryptographic Services
DcomLaunch	DCOM Server Process Launcher
Dhcp	DHCP Client
DPS	Diagnostic Policy Service
WdiSystemHost	Diagnostic System Host
MSDTC	Distributed Transaction Coordinator
Dnscache	DNS Client
gpsvc	Group Policy Client
IISADMIN	IIS Admin Service
IKEEXT	IKE and AuthIP IPsec Keying Modules
iphlpsvc	IP Helper
PolicyAgent	IPsec Policy Agent
LogicBase 2006 Server Extensions	LogicBase 2006 Server Extensions
clr_optimization_v2.0.50727_64	Microsoft .NET Framework NGEN v2.0.50727_X64

Table A-1 Windows services whitelist *(continued)*

Service	Service Display Name
netprofm	Network List Service
NlaSvc	Network Location Awareness
nsi	Network Store Interface Service
PlugPlay	Plug and Play
Power	Power
SessionEnv	Remote Desktop Configuration
TermService	Remote Desktop Services
UmRdpService	Remote Desktop Services UserMode Port Redirector
RpcSs	Remote Procedure Call (RPC)
RpcEptMapper	RPC Endpoint Mapper
SamSs	Security Accounts Manager
LanmanServer	Server
sppsvc	Software Protection
MSSQLSERVER	SQL Server (MSSQLSERVER)
SQLWriter	SQL Server VSS Writer
Symantec AntiVirus	Symantec Endpoint Protection
EventChannelHost	Symantec Event Channel Host
ccEvtMgr	Symantec Event Manager
AeXNSClient	Symantec Management Agent
SmcService	Symantec Management Client
ccSetMgr	Symantec Settings Manager
SPCDataFeedSvc	Symantec SPC Data Feed Service
SymSnapService	SymSnapService
SENS	System Event Notification Service
Schedule	Task Scheduler

Table A-1 Windows services whitelist *(continued)*

Service	Service Display Name
lmhosts	TCP/IP NetBIOS Helper
ProfSvc	User Profile Service
VDS	Virtual Disk
Symantec SymSnap VSS Provider	Symantec SymSnap VSS Provider
VMTools	VMware Tools Service
VSS	Volume Shadow Copy
eventlog	Windows Event Log
MpsSvc	Windows Firewall
Winmgmt	Windows Management Instrumentation
WAS	Windows Process Activation Service
WinRM	Windows Remote Management (WS-Management)
wuauserv	Windows Update
WinHttpAutoProxySvc	WinHTTP Web Proxy Auto-Discovery Service
LanmanWorkstation	Workstation
W3SVC	World Wide Web Publishing Service
SPCLue	Symantec SPCLue
LiveUpdate	LiveUpdate
SWFSVR	Symantec Workflow Server
altirisservicehoster	Altiris Service Hoster
W32Time	Windows Time

Windows components whitelist

Windows Server 2008 maintains components that can be enabled or disabled as appropriate for feature and application management. Protection Center uses a whitelist to enable the required components and disable all others.

Table A-2 shows the Windows components whitelist for Protection Center.

Table A-2 Windows components whitelist

Update ID	Update title
4eba1a7c-af81-4469-9602-0b4fe8ec28d0	Security Update for Windows Server 2008 R2 x64 Edition (KB2387149)
8eb97d69-d354-48d0-aedb-a09aaf52eb31	Security Update for Windows Server 2008 R2 x64 Edition (KB2393802)
c226e2b5-72d5-4ace-97d2-a555f0bbf79d	Security Update for Windows Server 2008 R2 x64 Edition (KB2419640)
1806e55a-c88d-4750-80f7-8916fcb1394e	Security Update for Windows Server 2008 R2 x64 Edition (KB2423089)
b8383ed5-de98-4c8d-a790-410cedc6fe9d	Security Update for Windows Server 2008 R2 x64 Edition (KB2425227)
0592e277-4c0e-4d99-8192-8db3a793b101	Security Update for Windows Server 2008 R2 x64 Edition (KB2442962)
2608711d-74e4-409e-9513-4844d9788a6c	Security Update for Windows Server 2008 R2 x64 Edition (KB2475792)
60db0e2f-fda5-474a-b759-c1c8ff5b269f	Security Update for Windows Server 2008 R2 x64 Edition (KB2479628)
07c7a225-474c-4610-b043-b5d54c6809ff	Security Update for Windows Server 2008 R2 x64 Edition (KB2483614)
4ce62edb-22c6-4de5-bd87-81a3e9594deb	Security Update for Windows Server 2008 R2 x64 Edition (KB2485376)
5cd65fec-fed8-42ea-8ccb-7d73994e992c	Security Update for Windows Server 2008 R2 x64 Edition (KB972270)
df1869dd-8d9b-4976-bfc9-df691163eec7	Security Update for Windows Server 2008 R2 x64 Edition (KB974571)
99dce205-ce79-4832-b451-5c53b9884226	Security Update for Windows Server 2008 R2 x64 Edition (KB975467)
a262fdba-368b-446d-b3d3-93221446086c	Security Update for Windows Server 2008 R2 x64 Edition (KB975560)
681cf167-f252-4207-8304-4cb9c33e6dae	Security Update for Windows Server 2008 R2 x64 Edition (KB978542)
50671659-f69d-4b82-a465-40cecf59d694	Security Update for Windows Server 2008 R2 x64 Edition (KB978601)

Table A-2 Windows components whitelist *(continued)*

Update ID	Update title
c2954091-5c05-40be-a4b6-685e2c338e8d	Security Update for Windows Server 2008 R2 x64 Edition (KB978886)
4f8f3eed-a00d-4dce-a3e0-80f7f5fb1c52	Security Update for Windows Server 2008 R2 x64 Edition (KB979309)
25776dd9-17f6-453e-8c69-010d6a12c263	Security Update for Windows Server 2008 R2 x64 Edition (KB979482)
07ee2f77-a85b-455a-8f21-103992516a70	Security Update for Windows Server 2008 R2 x64 Edition (KB979687)
8b747c27-0276-4079-9b98-744c6979fd42	Security Update for Windows Server 2008 R2 x64 Edition (KB979688)
29e4a0e6-321c-4ac5-a4ba-ec1ebfcabc11	Security Update for Windows Server 2008 R2 x64 Edition (KB980232)
18639555-bb92-4ac7-9d4c-08c4d24a5562	Security Update for Windows Server 2008 R2 x64 Edition (KB982132)
4883d202-4215-462c-8374-1ee29dde2a43	Security Update for Windows Server 2008 R2 x64 Edition (KB982214)
6ad385d8-c363-4259-937c-f17fb3c6ff0f	Security Update for Windows Server 2008 R2 x64 Edition (KB982666)
78e2d12c-6113-40ac-833f-9e1df1b02652	Security Update for Windows Server 2008 R2 x64 Edition (KB982799)
0927ff06-bfc7-489e-aa5a-8e5b42fb4c82	Update for Windows Server 2008 R2 x64 Edition (KB2443685)
cbb02d57-af87-4fc2-886e-730c605ea2de	Update for Windows Server 2008 R2 x64 Edition (KB2467023)
0b264f9d-bbf4-4070-8ff6-1e3b356050dc	Update for Windows Server 2008 R2 x64 Edition (KB976902)
11de740d-80aa-4f4f-b0fc-f70edd10153b	Update for Windows Server 2008 R2 x64 Edition (KB979538)
5af5fb75-62de-4359-b277-46f2136e37a1	Update for Windows Server 2008 R2 x64 Edition (KB982110)
6231868d-cd3e-43bc-a530-440722b40484	Microsoft .NET Framework 3.5 SP1 Update for Windows 7 and Windows Server 2008 R2 for x64-based Systems (KB982526)
f4e634d9-6eba-4c43-9b50-1bee41dbf767	Windows Malicious Software Removal Tool x64 - March 2011 (KB890830)

Firewall settings required to support Protection Center

Protection Center is configured to reject inbound connections to ports that are not on the whitelist. Protection Center can reach out on any port necessary to communicate with integrated products, regardless of which ports are blocked.

Table A-3 shows the firewall applications whitelist for Protection Center.

Table A-3 Firewall applications whitelist

Name	Path
CTDataLoad	C:\Program Files\Symantec\TaskManagement\CTDataLoad.exe
AtrsHost	C:\Program Files\Symantec\TaskManagement\AtrsHost.exe

Table A-4 summarizes the ports and protocols that are used by Protection Center.

Table A-4 Ports and protocols used by Protection Center

Port	Protocol	Description
80	HTTP	End user to Protection Center: Redirects users to HTTPS.
443	HTTPS	End user to Protection Center: Access to Protection Center console.
80	HTTP	Protection Center to LiveUpdate server: Default port for communication between Protection Center and the LiveUpdate server.
443	HTTPS	Protection Center to LiveUpdate server: Default port for communication between Protection Center and the LiveUpdate server.
21, any port over 1024	FTP	Protection Center to LiveUpdate server: FTP communication between Protection Center and the LiveUpdate server.
8080	HTTP	Protection Center to Protection Center: Apache Tomcat-hosted Archiver.
11434	HTTP	Protection Center to Protection Center: Symantec Workflow Solution.
50121 - 50124	HTTP	Integrated products to Protection Center: For integrated products that use the SMP agent to send data, these are the control ports used to receive Task Server communications.
443	HTTPS	Integrated products to Protection Center: For integrated products that use the SMP agent for data collection, this is the port that the data is sent over.
25	SMTP	Protection Center to SMTP server: Default email port.

Table A-4 Ports and protocols used by Protection Center *(continued)*

Port	Protocol	Description
53	UDP	Protection Center to DNS server: Domain name resolution.
123	NTP	Protection Center to NTP server: Network Time Protocol, used to keep system time synchronized between Protection Center and the integrated products.
7890, 7891	HTTPS	Protection Center to DeepSight Intermediate server: Used to capture Global Intelligence Network information from the DeepSight Intermediate server.
8530	HTTP	Protection Center to Microsoft WSUS: Default port used to pull Windows Software Update Services (WSUS) information from Microsoft WSUS servers. This port can be changed when setting up a WSUS server.
80, 443	HTTP	Protection Center to Windows Update: These ports are used when Protection Center communicates with Microsoft's update servers on the Internet instead of with a local WSUS server.

Protection Center performance

Table A-5 summarizes the items that may impact Protection Center performance.

Table A-5 Items that may impact Protection Center performance

Item	Description
Potential socket leak	A known issue with Windows Server 2008 R2 may cause Protection Center to stop working. For more information, see *Kernel sockets leak on a multiprocessor computer that is running Windows Server 2008 R2 or Windows 7* on the Microsoft Web site. http://support.microsoft.com/kb/2577795
System security check	Protection Center performs a system security check every 30 minutes to ensure that the security lockdowns have not been circumvented. This check uses system resources and can take up to five minutes to run, and has a minor impact on Protection Center performance.
Audit logging	Protection Center does perform some audit logging, but the impact on Protection Center performance is negligible.
Secure console access	Using an SSL connection to access the Protection Center console takes up about 15% more resources than a regular non-SSL connection. However, this is the same for any SSL-enabled web server or web application.

Index

R

S

U

W