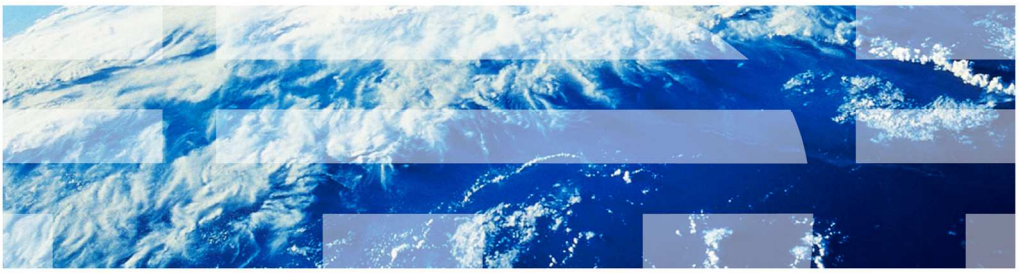
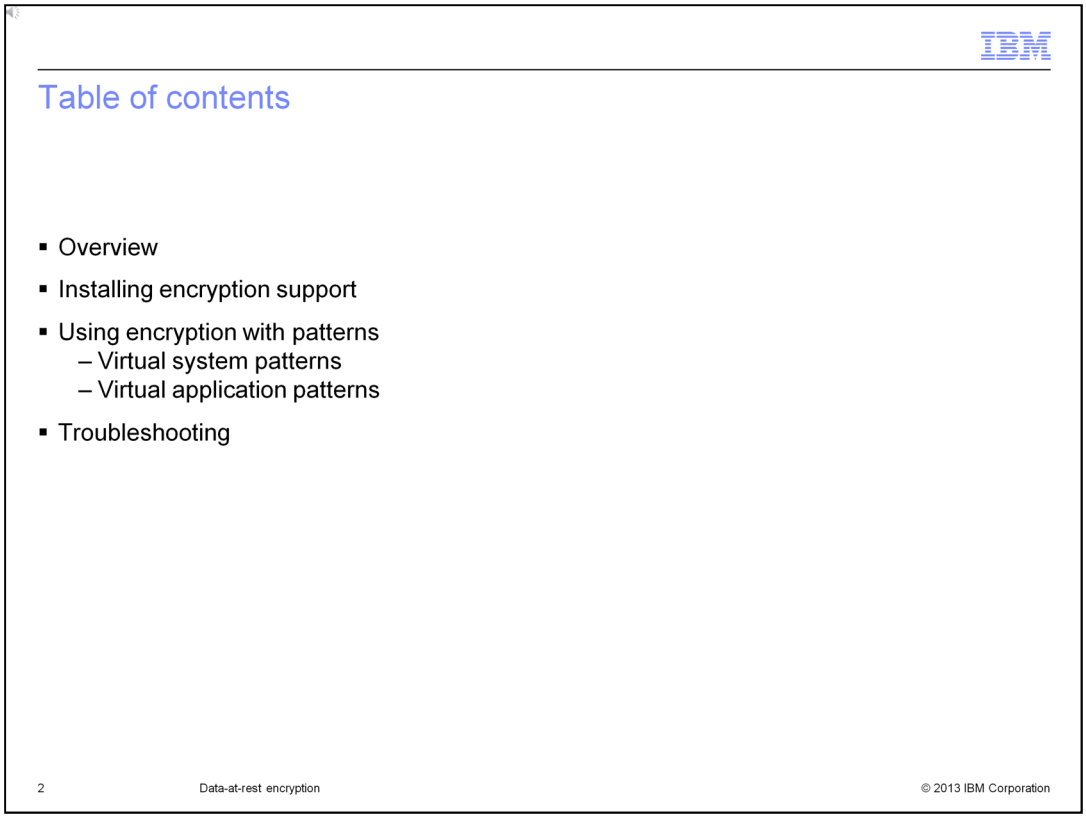
IBM PureApplication System

Data-at-rest encryption



This presentation covers the support for data-at-rest encryption in IBM PureApplication™ System V1.1.



This presentation begins with a brief introduction to data-at-rest encryption, followed by sections on installing encryption support, using encryption with patterns, and troubleshooting.

Integrated file system encryption

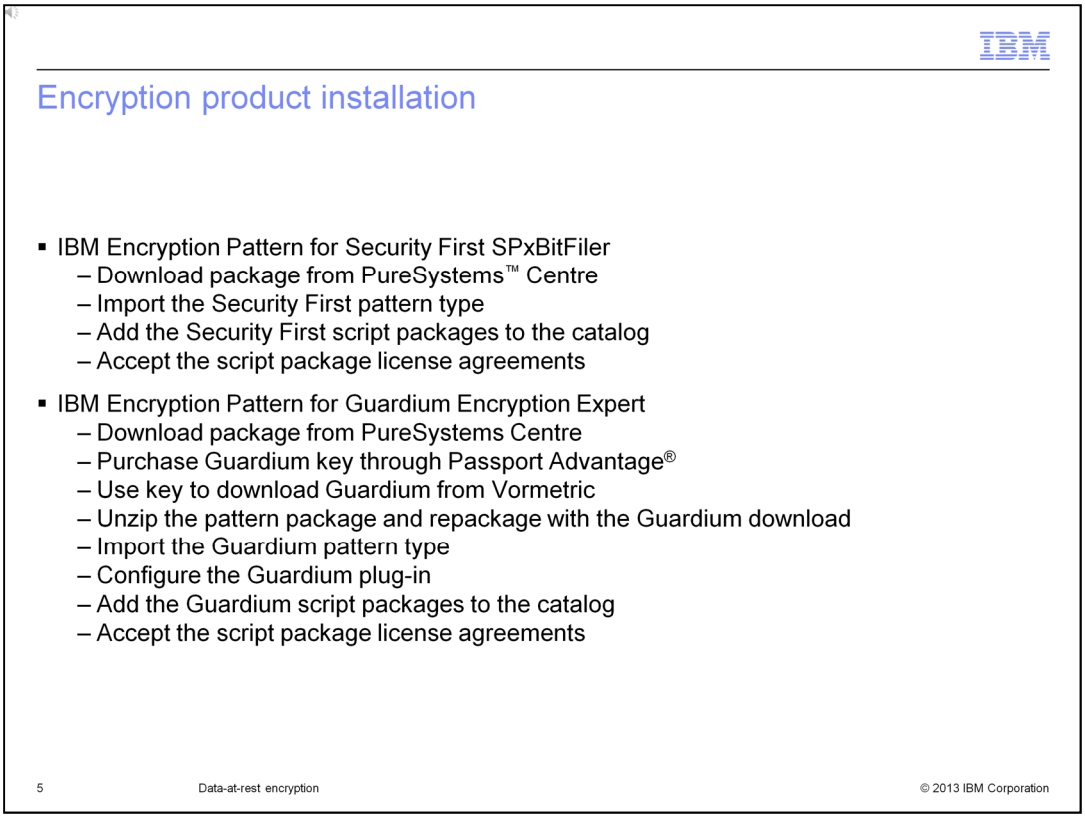
- Ensure security of data-at-rest with integrated file system encryption
  - Specify paths to be encrypted using the pattern editor interface
- Support for all virtual application patterns and virtual system patterns
  - Virtual application support through encryption policy
  - Virtual system support through script package
- Requires separate purchase
  - IBM Encryption Pattern for Guardium® Encryption Expert
    - Policy-based encryption service
    - Managed using Guardium Data Security Manager (DSM)
    - http://www-01.ibm.com/software/data/guardium/encryption-expert/
  - IBM Encryption Pattern for Security First SPxBitFiler
    - Standalone encryption service
    - http://www.securityfirstcorp.com/spx_bitfiler.html

3 Data-at-rest encryption

This slide introduces you to the data-at-rest encryption support in PureApplication System V1.1.

PureApplication System V1.1 includes support for protecting your data-at-rest by using integrated file system encryption products that can be configured using the pattern editors in the workload console. These products are purchased separately and provide data-at-rest encryption for both your virtual application patterns and virtual system patterns. IBM Encryption Pattern for Guardium Encryption Expert provides support for integrating your patterns with Guardium Data Security Manager, which enables centralized, policy-based management of data encryption services. IBM Encryption Pattern for Security First SPxBitFiler provides a stand-alone encryption service for your patterns and exposes configuration parameters for setting encryption rules for each virtual machine.

This section covers installing encryption products for use with PureApplication System.



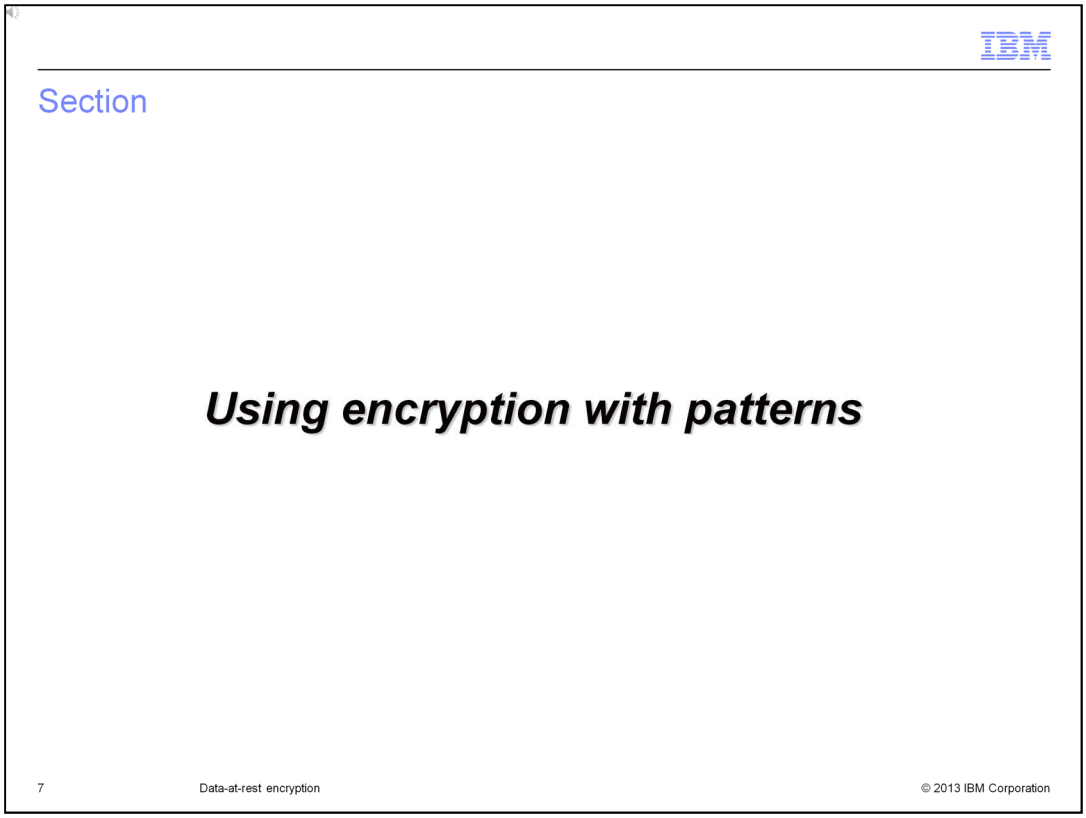
File system encryption support for patterns requires one of these two supported encryption products to be installed on your system. If one of the supported encryption products is not yet installed on your system, your organization will need to purchase and install one of the products from PureSystems Centre. After downloading and decompressing one of the security products from PureSystems Centre, install it by importing the pattern type and adding the included script packages to the catalog. Before you can import the Guardium pattern type, you must also purchase a Guardium key, use the key to download Guardium from Vormetric, and then repackage your downloaded pattern with the Guardium code.

Configuring the Guardium plug-in

- Configure the Guardium plug-in with information about Data Security Manager
  - All virtual application patterns will use this configuration
  - Virtual system patterns use script packages for Data Security Manager configuration
- Workload console > Cloud > System plug-ins

6 Data-at-rest encryption

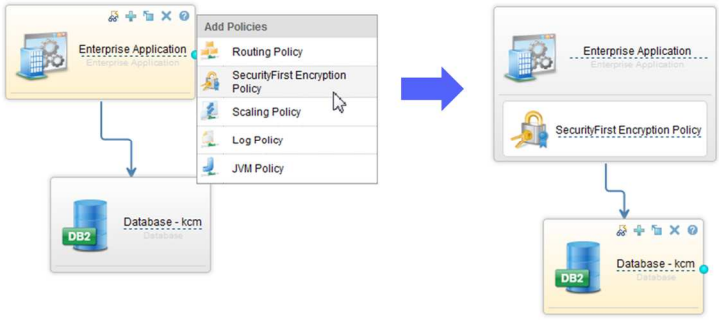
To enable file system encryption for your virtual application patterns, you must first add the pattern type for the product that you purchased to your system. If you are using the Guardium pattern, then you need to provide the information for connecting to your Data Security Manager and the policies that you want to use as configuration properties of the Guardium plug-in. All virtual application patterns with an attached Guardium security policy will use this configuration. When working with virtual system patterns, script packages are used to provide the Data Security Manager and policy configuration information.



This section covers using data-at-rest encryption with virtual application and virtual system patterns.

Encryption support for virtual application patterns

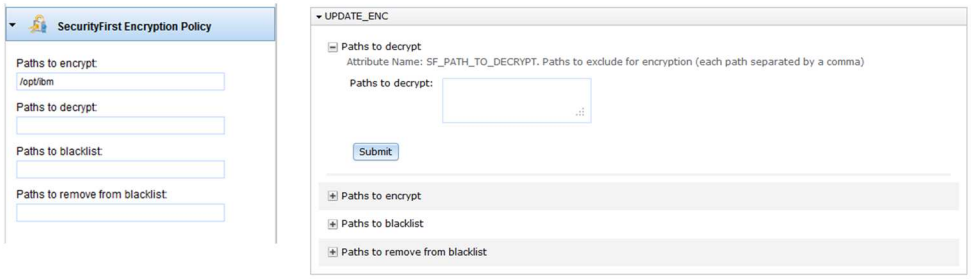
- Encryption support is provided by encryption policies
  - Security First Encryption Policy
  - Guardium Encryption Policy
- Add policies at component or application level



Encryption policies are used to add encryption support to your virtual application patterns and can be attached to your virtual applications in the same way as other types of policies. This slide shows a Security First encryption policy being attached to an enterprise application component. Like other policies, encryption policies can also be attached at the application level, to provide encryption support for all components in a pattern.

Encryption policy configuration

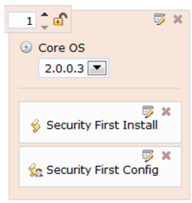
- Define deployment-time encryption options in the policy configuration panel
- Options can be changed after deployment using the “Operations” panel



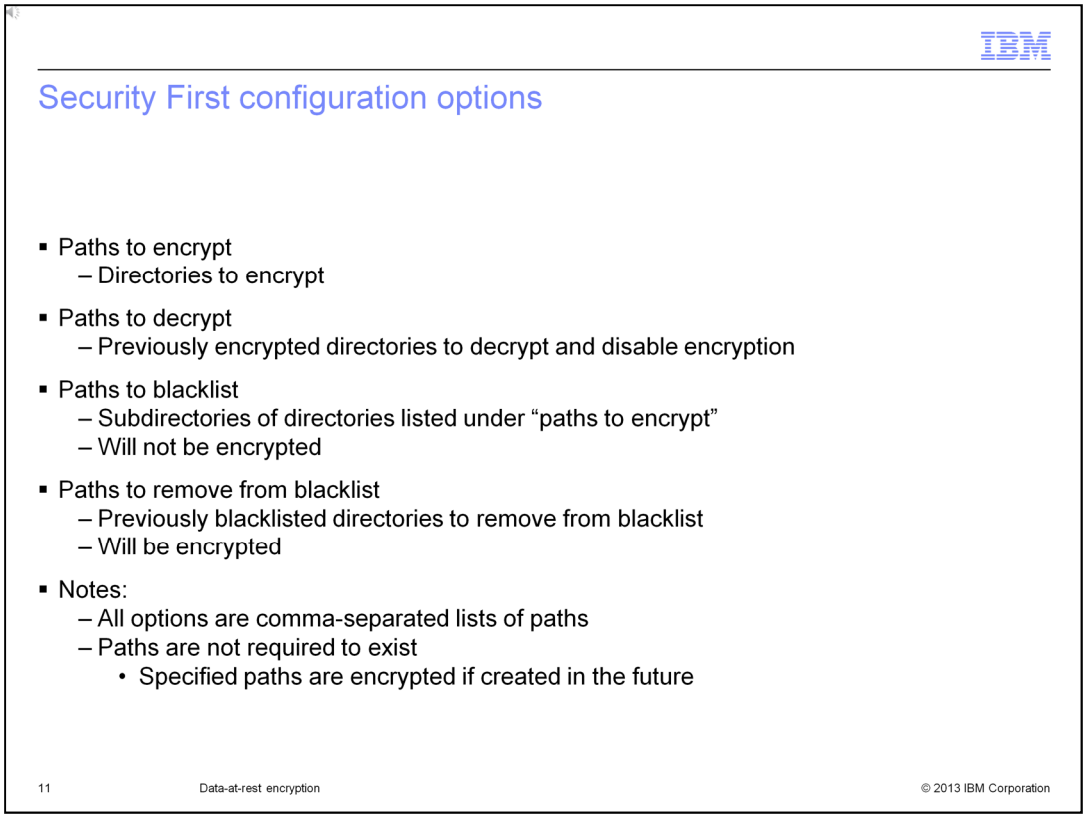
When an encryption policy has been attached to a component or application, configuration options for the policy are displayed in the virtual application pattern editor. These options are used to define deployment-time parameters, including the directories on the file system that should be encrypted. To change these options after deployment, use the “operations” panel for the deployed instance.

Encryption support for virtual system patterns

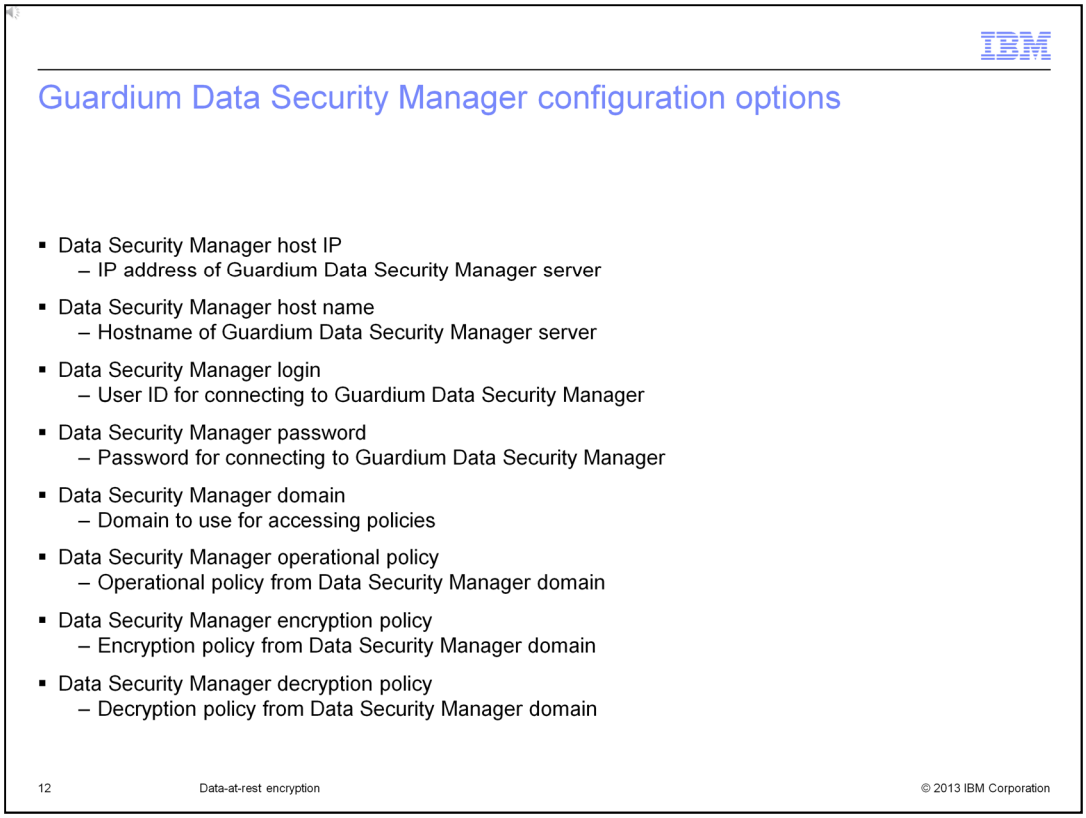
- Encryption support is provided by script packages
  - Attach script packages to parts in a pattern
  - Configure options using script package parameters
- Script package order is important
  - Guardium
    - Install Guardium
    - Configure Guardium
    - Delete Guardium
  - Security First
    - Security First Install
    - Security First Config
- "Delete Guardium" removes the virtual machine from the Guardium Data Security Manager domain



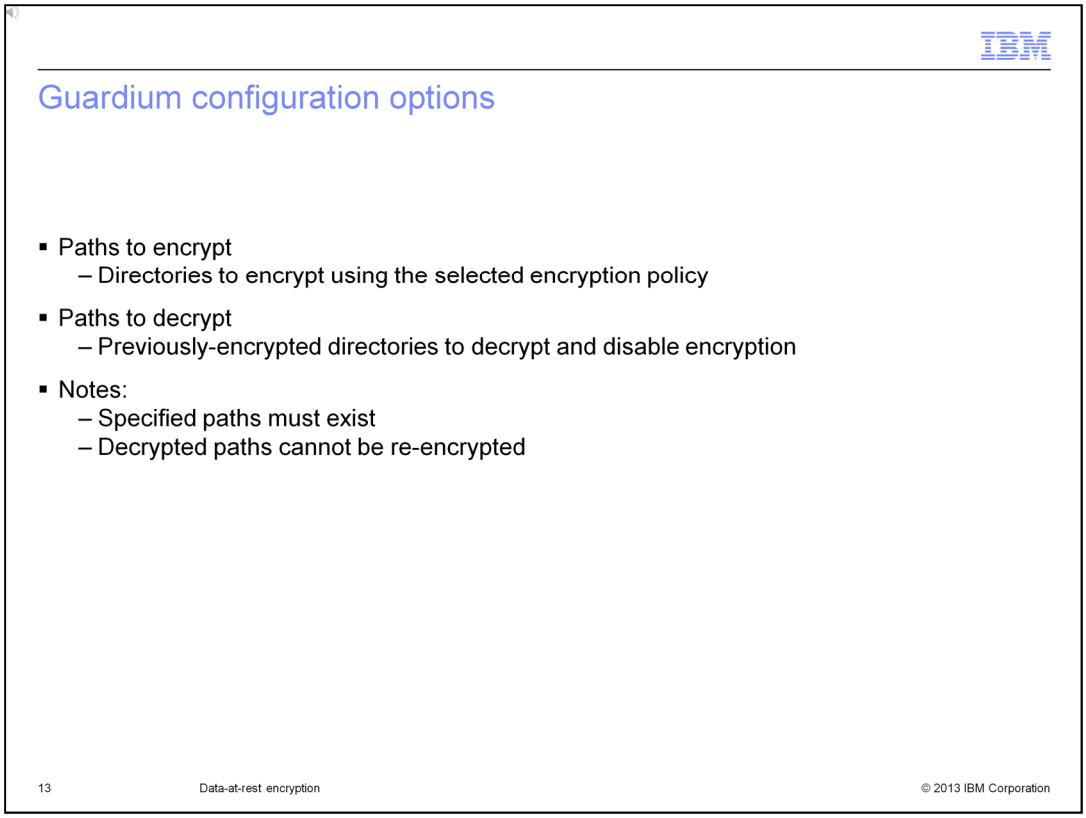
File system encryption support can be added to virtual system patterns by using script packages. To add file system encryption support to a part in a virtual system pattern, attach the script packages that were provided with the pattern that you downloaded from the PureSystems Centre. Script ordering is important—the "install" script must always run before the "configure" script. Deployment-time configuration options for the encryption products are exposed as parameters on the script packages. Script packages must be attached and configured individually for each part that requires file system encryption support. There is no mechanism for applying encryption support at the pattern level.



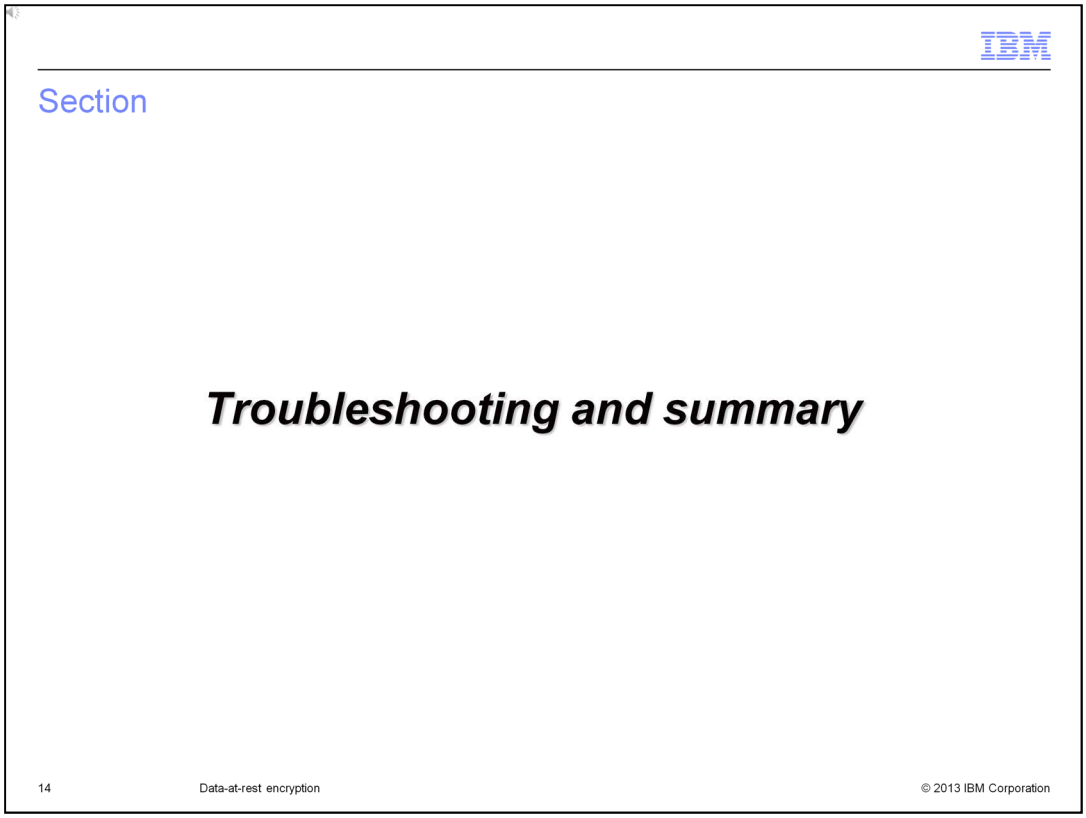
Security First BitFiler is configured using the four options shown here. These are configured either as properties on the security policy for virtual application patterns or as script package parameters for virtual system patterns. Each option takes a comma-separated list of paths as input. The “paths to encrypt” option is where you specify the list of paths to be encrypted. The “paths to decrypt” option is where you specify the list of previously-encrypted directories that should no longer be encrypted. The “paths to blacklist” option is used to specify subdirectories within the directories that are listed in “paths to encrypt” that should be excluded from encryption. The “paths to remove from blacklist” option is used to remove previously-blacklisted paths. These will now be encrypted, since they are covered by the “paths to encrypt” option.



These options are configured for virtual system patterns using the “install guardium” script package and for virtual application patterns using the configuration panel for the Guardium plug-in. This means that a single Data Security Manager configuration is used for all virtual application patterns, while each part of each virtual system pattern can use a different Data Security Manager configuration. These options are used to specify how to connect to the Data Security Manager and which domains and policies should be used.



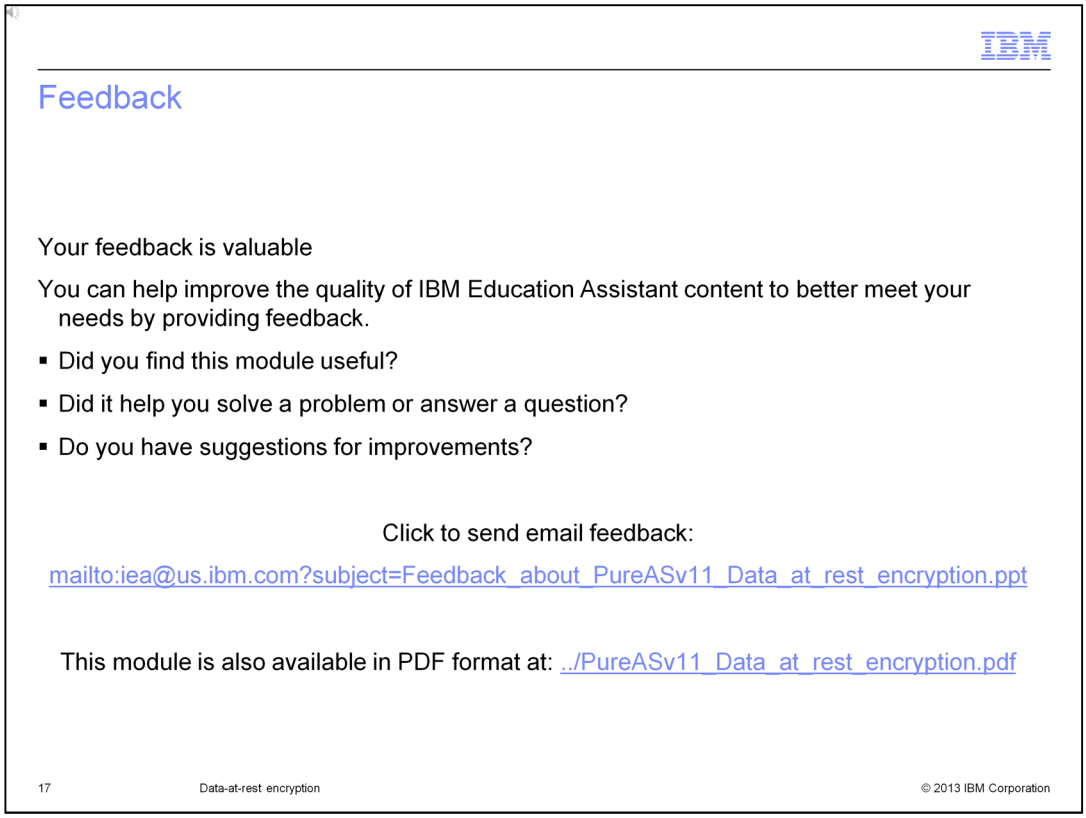
You can provide deployment-specific options for Guardium by using the Guardium encryption policy for virtual application patterns and by using the “configure guardium” script package for virtual system patterns. You can specify paths to encrypt and previously-encrypted paths to decrypt and disable encryption. Note that the paths specified in these parameters must exist and that you cannot re-encrypt a decrypted path when using Guardium encryption.



This section covers basic troubleshooting for encryption patterns and provides a summary of the presentation.

Both of the supported encryption products are installed on virtual system instances using plug-in injection after the attached script packages write configuration data to JSON files on the instance. This means that when troubleshooting installation or configuration problems with the encryption products, only the JSON data is contained in the script package log files. For more information about installation and configuration of the encryption products, locate the trace.log file at the path shown on this slide. When using Guardium, the “delete guardium” script is designed to run when the instance is deleted and removes the instance from the Data Security Manager domain. For the script package to run as designed, the instance must be deleted while running. If the instance is deleted while stopped, you must manually remove the IP address of the instance from the Data Security Manager domain using the Guardium web interface. Otherwise, the IP address that was used by the deleted instance cannot be reused.

PureApplication System V1.1 provides support for two data-at-rest encryption products, which can be purchased from PureSystems Centre separately and installed onto your system. IBM Encryption Pattern for Guardium Encryption Expert and IBM Encryption Pattern for Security First SPxBitFiler both provide integrated file system encryption for virtual system patterns and virtual application patterns.



You can help improve the quality of IBM Education Assistant content by providing feedback.

Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, Guardium, Passport Advantage, PureApplication, and PureSystems are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of other IBM trademarks is available on the web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml

Guardium, is a trademark or registered trademark of Guardium, Inc., an IBM Company, in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.