DeviceLock® Discovery 8.3

User Manual

Trademarks

DeviceLock and the DeviceLock logo are registered trademarks of DeviceLock, Inc. All other product names, service marks, and trademarks mentioned herein are trademarks of their respective owners.

DeviceLock Discovery - User Manual
Software version: 8.3
Updated: July 2019

Contents

About This Manual

This manual provides detailed information about how to install and use DeviceLock Discovery. It is primarily intended for administrators, security specialists, and other IT professionals who focus on how to provide data security within an organization. This manual assumes some basic knowledge of the Microsoft Windows operating system and networking as well as the ability to create a local area network (LAN).

Conventions

The following table lists the formatting conventions used in this manual.

Element	Convention
Bold text	Indicates user interface elements such as menus, commands, dialog box titles and options.
Italic text	Used for comments.
Blue text	Used for cross-references and hyperlinks.
Note	Highlights supplementary information pertinent to the process being described.
Tip	Highlights information detailing the recommended course of action for the best result.
Important	Highlights information about actions that should be performed with care.
Plus sign (+)	A plus sign between two keystrokes means that you must press them at the same time.

DeviceLock Discovery Overview

In this chapter:

Introducing DeviceLock Discovery

DeviceLock Discovery further extends DeviceLock DLP, helping network administrators and security personnel locating certain types of content stored within and outside the limits of the corporate network. Discovering unwanted content is essential when trying to protect the company's intellectual property, control employee activities and administer computer networks.

DeviceLock Discovery Server is a server component and a part of DeviceLock Content Security Server. DeviceLock Discovery is designed to scan users' workstations and storage systems located inside and outside the company's corporate network, looking for certain types of content according to pre-defined rules. Administrators can assign rules specifying which content is not allowed on the corporate network.

DeviceLock Discovery can audit what types of content are stored on a particular workstation or storage device. Based on the defined security context, this capability allows network administrators and IT security personnel to perform a comprehensive audit regarding the content stored on the organization's premises.

Understanding DeviceLock Discovery

DeviceLock Discovery is used to discover certain types of content existing on the computers and storage devices connected to the local network. These include supported local synchronization directories for selected cloud storage services. Discovery Agent automatically detects all synchronization folders on computer for selected services and performs scanning and configured Discovery actions for files stored in these folders. When used together with DeviceLock, the DeviceLock Discovery greatly enhances the capabilities of the Content-Aware Rules feature. With DeviceLock Discovery, you can not only locate information, but perform a number of actions to grant or deny access to information, alert the administrator, remove or encrypt discovered content or notify the computer user.

DeviceLock Discovery discovers information based on real file types, and allows using regular expression patterns with numerical conditions and Boolean combinations of matching criteria and keywords. Recognizing more than eighty file formats and data types, DeviceLock Discovery extracts and filters the content of data stored on computers' local hard drives, plug-n-play storage devices and NAS servers attached to the local area network. With DeviceLock Discovery, you can also narrow the search to filter information down to just those pieces meaningful to security auditing, incident investigations and forensic analysis.

The key features and benefits of DeviceLock Discovery are as follows:

Content-based discovery. You can discover information and automatically take pre-defined actions based on real type of information as determined by its actual content. Content-based discovery can locate many types of data even if the files are renamed and their extensions changed. Thus, you can identify sensitive content receiving an immediate alert, removing the content on the spot or changing available access rights.

Document classification-based discovery. You can discover documents and automatically take pre-defined actions based on:

- Digital fingerprints of sensitive documents being taken and stored on the DeviceLock Enterprise Server. Fingerprint-based discovery can identify full copies as well as pieces of documents, even if the document has been changed.

- Classification labels for third-party products, such as the Boldon James Classifier applications, in which document attributes are set according to the level of sensitivity of the document.

Expansive coverage of multiple file formats and data types. You can identify content in the following file formats and data types: Adobe Acrobat (including encrypted files if the type of encryption in the file is one of the following: 40-bit RC4, 128-bit RC4, 128-bit AES and 256-bit AES, and the file permissions do not disable text extraction) (*.pdf), Adobe Framemaker MIF (*.mif), Ami Pro (*.sam), Ansi Text (*.txt), ASCII Text, ASF media files (metadata only) (*.asf), AutoCAD (*.dwg, *.dxf), CSV (Comma-separated values) (*.csv), DBF (*.dbf), EBCDIC, EML (emails saved by Outlook Express) (*.eml), Enhanced Metafile Format (*.emf), Eudora MBX message files (*.mbx), Flash (*.swf), GZIP (*.gz), HTML (*.htm, *.html), iCalendar (*.ics), Ichitaro (versions 5 and later) (*.jtd, *.jbw), JPEG (*.jpg), Lotus 1-2-3 (*.123, *.wk?), MBOX email archives such as Thunderbird (*.mbx), MHT archives (HTML archives saved by Internet Explorer) (*.mht), MIME messages (including attachments), MSG (emails saved by Outlook) (*.msg), Microsoft Access MDB files (*.mdb, *.accdb, including Access 2007 and Access 2010), Microsoft Document Imaging (*.mdi), Microsoft Excel (*.xls), Microsoft Excel 2003 XML (*.xml), Microsoft Excel 2007, 2010, and 2013 (*.xlsx), Microsoft OneNote 2007, 2010, and 2013 (*.one), Microsoft Outlook data files (*.PST), Microsoft Outlook/Exchange Messages, Notes, Contacts, Appointments, and Tasks, Microsoft Outlook Express 5 and 6 (*.dbx) message stores, Microsoft PowerPoint (*.ppt), Microsoft PowerPoint 2007, 2010, and 2013 (*.pptx), Microsoft Rich Text Format (*.rtf), Microsoft Searchable Tiff (*.tiff), Microsoft Visio (*.vsd, *.vst, *.vss, *.vdw, *.vsdx, *.vssx, *.vstx, *.vsdm, *.vssm, *.vstm), Microsoft Word for DOS (*.doc), Microsoft Word for Windows (*.doc), Microsoft Word 2003 XML (*.xml), Microsoft Word 2007, 2010, and 2013 (*.docx), Microsoft Works (*.wks), MP3 (metadata only) (*.mp3), Multimate Advantage II (*.dox), Multimate version 4 (*.doc), OpenOffice versions 1, 2, and 3 documents, spreadsheets, and presentations (*.sxc, *.sxd, *.sxi, *.sxw, *.sxg, *.stc, *.sti, *.stw, *.stm, *.odt, *.ott, *.odg, *.otg, *.odp, *.otp, *.ods, *.ots, *.odf) (includes OASIS Open Document Format for Office Applications), Quattro Pro (*.wb1, *.wb2, *.wb3, *.qpw), QuickTime (*.mov, *.m4a, *.m4v), RAR (*.rar), TAR (*.tar), TIFF (metadata only) (*.tif), TNEF (winmail.dat), Treepad HJT files (*.hjt), Unicode (UCS16, Mac or Windows byte order, or UTF-8), Visio XML files (*.vdx), Windows Metafile Format (*.wmf), WMA media files (metadata only) (*.wma), WMV video files (metadata only) (*.wmv), WordPerfect 4.2 (*.wpd, *.wpf), WordPerfect (5.0 and later) (*.wpd, *.wpf), WordStar version 1, 2, 3 (*.ws), WordStar versions 4, 5, 6 (*.ws), WordStar 2000, Write (*.wri), XBase (including FoxPro, dBase, and other XBase-compatible formats) (*.dbf), XML (*.xml), XML Paper Specification (*.xps), XSL, XyWrite, ZIP (*.zip) as well as PostScript, PCL5, PCL6 (PCL XL), HP-GL/2, EMF spooled files and GDI printing (ZjStream).

> **Note:** Content in AutoCAD (DWG, DXF) file formats can be identified on Windows XP and later systems.

Continuous protection. You can apply content-based security policies to your entire network periodically with scheduled scans.

Multiple content detection methods. You can use multiple methods to identify sensitive content contained in documents (based on regular expressions, keywords, and document properties).

Centralized content management. Flexible, content-aware Rules and Actions are managed based on content groups that enable you to centrally define types of content types that you want to control.

Ability to override access rights. You can selectively allow or deny access to certain content stored on network computers regardless of preset permissions.

Inspection of files within archives. Allows you to perform deep inspection of each individual file contained in an archive. The following inspection algorithm is used: when a compressed archive is detected, all files are extracted from the archive and analyzed individually to detect the content to which to apply the actions defined in Rules and Actions. If the content of at least one file from the archive gets a positive match in the Rules and Actions section, DeviceLock Discovery will apply the corresponding rule or action to the entire archive.

All nested archives are also unpacked and analyzed one by one. Archive files are detected by content, not by extension. The following archive formats are supported: 7z (.7z), ZIP (.zip), GZIP (.gz, .gzip, .tgz), BZIP2 (.bz2, .bzip2, .tbz2, .tbz), TAR (.tar), RAR (.rar), CAB (.cab), ARJ (.arj), Z (.z, .taz), CPIO (.cpio), RPM (.rpm), DEB (.deb), LZH (.lzh, .lha), CHM (.chm, .chw, .hxs), ISO (.Iso), UDF (.Iso), COMPOUND (.Msi), WIM (.wim, .swm), DMG (.dmg), XAR (.xar), HFS (.hfs), NSIS (.exe), XZ (.xz), MsLZ (.mslz), VHD (.vhd), FLV (.flv), SWF (.swf) as well as CramFS, SquashFS (.squashfs), NTFS, FAT and MBR file system and disk images. Split (or multi-volume) and password-protected archives are not unpacked.

Optical Character Recognition (OCR). The use of the OCR technology allows you to recognize and extract text from scanned documents, camera-captured documents (if these documents were aligned 90 degrees to the camera), and screen shots of documents for further content analysis by Content-Aware Rules.

OCR includes the following capabilities:

- An entire image or some portions of the image can be inverted, rotated, or mirrored.
- Images with poor brightness or low contrast are supported.
- Most fonts can be accurately recognized.

OCR has the following limitations:

- Recognition of handwritten text or any fonts that look like handwritten text is not supported.
- Embossed and engraved texts are not recognized.
- Best recognition results are achieved for black text on a white background.

The built-in OCR supports the following languages: Arabic, Bulgarian, Catalan, Chinese - Simplified, Chinese - Traditional, Croatian, Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Hungarian, Indonesian, Italian, Japanese, Korean, Latvian, Lithuanian, Norwegian, Polish, Portuguese, Romanian, Russian, Slovak, Slovenian, Spanish, Swedish, and Turkish. The following image files are supported for OCR processing: BMP files, Dr. Halo CUT files, DDS files, EXR files, Raw Fax G3 files, GIF files, HDR files, ICO files, IFF files (except Maya IFF files), JBIG files, JNG files, JPEG/JIF files, JPEG- 2000 files, JPEG-2000 codestream files, KOALA files, Kodak PhotoCD files, MNG files, PCX files, PBM/PGM/PPM files, PFM files, PNG files, Macintosh PICT files, Photoshop PSD files, RAW camera files, Sun RAS files, SGI files, TARGA files, TIFF files, WBMP files, XBM files, and XPM files.

> **Note:** The OCR feature is only supported on Windows XP and later versions of Windows.

Text in picture detection. The use of the text-in-picture detection technology allows you to classify all images into two groups: text images (containing text, such as scanned documents or screen shots of documents) and non-text images (those that don't contain text). Timely identifying text images helps prevent or investigate leakage of sensitive information within image files. The following image files are supported: BMP files, Dr. Halo CUT files, DDS files, EXR files, Raw Fax G3 files, GIF files, HDR files, ICO files, IFF files (except Maya IFF files), JBIG files, JNG files, JPEG/JIF files, JPEG-2000 files, JPEG-2000 codestream files, KOALA files, Kodak PhotoCD files, MNG files, PCX files, PBM/PGM/PPM files, PFM files, PNG files, Macintosh PICT files, Photoshop PSD files, RAW camera files, Sun RAS files, SGI files, TARGA files, TIFF files, WBMP files, XBM files, XPM files.

Inspection of images embedded in documents. Allows you to perform deep inspection of each individual image embedded in Adobe Portable Document Format (including encrypted files if the type of encryption in the file is one of the following: 40-bit RC4, 128-bit RC4, 128-bit AES and 256-bit AES, and the file permissions do not disable text extraction) (PDF) files, Rich Text Format (RTF), AutoCAD files (.dwg, .dxf), and Microsoft Office documents (.doc, .xls, .ppt, .vsd, .docx, .xlsx, .pptx, .vsdx). All embedded images are extracted from these documents to the Temp folder of the System user and analyzed independently from text. The text contained inside documents is checked against the list of Rules and Actions that are created based on Keywords, Pattern or Complex content groups. Embedded images are checked against Rules and Actions that are created based on File Type Detection, Document Properties or Complex content groups. The appropriate action will be applied to the entire document if either its text or any of the images contained in the document have a match in the Rules and Actions list.

Note: Deep inspection of images embedded in files of AutoCAD (DWG, DXF) formats can be performed on Windows XP and later systems only.

How DeviceLock Discovery Works

DeviceLock Discovery can scan remote computers by using one of the three methods.

1. DeviceLock Discovery can scan remote computers via the SMB protocol (network shares).

2. Alternatively, DeviceLock Discovery can perform the scanning via its own lightweight agent (DeviceLock Discovery Agent).

3. Finally, DeviceLock Discovery can scan remote computers by using a lightweight agent built into DeviceLock Service.

Depending upon a particular network configuration and system requirements, administrators may choose one or the other method.

SMB access is the easiest to deploy. Requiring neither DeviceLock software installation nor configuration for each local target endpoint, SMB access is a perfect method for remote background scanning of network shares on NAS devices, as well as files servers and other computers running any operating systems including those not directly supported by DeviceLock.

Discovery Server   Scan via SMB   SMB resources
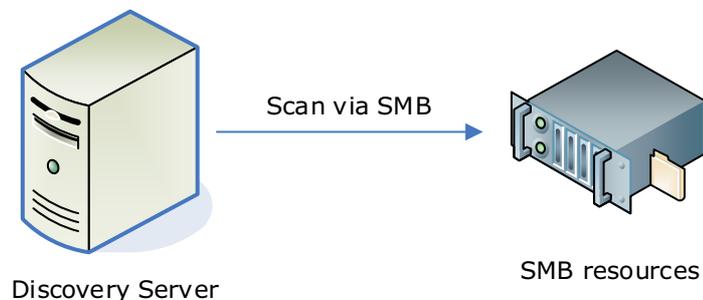
Using the **DeviceLock Discovery Agent** is ideal for scanning computers that have no DeviceLock Service installed. This method will require the deployment of the DeviceLock Discovery Agent throughout all computers to be scanned.
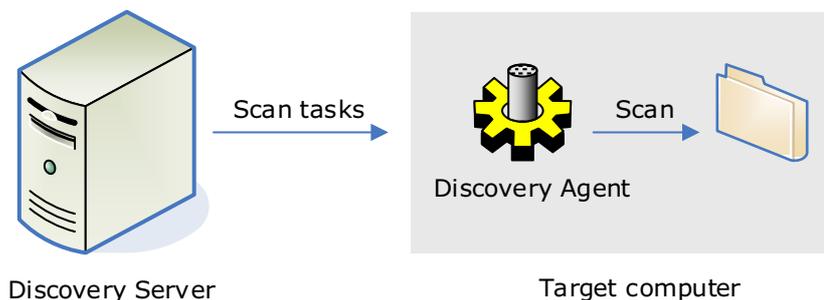
Leveraging the **DeviceLock Service** is a perfect solution for customers already using DeviceLock. As this method uses the existing installations of the DeviceLock Service, no additional deployment is required. However, this method will only scan Windows-based computers with DeviceLock Service already installed, and will neither be able to scan Mac computers nor computers and networks devices with unsupported operating systems such as NAS devices.
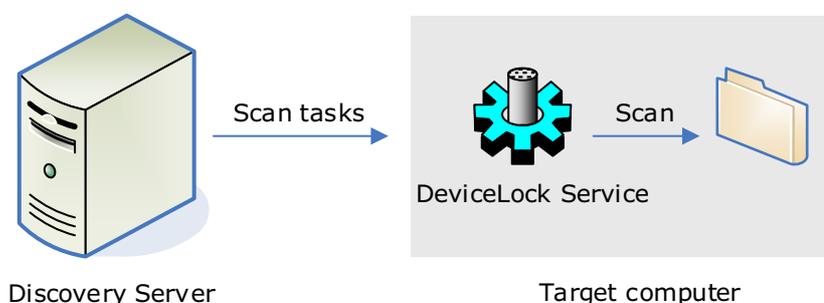
DeviceLock Discovery can be configured to perform certain actions on files being discovered. For example, it can be configured to delete or encrypt a certain file, modify its access rights, send an alert to an administrator, log the event or notify the user of the computer being scanned.

The results and logs are kept in a centralized SQL Server database. An HTML report is generated and kept in the same database. By analyzing the report, administrators can get a clear understanding on search results and review the findings of any content discovered by DeviceLock Discovery. The report is created every time a scanning task finishes.

Scan agent system requirements

Computers to scan by the DeviceLock Discovery Agent must meet the following requirements:

Operating System	Microsoft Windows 2000/XP/Vista/7/8/8.1/10 and Windows Server 2003/2003 R2, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019 Installation is supported on both the 32-bit and the 64-bit editions of the operating system.
RAM	Minimum: 512 MB
Hard Disk Space	Minimum: 200 MB
Processor Type	Minimum: Intel Pentium 4

Computers to scan by the DeviceLock Service must meet the following requirements:

Operating System for DeviceLock Service for Windows	Microsoft Windows NT 4.0 SP6/2000/XP/Vista/7/8/8.1/10 and Windows Server 2003/2003 R2, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019 Installation is supported on both the 32-bit and the 64-bit editions of the operating system.
RAM	Minimum: 512 MB
Hard Disk Space	Minimum: 400 MB
Processor Type	Minimum: Intel Pentium 4
Supported Virtualization Products	Microsoft Remote Desktop Services (RDS), Citrix XenDesktop/XenApp, Citrix XenServer, VMware Horizon View, VMware Workstation, VMware Player, Oracle VM VirtualBox, Windows Virtual PC

Licensing

DeviceLock Discovery is licensed separately from DeviceLock DLP.

If you want to use the capabilities of DeviceLock Discovery, you must purchase DeviceLock Discovery licenses. DeviceLock Discovery is licensed on per computer basis. A license is required for each computer or network device scanned with DeviceLock Discovery, regardless of whether the system is set to scan the entire computer or a single folder.

The trial period for DeviceLock Discovery is 30 days. A maximum of two computers can be scanned with the evaluation version.

Installing DeviceLock Discovery

In this chapter:

To install DeviceLock Discovery, the administrator needs to install the DeviceLock Content Security Server (for instructions, see Installing DeviceLock Content Security Server) along with a license for DeviceLock Discovery (see Installing DeviceLock Discovery licenses later in this document).

The DeviceLock Management Console is required to administer and use DeviceLock Discovery. For the console installation instructions, see Installing Management Consoles in the DeviceLock User Manual at www.devicelock.com/support/docs.html.

Installing DeviceLock Content Security Server

This section covers the steps to install DeviceLock Content Security Server:

1. Prepare for Installation
2. Start Installation
3. Perform Configuration and Complete Installation

Prepare for Installation

Before you install DeviceLock Content Security Server, consider the following:

- The DeviceLock Content Security Server setup program installs two DeviceLock components: Search Server and Discovery Server.

- The computer on which you install DeviceLock Content Security Server must meet the following system requirements:

Operating System	Microsoft Windows Server 2003/2003 R2, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019
	Installation is supported on both the 32-bit and the 64-bit editions of the operating system.
SQL Server	Microsoft SQL Server 2005, 2008, 2008 R2, 2012, 2014 or 2016, any edition, including SQL Server Express.
	Important: SQL Server is required for the Search Server and Discovery Server to function (for more information, see Database Settings).
Hard Disk Space	Minimum: 1 GB.
	Recommended: 800 GB (if an SQL database is used).

- You must have administrator permissions to install DeviceLock Content Security Server.

- For optimal performance and reliability, we recommend that you install DeviceLock Enterprise Server and DeviceLock Content Security Server on different computers.

- There is a special Search Server license which you must purchase for DeviceLock Content Security Server. You can use the same license on an unlimited number of computers running DeviceLock Content Security Server. The Search Server licensing model is based on the number of log entries to be indexed for full-text search. Each license allows Search Server to index 1,000 entries from the shadow logs (Shadow Log and Deleted Shadow Data Log), and 5,000 entries from every other log (Audit Log, Server Log, Monitoring Log, and Policy Log). Depending on the actual number of log entries on your DeviceLock Enterprise Servers, you can purchase as many licenses as required. If you use several licenses for Search Server, it can index as many log entries as the combined licenses allow. The trial period for DeviceLock Content Security Server is 30 days. During the trial period, Search Server can index 2,000 entries from the shadow logs and 10,000 entries from every other log.

- There is a special DeviceLock Discovery license which you must purchase for DeviceLock Content Security Server. A license is required for each computer or network device scanned with DeviceLock Discovery, regardless of whether the system is set to scan the entire computer or a single folder. The trial period for DeviceLock Discovery is 30 days. The maximum of two computers can be scanned with the evaluation version.

- In case you have several DeviceLock Enterprise Servers on your network, you can also install several DeviceLock Content Security Servers to spread the load.

- When you have several DeviceLock Content Security Servers installed each Search Server will have its own search index. Hence, you have to connect to every DeviceLock Content Security Server and run the same search queries on every Search Server in order to get the complete result set from all the data stored on all DeviceLock Enterprise Servers.

- There are two scenarios for connecting DeviceLock Discovery Server and MS SQL Server. You should decide which scenario best fits your needs before installing the product. DeviceLock Discovery Server supports ONE-TO-ONE and MANY-TO-MANY modes:

   1. **ONE-TO-ONE**: You install one DeviceLock Content Security Server and connect it to one Microsoft SQL Server. This scenario is most appropriate for small networks (up to several hundreds of computers).

   2. **MANY-TO-MANY**: You install several DeviceLock Content Security Servers and connect each of them to its own Microsoft SQL Server. This scenario is typical for medium and large networks geographically distributed across a variety of segments.

- We strongly recommend that you exit all Windows programs before you start Setup.

Start Installation

Use this procedure to begin the installation process.

To start installation

1. Open the **DeviceLock.zip** file, and then double-click the **setup_dlcss.exe** file to start the Setup program.

   You must run the Setup program on each computer on which you want to install DeviceLock Content Security Server.

2. Follow the instructions in the Setup program.

3. On the **License Agreement** page, read the License Agreement and then click **I accept the terms in the license agreement** to accept the licensing terms and conditions and proceed with the installation.

4. On the **Customer Information** page, type your user name and organization, and then click **Next**.

5. On the **Destination Folder** page, accept the default installation folder or click **Change** to modify the path as needed. Click **Next**.

   The default installation folder is `%ProgramFiles%\DeviceLock Content Security Server` on 32-bit Windows or `%ProgramFiles(x86)%\DeviceLock Content Security Server` on 64-bit Windows.

6. On the **Ready to Install the Program** page, click **Install** to begin the installation.

   The DeviceLock Content Security Server configuration wizard starts.

   If you are installing an upgrade or simply reinstalling DeviceLock Content Security Server, and want to keep its current configuration, you do not need to go through the configuration wizard again - just click **Next** and then **Cancel** to close the wizard and keep all existing settings unchanged.

   In case you need to change some parameters but keep others - edit only needed parameters and go through all the configuration wizard's pages up to the **Finish** button on the final page.

   Note: If you are installing Content Security Server for the first time (there are no existing settings on this computer yet) and you cancel the configuration wizard, Setup will not be able to install DeviceLock Content Security Server's service, so you will need to run the configuration wizard again.

Perform Configuration and Complete Installation

The configuration wizard opens automatically during the installation process. This wizard provides the following pages that help you configure DeviceLock Content Security Server:

- Service Account and Connection Settings
- Server Administrators and Certificate
- License Information
- Database Settings
- Completing Configuration

Service Account and Connection Settings

On this page, you configure startup options for the DeviceLock Content Security Server service.
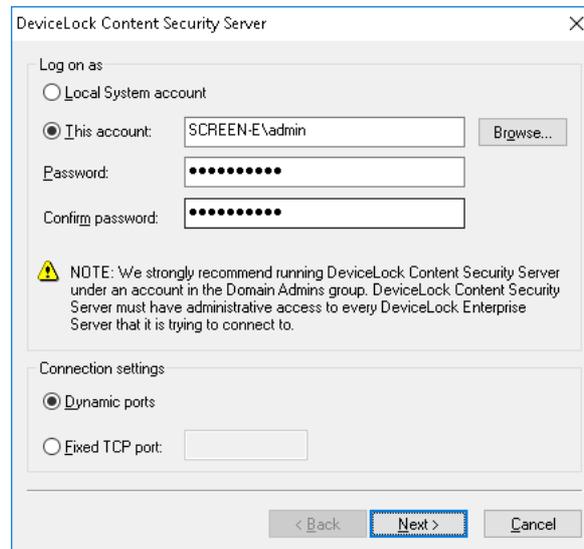
Log on as

First of all, you should choose an account under which the DeviceLock Content Security Server service will start. As with many other Windows services, the DeviceLock Content Security Server service can start under the special local system account (the SYSTEM user) and on behalf of any user.

To start the service under the SYSTEM user, select the **Local System account** option. Keep in mind that the process working under the SYSTEM user cannot access shared network resources and authenticates on remote computers as an anonymous user. Therefore, DeviceLock Content Security Server configured to run under the SYSTEM user is not able to access DeviceLock Enterprise Server running on the remote computer and it must use DeviceLock Certificate for authentication on it.

For more information about authentication methods, see description of the Certificate Name parameter.

> **Important:** If the DeviceLock Content Security Server service is configured to run under the Local System account, DeviceLock Discovery Server cannot install or remove DeviceLock Discovery Agents on remote computers.

To start the service on behalf of the user, select the **This account** option, enter the user's account name and the password. It is recommended to use a user account that has administrative privileges on all the computers where DeviceLock Enterprise Server is running. Otherwise, you will need to use DeviceLock Certificate authentication.

If you are installing DeviceLock Content Security Server in the domain environment, we recommend that you use a user account that is a member of the Domain Admins group. Since Domain Admins is a member of the local group Administrators on every computer in the domain, members of Domain Admins will have full access to every computer.

Also, do not forget that if **Default Security** is disabled on:

- DeviceLock Enterprise Server that runs remotely, the user account specified in the **This account** option must be also in the list of server administrators with at least **Read-only** level of access on that DeviceLock Enterprise Server. Otherwise, the DeviceLock Certificate authentication needs to be used.

- DeviceLock Service that runs remotely, the user account specified in the **This account** option must be also in the list of DeviceLock administrators with at least **Read-only** access rights on that DeviceLock Service. Otherwise, the DeviceLock Certificate authentication should be used or explicit credentials should be specified in the respective DeviceLock Discovery unit.

Connection settings

You can instruct DeviceLock Content Security Server to use a fixed TCP port for communication with the management console, making it easier to configure a firewall. Type the port number in **Fixed TCP port**. To use dynamic ports for RPC communication, select the **Dynamic ports** option. By default, DeviceLock Content Security Server uses port 9134.

Click **Next** to start the DeviceLock Content Security Server service and to proceed to the second page.

Starting the Service

If the current user does not have full administrative access to DeviceLock Content Security Server (in case it already exists and you're installing an upgrade), the configuration wizard will not be able to install the service and apply changes. The following message will appear: "Access is denied." Also, a similar error may occur when the current user does not have local administrative privileges on the computer where DeviceLock Content Security Server is installing.

If you have specified an incorrect user name for the **This account** option or the wrong user password, DeviceLock Content Security Server will not be able to start. The following message will appear: "The account name is invalid or does not exist, or the password is invalid for the account name specified."

You will be notified if the user's account specified for the **This account** option is not a member of the Domain Admins group. The following message will appear: "The account <name> does not belong to the Domain Admins group. Do you want to continue?"

You may continue by clicking **Yes**. However, make sure that either of the following is true.

For Search Server:

- The specified user has administrative access to all remotely running DeviceLock Enterprise Servers

    - OR -

- DeviceLock Certificate (private key) is installed on every computer running DeviceLock Enterprise Server

For DeviceLock Discovery Server:

- The specified user has administrative access to all computers scanned by DeviceLock Discovery Server. This includes computers running DeviceLock Services, DeviceLock Discovery Agents, as well as any computers not having the Agent installed.

    - OR -

- DeviceLock Certificate (public key) is installed on every computer (with DeviceLock Service) scanned by DeviceLock Discovery Server

    - OR -

- Credentials for accessing remote computers are specified in the scanning settings.

If the user's account specified for the **This account** option does not have the "Log On As A Service" system privilege, the wizard automatically assigns it. This privilege is needed to start the service on behalf of the user. The following message will appear: "The account <name> has been granted the Log On As A Service right."

If all of the service's startup parameters were specified correctly, the wizard starts DeviceLock Content Security Server. The following message will appear: "Please wait while the program is interacting with a service. Starting service DLCSS on Local Computer…"

It takes some time (up to a minute) before the DeviceLock Content Security Server service is started and the next page of the wizard is displayed.

Server Administrators and Certificate

On this page of the wizard, you can set up the list of users that have administrative access to DeviceLock Content Security Server, and install DeviceLock Certificate (the private key) if needed.
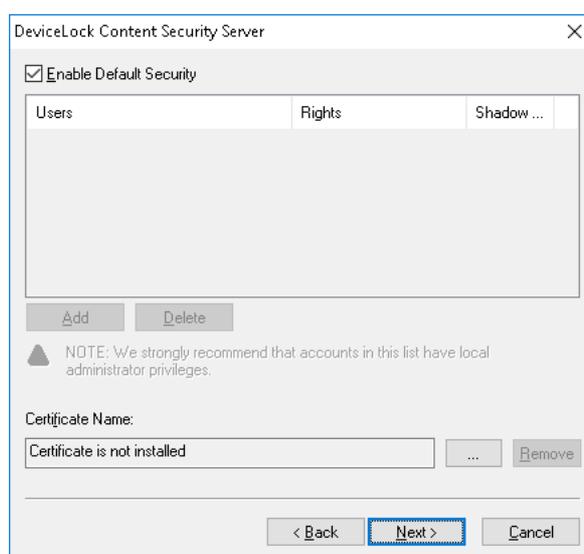
Enable Default Security

In the default security configuration all users with local administrator privileges (i.e. members of the local Administrators group) can connect to DeviceLock Content Security Server using a management console, change its settings, run search queries, configure content detection settings, and run discovery tasks.

To turn on the default security, select the **Enable Default Security** check box.

If you need to define more granular access to DeviceLock Content Security Server, turn off the default security by clearing the **Enable Default Security** check box.

Then you need to specify authorized accounts (users and/or groups) that can connect to DeviceLock Content Security Server. To add a new user or group to the list of accounts, click **Add**. You can add several accounts simultaneously.

To delete a record from the list of accounts, use the **Delete** button. Using Ctrl and/or Shift you can highlight and remove several records simultaneously.

To determine the actions allowed to a user or group, select the desired level of access to the server:

- **Full access** - Allows the user or group to install and uninstall DeviceLock Content Security Server, connect to it by using DeviceLock Management Console, and perform any actions on the server, such as: view and change server settings; create and run search queries and tasks; view and change content detection settings; create and run discovery tasks and reports.

- **Change** - Same as full access to the server with the exception of the right to make changes to the list of server administrators or change the level of access to the server for the users or groups already in that list.

- **Read-only** - Allows the user or group to connect to DeviceLock Content Security Server by using DeviceLock Management Console; view server settings; run search queries; view and run existing search tasks; view content detection settings; view discovery reports and manually create new reports based on the existing reports and data already prepared by discovery tasks. This option does not give the right to run discovery tasks, make any changes on the server, or create a new index for the Search Server.

For users and groups with the Change or Read-only level of access, the **Shadow Data Access** option can be selected to allow access to shadowed data. The users and groups that have this option selected can open, view and download shadow data on a search results page or search report, and search inside of shadowed files.

> **Important:** We strongly recommend that the accounts designated as server administrators be given local administrator rights because, in some instances, installing, updating and uninstalling DeviceLock Content Security Server may require access to Windows Service Control Manager (SCM) and shared network resources.

Certificate Name

You may need to deploy the private key to DeviceLock Content Security Server if you want to enable authentication based on DeviceLock Certificate.

There are two methods of DeviceLock Search Server authentication on a remotely running DeviceLock Enterprise Server:

- **User authentication** - The DeviceLock Content Security Server service is running under the user's account that has administrative access to DeviceLock Enterprise Server on the remote computer. For more information on how to run DeviceLock Content Security Server on behalf of the user, please read the description of the Log on as parameter.

- **DeviceLock Certificate authentication** - In situations where the user under which the DeviceLock Content Security Server service is running cannot access DeviceLock Enterprise Server on the remote computer, you must authenticate based on a DeviceLock Certificate.

  The same private key should be installed on DeviceLock Enterprise Server and on DeviceLock Content Security Server.

There are three methods of DeviceLock Discovery Server authentication when scanning a remote computer:

- **User authentication** - The DeviceLock Content Security Server service is running under a certain user account, and these credentials are used to access remote computers being scanned. These credentials will be supplied to either DeviceLock Service, DeviceLock Discovery Agent, or the remote computer if scanning is performed without an agent. For more information on how to run DeviceLock Content Security Server on behalf of a user, please read the description of the Log on as parameter.

- **Alternative credentials authentication** - The DeviceLock Content Security Server service is running under a user account that has administrative privileges at least on the local computer. DeviceLock Discovery Server will use alternative credentials to log in to remote computer being scanned.

- **DeviceLock Certificate authentication** - Authentication based on a DeviceLock Certificate is used to authenticate on remote computers running DeviceLock Service with the certificate's public key installed.

To install DeviceLock Certificate, click the ⋯ button, and select the file containing the certificate's private key. To remove DeviceLock Certificate, click **Remove**.

Click **Next** to apply changes and proceed to the next page of the configuration wizard.

License Information

On this page, you can install your licenses for Search Server and/or DeviceLock Discovery. Search Server and DeviceLock Discovery are licensed separately. The trial period is 30 days.
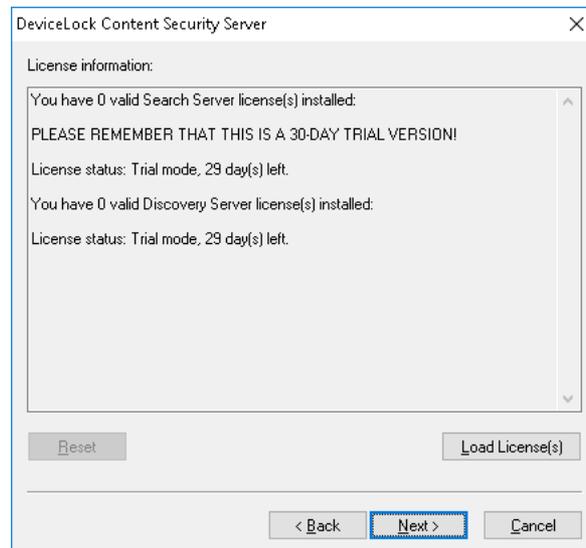
To install a license, click **Load License(s)** and select the license file. You can load several license files in series - one by one. The **License information** box displays summary information about the licenses you're installing.

After Content Security Server has been installed, you can use the DeviceLock Management Console to install a license or view the current license information, including the number of installed licenses and the number of used licenses for Search Server and/or DeviceLock Discovery.

Click **Next** to proceed to proceed to configuring the database.

Database Settings

On this page, the wizard prompts you to configure database parameters.

Important: Do not skip this page, as a database is required for the Search Server and Discovery Server to function. Without a database, it is impossible to search using content-aware groups, save and automate search queries, or use the Discovery Server for content discovery.

Database name

View or change the name of the database for DeviceLock Content Security Server. The default name suggested by the wizard is **DLCSSDB**.

Note: You should not create a database with the specified name manually because the configuration wizard creates the database automatically or uses the existing one.

Connection type

There are two ways to define a connection to SQL Server:

1. **ODBC Driver** - You enter the name of SQL Server in **SQL Server name** and select the authentication mode (Windows or SQL Server).

   The **SQL Server name** parameter must contain not just the name of the computer where SQL Server is running but the name of SQL Server itself. Usually the SQL Server name consists of two parts: the computer name and the instance name divided by a backslash (e.g. computer\instance). Sometimes the instance name is empty (default) and you can use the computer name as an SQL Server name. To retrieve SQL Server names available in your local network, press the **Browse** button. (You should have access to the remote registry of the SQL Server machine to retrieve the instance name.)

   If the **SQL Server name** parameter is empty, it means that SQL Server is running on the same computer as DeviceLock Content Security Server and has an empty (default) instance name.

   To establish a connection to SQL Server, you must also configure authentication parameters.

   Select the **Windows authentication** option to authenticate on SQL Server under the account used to run DeviceLock Content Security Server's service.

If the service is running under the SYSTEM account and SQL Server is located on the remote computer, service will not be able to connect to SQL Server since the SYSTEM account doesn't have a right to access the network. For more information on how to run DeviceLock Content Security Server on behalf of a user, see the description of the Log on as parameter.

Select the **SQL Server authentication** option to allow SQL Server to perform the authentication itself by checking the login and password previously defined. Before selecting the **SQL Server authentication** option, make sure that your SQL Server was configured to use mixed-mode authentication. Enter the SQL user name (login) in **Login name** and its password in **Password**.

> **Note:** Windows Authentication is much more secure than SQL Server Authentication. When possible, you should use Windows Authentication.

2. **System Data Source** - You select the predefined system data source from the **Data Source Name** list.

   To define data sources, use **ODBC Data Source Administrator** from **Control Panel** > **Administrative Tools**.
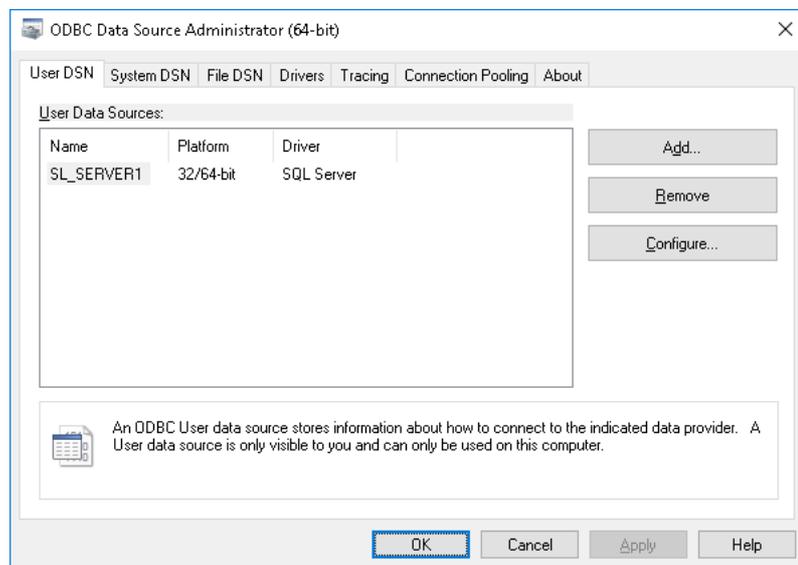
If, in the data source configuration, SQL Server Authentication was chosen, then you also need to specify the SQL user name (login) in **Login name** and its password in **Password**. If Windows Authentication was selected, then you should leave these fields blank.

To refresh the **Data Source Name** list, press the **Refresh** button.

Test Connection

When connection to SQL Server is defined you may want to test it. Click the **Test Connection** button to make sure that all the parameters were specified correctly.

Please note that it only checks connectivity and your access rights to SQL Server. If there are problems with the database or your access rights to this database, you don't see those problems in the **Test Connection** dialog box.
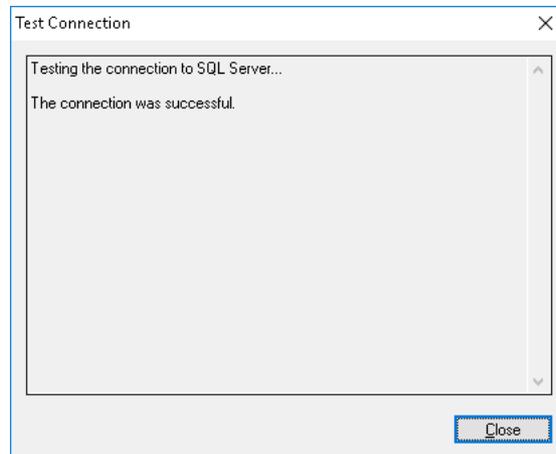
If some connection parameters were specified incorrectly, you may see one of these errors:

- **SQL Server does not exist or access denied** - An incorrect SQL Server name is specified in the **SQL Server name** parameter or the remote SQL Server's computer is not accessible. It is possible that you've specified the name of the computer where SQL Server is running but this SQL Server also has an instance name which should be specified as well (e.g. computer\instance).

- **Login failed for user 'COMPUTER_NAME$'** - Windows Authentication is selected but the user account used to run the DeviceLock Content Security Server service can't get access to the computer with SQL Server. It may happen when the service starts either under the SYSTEM user or on behalf of a user that doesn't have local administrative privileges on the remote SQL Server's computer.

- **Login failed for user 'user_name'** - SQL Server Authentication is selected with either an incorrect SQL user name (login) or wrong password specified. Please note that SQL users are different from Windows users and you can't use the regular Windows account in the **Login name** parameter. SQL users exist only in SQL Server and to manage them you should use SQL Server management consoles (such as Microsoft SQL Server Management Studio).

- **Login failed for user 'user_name'. The user is not associated with a trusted SQL Server connection** - SQL Server Authentication is but your SQL Server doesn't support this mode. You should either use Windows Authentication or allow your SQL Server to work in the mixed mode (SQL Server and Windows Authentication mode).

- **Login failed for user ''. The user is not associated with a trusted SQL Server connection** - The data source specified in **Data Source Name** is configured to use the SQL Server Authentication mode but the **Login name** parameter is empty.

- **Data source name not found and no default driver specified** - You've selected **System Data Source** from the **Connection type** list and specified either an empty or non-existent name in **Data Source Name**.

Press the **Next** button to apply changes and proceed to the last page.

Completing Configuration

It takes some time to create the database specified in **Database name** if it does not exist on this SQL Server yet. If the database already exists and it has the proper format (i.e. was created by DeviceLock) then DeviceLock Content Security Server keeps all existing data and uses this database. If necessary, DeviceLock automatically updates the database to the latest version.
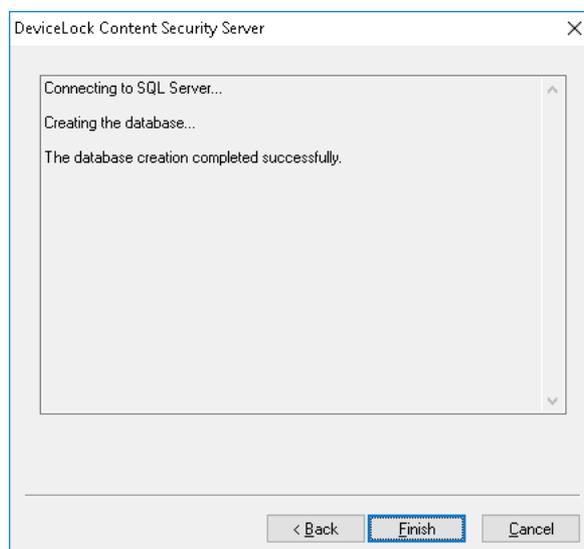
On this page of the configuration wizard you can observe the applying of the database settings specified, and view errors that might occur when configuring the database.

If some parameters on the previous page of the wizard were specified incorrectly, you might encounter the following errors:

- **CREATE DATABASE permission denied in database 'name'** - The user account (login) used to connect to SQL Server doesn't have sufficient rights to create the database. The login should have at least the dbcreator Server role (see **Server Roles** in **Login Properties** of Microsoft SQL Server Management Studio).

- **The server principal "user_name" is not able to access the database "name" under the current security context** - The user account (login) used to connect to SQL Server doesn't have access to the existing database. The login should be mapped to this database (see **User Mapping** in **Login Properties** of Microsoft SQL Server Management Studio).

- **SELECT permission denied on object 'name', database 'name', schema 'name'** - The user account (login) used to connect to SQL Server doesn't have read/write access to the existing database. The login should have at least db_datareader and db_datawriter Database roles (see **User Mapping** in **Login Properties** of Microsoft SQL Server Management Studio).

- **Invalid object name 'name'** - The database specified in the **Database name** parameter already exists on this SQL Server but has an incorrect format. It happens when you are trying to use the database that was not created by DeviceLock Content Security Server or if the database was corrupted.

- **DeviceLock Database has an unsupported format** - The database specified in the **Database name** parameter already exists but is outdated. This existing database has an unsupported format so it can't be automatically upgraded to the new format. You should either use another database or create a new one.

- **DeviceLock Database has a format that is not supported by the current server version** - The database specified in the **Database name** parameter already exists but it was created by the more recent version of DeviceLock Content Security Server. You should either use the latest version of DeviceLock Content Security Server or use another database (or create a new one).

Also, the wizard might display some of the SQL Server connection errors listed in the Test Connection section earlier in this document.

Use the **Back** button to return to the previous page of the wizard and make necessary changes.

If there are no errors, click the **Finish** button to close the wizard and continue the installation process.

Next, on the **Installation Wizard Completed** page, click **Finish** to complete the installation. On this page, you will have the option to go to the DeviceLock home page. This option is selected by default.

> **Note:** You can uninstall DeviceLock Content Security Server as follows:
> - Use **Programs and Features** in Control Panel (**Add or Remove Programs** on earlier versions of Windows) to remove **DeviceLock Content Security Server**,
>   - OR -
> - Select **Remove DeviceLock Content Security Server** on the Windows **Start** menu.

Setting Up Discovery Server

In this chapter:

Navigating Discovery Server

Before addressing the functionality of DeviceLock Discovery Server, you need to examine how to perform basic navigation. Use the **DeviceLock Content Security Server** node in DeviceLock Management Console to configure and use DeviceLock Content Security Server.
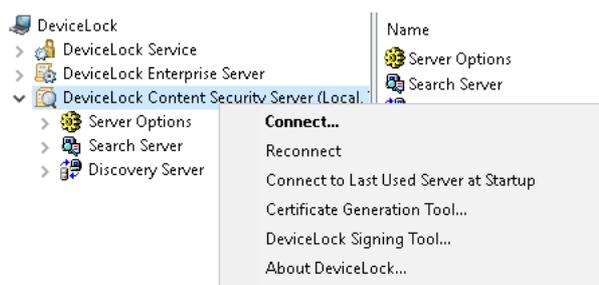
Right-click the **DeviceLock Content Security Server** node to display the following commands:

- **Connect** - Connects to the computer running DeviceLock Discovery Server.

  For detailed description of this command, refer to the Connecting to Computers section in the DeviceLock User Manual at www.devicelock.com/support/docs.html.

  When you connect to a computer where an old version of DeviceLock Discovery Server is installed, you may receive the following message: "The product version on the client and server machines does not match." In this case, you need to install the new version of DeviceLock Discovery Server on this computer. For installation instructions, refer to the Installing DeviceLock Discovery section.

- **Reconnect** - Connects to the currently connected computer once again.

- **Connect to Last Used Server at Startup** - Check this command to instruct DeviceLock Management Console to automatically connect to the last used server each time the console starts up.

- **Certificate Generation Tool** - Starts a tool for generating DeviceLock Certificates. For details, refer to the Generating DeviceLock Certificates section in the DeviceLock User Manual at www.devicelock.com/support/docs.html.

- **DeviceLock Signing Tool** - Starts a tool to grant users temporary access to devices and to sign files containing DeviceLock Service settings. For details, refer to the DeviceLock Signing Tool section in the DeviceLock User Manual at www.devicelock.com/support/docs.html.

- **About DeviceLock** - Displays the dialog box with information about the DeviceLock version and your licenses.

Expand the **DeviceLock Content Security Server** node, and select the **Server Options** node:
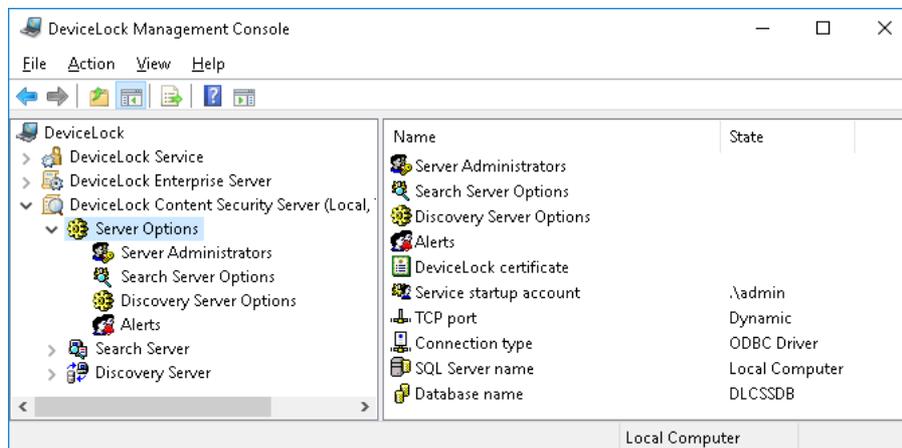
You can use this node to configure the following common settings for DeviceLock Search Server and Discovery Server:

- **Server Administrators** - Use this setting to specify members of the Server Administrators group and their associated access rights.

- **Search Server Options** - Use this option to configure settings related to full-text search.

- **Discovery Server Options** - Use this option to configure settings related to content discovery.

- **Alerts** - Use this option to configure delivery settings for alerts.

- **DeviceLock certificate** - Use this setting to install, change or remove the DeviceLock Certificate pair.

- **Service startup account** - Use this setting to specify the startup account information, such as the account name and the password, for the server service.

- **TCP port** - Use this setting to specify the TCP port that the DeviceLock Management Console uses to connect to the server.

- **Connection type** - Use this setting to specify how DeviceLock Content Security Server connects to the database. Available options include **ODBC Driver** and **System Data Source**.

- **SQL Server name** - Use this setting to specify the name of SQL Server used by DeviceLock Content Security Server.

- **Database name** - Specifies the name of the database in SQL Server that is used to store the DeviceLock Search Server and Discovery Server data.

- **SQL Server login** - Use this setting to specify the login and password for the SQL Server Authentication mode.

Expand the **Server Options** node and select the **Discovery Server Options** node. You can use this node to configure the following settings specific to DeviceLock Discovery Server:

- **DeviceLock Enterprise Server(s)** - Use this setting to specify one or more DeviceLock Enterprise Servers that host the fingerprints database.

- **Discovery Server license(s)** - Use this setting to install the required number of DeviceLock Discovery licenses.

- **Log options** - Use this setting to specify event logging options for Discovery Server. Enables you to configure the types of events to be logged.

- **E-Mail Message for Alerts** - Use this setting to configure the template of e-mail messages used to alert administrators about discovered content.

- **Syslog Message for Alerts** - Use this setting to configure the syslog message template of alerts.

- **Discovery notification message** - Use this setting to configure the template of a tray notification message shown to the currently logged in users when a discovery event occurs.

- **Data collection interval** - Use this setting to specify the interval of collecting data from discovery agents.

- **Oracle IRM Server Settings** - Use this setting to configure DeviceLock Discovery Server for Oracle IRM support.

- **Binary files content inspection** - Use this setting to enable keywords- and pattern-based content discovery for text held in arbitrary binary files.

General Settings

There are three types of configuration settings for the DeviceLock Content Security Server:

- **General settings** - Affect the operation of the DeviceLock Content Security Server as a whole. The current section provides instructions for managing these settings.

- **Search Server settings** - Affect the operation of the Search Server, a part of the DeviceLock Content Security Server. For details, refer to the Managing Search Server Settings section in the DeviceLock User Manual at www.devicelock.com/support/docs.html.

- **Discovery Server settings** - Affect the operation of the Discovery Server. For instructions on how to manage these settings, see Discovery Server Options.

The administrator can configure general server settings when installing the DeviceLock Content Security Server, or use the DeviceLock Management Console to configure and/or modify them after the server has been installed and is functioning.

> **Note:**
>
> - Only server administrators with sufficient rights can manage and use the DeviceLock Content Security Server.
> - To begin, connect the DeviceLock Management Console to the computer running the DeviceLock Content Security Server: Right-click **DeviceLock Content Security Server**, and then click **Connect**. For more information, refer to the Connecting to Computers section in the DeviceLock User Manual at www.devicelock.com/support/docs.html.

With the DeviceLock Management Console, the administrator can perform the following server configuration tasks:

- Configure which users have access to the DeviceLock Content Security Server.

- Change the startup account information, such as the account name or the password, for the DeviceLock Content Security Server service.

- Install or remove the DeviceLock certificate to authenticate communications between the DeviceLock Content Security Server and the DeviceLock Enterprise Server.

- Change the TCP port to connect the DeviceLock Management Console to the DeviceLock Content Security Server.

- View or change the DeviceLock Content Security Server's database connection settings.

One can perform these tasks individually or collectively.

To perform the tasks collectively, use the DeviceLock Content Security Server configuration wizard. This is the wizard that starts automatically when installing or upgrading the DeviceLock Content Security Server.

To perform configuration tasks collectively

1. In the console tree, expand **DeviceLock Content Security Server**.

2. Under **DeviceLock Content Security Server**, right-click **Server Options**, and then click **Properties**.

   The first page of the wizard appears.

3. Move through the wizard pages. After completing each page, move to the following one by clicking **Next**, or move to the preceding one by clicking **Back**. On the final page, click **Finish** to complete the wizard.

   For description of the wizard pages, see the Perform Configuration and Complete Installation section in the DeviceLock Content Security Server installation instruction.

Using the DeviceLock Management Console, the administrator can perform the following tasks to configure individual server settings:

- Configuring access to the DeviceLock Content Security Server
- Setting the service startup account
- Installing or removing a DeviceLock certificate
- Configuring the TCP Port setting
- Managing the database connection settings

Configuring access to the DeviceLock Content Security Server

The administrator can specify the users who are allowed to access the DeviceLock Content Security Server. This restricts outsiders from accessing or damaging the server.

To configure which users have access to the server

1. In the console tree, expand **DeviceLock Content Security Server**.

2. Under **DeviceLock Content Security Server**, do one of the following:

   - Select **Server Options**. In the details pane, double-click **Server Administrators** or right-click **Server Administrators** and then click **Properties**.

     - OR -

   - Expand **Server Options**. Under **Server Options**, right-click **Server Administrators** and then click **Properties**.

3. In the **DeviceLock Content Security Server** dialog box that appears, do the following:

   To enable default security

   - Select the **Enable Default Security** check box.

   If default security is enabled, members of the local Administrators group will have full access to DeviceLock Content Security Server.

   To restrict access to the server to specific users

   a) Clear the **Enable Default Security** check box.

   b) Under **Users**, click **Add** to add the specific users to be allowed access to the DeviceLock Content Security Server.

   c) In the **Select Users or Groups** dialog box that appears, in the **Enter the object names to select** box, type the name of the user or group, and then click **OK**.

   The selected users/groups become server administrators, which are listed under **Users** in the **DeviceLock Content Security Server** dialog box. Server administrators are authorized to perform the tasks related to configuring and using the DeviceLock Content Security Server and, by default, they have full access to the server.

To change the server access level for a particular administrator, select the respective user or group under **Users**, and then choose from the following options in the list of access rights:

- **Full access** - Allows the user or group to install and uninstall the DeviceLock Content Security Server, connect to it by using the DeviceLock Management Console, and perform any actions on the server, such as: view and change server settings; create and run search queries and tasks; view and change content detection settings; create and run discovery tasks and reports.

- **Change** - Same as full access to the server with the exception of the right to make changes to the list of server administrators or change the level of access to the server for the users or groups already in that list.

- **Read-only** - Allows the user or group to connect to the DeviceLock Content Security Server by using the DeviceLock Management Console; view server settings; run search queries; view and run existing search tasks; view content detection settings; view discovery reports and manually create new reports based on the existing reports and data already prepared by discovery tasks. This option does not give the right to run discovery tasks, make any changes on the server, or create a new index for the Search Server.

For users and groups with the **Change** or **Read-only** level of access, the **Shadow Data Access** option can be selected to allow access to shadowed data. The users and groups that have this option selected can open, view and download shadow data on search result pages or search reports, and search inside of shadowed files.

Note: We strongly recommend that the accounts designated as server administrators be given local administrator rights.

To revoke server administrator rights from a particular user or group, select that user or group in the **Users** area, and then click the **Delete** button.

One can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.

4. Click **OK**.

Setting the service startup account

Over time, the administrator might need to change the account that was specified as the service startup account when installing the DeviceLock Content Security Server. It is also possible to change the password of the service startup account.

To change the service startup account or password

1. In the console tree, expand **DeviceLock Content Security Server**.

2. Under **DeviceLock Content Security Server**, select **Server Options**.

3. In the details pane, double-click **Service startup account** or right-click **Service startup account** and then click **Properties**.

4. In the **DeviceLock Content Security Server** dialog box that appears, do the following:

   To change the service startup account

   a) In the **Log on as** area, click **Browse**.

   b) In the **Select User** dialog box that appears, in the **Enter the object name to select** box, type the name of the user, and then click **OK**.

   The selected user is displayed in the **This account** box in the **DeviceLock Content Security Server** dialog box.

   We recommend the use of an account with administrator rights on all computers running the DeviceLock Enterprise Server. In an Active Directory environment, we recommend the use an account that is a member of the Domain Admins group. Otherwise, DeviceLock certificate authentication should be used.

   To change the service account password

   a) In the **Log on as** area, type a new password in the **Password** box.

   b) Re-type the new password in the **Confirm password** box.

   To assign the Local System account to the server service

   • In the **Log on as** area, click **Local System account**.

   Note: If the service uses the Local System account, the Discovery Server:
   • Cannot access Discovery Agents running on remote computers and must use the DeviceLock Certificate for authentication on it.
   • Cannot install or remove Discovery Agents on remote computers.

5. Click **OK**.

Installing or removing a DeviceLock certificate

The Discovery Server may not be able to access the Discovery Agent due to insufficient access rights of the service startup account of the DeviceLock Content Security Server. In this case, DeviceLock certificate authentication should be set up by installing the private key of a DeviceLock certificate on the DeviceLock Content Security Server. The public key of that certificate must be installed for the DeviceLock Service on each computer to be scanned by the Discovery Agent. For details on DeviceLock certificates, refer to the DeviceLock Certificates section in the DeviceLock User Manual at www.devicelock.com/support/docs.html.

To install or remove DeviceLock Certificate on DeviceLock Content Security Server

1. In the console tree, expand **DeviceLock Content Security Server**.

2. Under **DeviceLock Content Security Server**, select **Server Options**.

3. In the details pane, double-click **DeviceLock certificate** or right-click **DeviceLock certificate** and then click **Properties**.

4. In the **DeviceLock Content Security Server** dialog box that appears, do the following:

    To install the private key of the DeviceLock certificate

    a) Next to the **Certificate Name** box, click the ▫ button to open the **Select the DeviceLock Certificate file** dialog box and browse for the file to use.

    b) In the **Select the DeviceLock Certificate file** dialog box, locate and select the certificate file, and then click **Open**.

    To remove the private key of the DeviceLock certificate

    • Next to the **Certificate Name** box, click **Remove**.

5. Click **OK**.

Configuring the TCP Port setting

Over time, the administrator might need to change the TCP port that the DeviceLock Management Console uses to connect the DeviceLock Content Security Server.

To change the TCP port for connecting the console

1. In the console tree, expand **DeviceLock Content Security Server**.

2. Under **DeviceLock Content Security Server**, select **Server Options**.

3. In the details pane, double-click **TCP port** or right-click **TCP port** and then click **Properties**.

4. In the **Connection Settings** area of the **DeviceLock Content Security Server** dialog box that appears, do one of the following:

    • Click **Dynamic ports** to use a dynamic port selection.

    - OR -

    • Click **Fixed TCP port** to use a specified port. Then, type the desired port number in the **Fixed TCP port** box.

    By default, the DeviceLock Content Security Server uses TCP port 9134.

5. Click **OK**.

Managing the database connection settings

A database connection is required for the Discovery Server to function. If there is no connection to the database, the Discovery Server is unavailable. The administrator can use the console to view or change the database connection settings.

To view or change the database connection settings

1. In the console tree, expand **DeviceLock Content Security Server**.

2. Under **DeviceLock Content Security Server**, select **Server Options**.

3. In the details pane, double-click any of these options: **Connection type**, **SQL Server name**, **Database name**, or **SQL Server login**. Alternatively, right-click an option, and then click **Properties**.

4. In the dialog box that appears, view or change the following connection settings:

   - **Database name** - The name of the DeviceLock Content Security Server's database.

   - **Connection type** - Either **ODBC Driver** or **System Data Source** can be selected. The following settings depend upon the selected connection type.

   - **SQL Server name** - Applies to **ODBC Driver**. Specifies the SQL Server instance that hosts the DeviceLock Content Security Server's database. If not specified, indicates the default instance running on the local computer.

   - **Windows authentication**/**SQL Server authentication** - Applies to **ODBC Driver**. Choose the authentication method appropriate to the SQL Server configuration. If choosing **SQL Server authentication**, supply the name and password of the SQL Server login to access the database.

   - **Data source name** - Applies to **System Data Source**. Select the appropriate name from the list. Data sources can be created by using the **Data Sources (ODBC)** applet from **Control Panel** > **Administrative Tools**.

5. Click **Next**, wait while the console completes the connection, and then click **Finish**.

For details on the database connection settings, see the Database Settings section in the DeviceLock Content Security Server installation instruction.

Discovery Server Options

The following Discovery Server options are available:

- **DeviceLock Enterprise Server(s)** - Allows you to specify one or more DeviceLock Enterprise Servers that host the fingerprints database.

- **Discovery Server license(s)** - Allows you to install your license for DeviceLock Discovery.

- **Log options** - Allows you to specify the types of event to record to the Discovery tasks log.

- **E-Mail Message for Alerts** - Allows you to customize the e-mail message template for Discovery alerts.

- **Syslog Message for Alerts** - Allows you to customize the syslog message template for Discovery alerts.

- **Discovery notification message** - Allows you to customize the Discovery message that pops up in the system notification area of the computer being scanned.

- **Data collection interval** - Allows you to specify the time interval through which Discovery Agent begins to report the availability of new data for transmission to the Discovery server.

- **Oracle IRM Server Settings** - Allows you to configure DeviceLock Discovery Server for Oracle IRM support.

- **Binary Files Content Inspection** - Allows you to enable keywords- and pattern-based content discovery for text held in arbitrary binary files.

To start configuring an option, double-click that option, or right-click it and use commands on the shortcut menu that appears.

Managing Discovery Server options involves the following tasks:

- Specifying Digital Fingerprints Database Server(s)

- Installing DeviceLock Discovery licenses

- Configuring log options

- Setting up alert and notification messages

- Setting the data collection interval

- Managing Oracle IRM Server settings

- Enabling binary files content inspection

Specifying Digital Fingerprints Database Server(s)

To use digital fingerprints for content discovery, DeviceLock Discovery requires at least one DeviceLock Enterprise Server to be specified that hosts the fingerprints database. For details on the digital fingerprinting technique, refer to the Digital Fingerprints section in the DeviceLock User Manual at www.devicelock.com/support/docs.html.

To specify servers that host the fingerprints database, right-click **DeviceLock Enterprise Server(s)** in **Discovery Server Options** and then click **Properties**, or double-click **DeviceLock Enterprise Server(s)**. Then, use the dialog box that appears to view or change the list of servers.

To add a server to the list, type the name of the computer on which the DeviceLock Enterprise Server is installed. You could type, for instance, the computer's fully qualified domain name (FQDN), short name or IP address. To add multiple servers, type computer names separated by a semicolon (;).

Individual computer names can be changed or removed from the list. To clear the list, click the **Remove** button.

Installing DeviceLock Discovery licenses

There is a special DeviceLock Discovery license which you must purchase in order to enable content discovery. DeviceLock Discovery is licensed on a per computer basis. A license is required for each computer or network device scanned with DeviceLock Discovery Server.

The DeviceLock Discovery licensing model is based on the number of computers to be scanned with DeviceLock Discovery. Each license allows DeviceLock Discovery to scan a single computer, regardless of whether the system is set to scan the entire computer or a single folder.

Depending on the actual number of computers on your network to be scanned with DeviceLock Discovery, you can purchase as many licenses as required. If you use several licenses for DeviceLock Discovery, it can scan as many computers as the combined licenses allow. The trial period for DeviceLock Discovery is 30 days. During the trial period, DeviceLock Discovery can scan a maximum of two computers. You can purchase and install additional DeviceLock Discovery licenses at any time.

You can install additional DeviceLock Discovery licenses by opening the **Discovery Server Options** node and then double-clicking the **Discovery Server license(s)** parameter. In the dialog box that appears, click the **Load License(s)** button to select the license file. It is possible to load several license files in series - one by one.

After you have loaded your license files, the dialog box displays the license information summary where **Total license(s)** is the total number of installed licenses while **Used license(s)** is the number of licenses currently in use for scanning computers or network devices with DeviceLock Discovery.

Configuring log options

Double-click the **Log options** parameter to open the dialog box where you can specify the types of event to record to the Discovery tasks log.
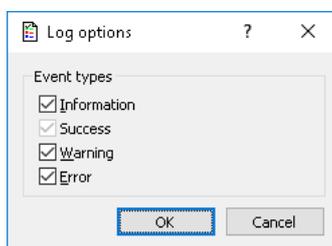
To enable or disable the recording of particular event types, select or clear respective check boxes:

- **Information** - Certain action performed.
- **Success** - Task or operation completed successfully.
- **Warning** - A problem might occur unless action is taken.
- **Error** - A problem has occurred.

> **Note:** The events indicating success are always recorded, therefore the Success check box is selected and cannot be cleared.

Setting up alert and notification messages

Network administrators as well as users on computers being scanned can be notified about certain events. Two kinds of notification are available:

- **Alerts** are SNMP traps, syslog messages or email messages that the DeviceLock Discovery Agent generates to help administrators keep track of the scanning process and be notified immediately if certain types of content are discovered.

- **Notifications** are system messages displayed to the current users on the computers being scanned, in a pop-up window next to the system clock in the taskbar. Notifications appear when the DeviceLock Discovery Agent detects content matches with discovery rules that are in effect.

> **Note:** DeviceLock displays user notifications when scanning with the Discovery Agent only. In the case of agentless scanning, user notifications are not displayed.

In **Discovery Server Options**, the contents of alert and notification messages can be configured by using the respective options.

To configure email message for alerts

1. Double-click the **E-Mail Message for Alerts** item in the **Discovery Server Options** node.

   - OR -

   Right-click the **E-mail Message for Alerts** item in the **Discovery Server Options** node, and select **Properties** from the shortcut menu.

   The E-mail Message for Alerts dialog box appears.
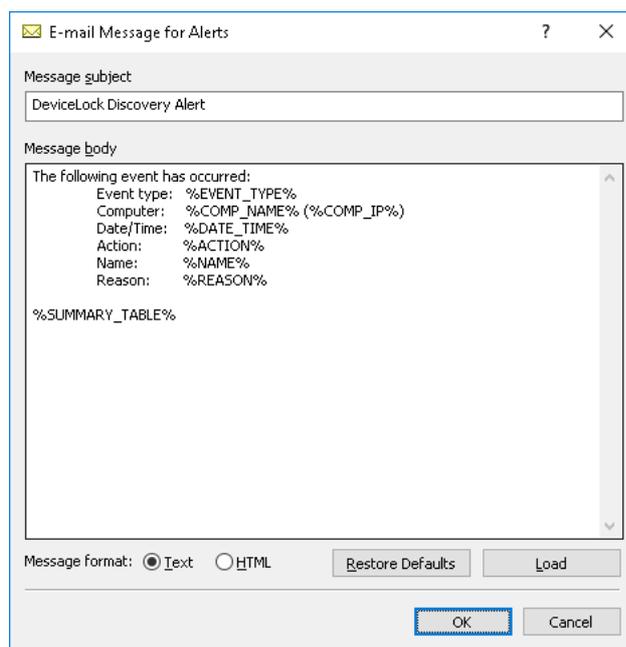
2. In the **E-mail Message for Alerts** dialog box, edit the template of the e-mail message, and click **OK**.

The template contains the following information:

- **Message subject** - The text used in the **Subject** line of the e-mail message. By default, the subject text of the e-mail message for alerts is as follows: **DeviceLock Discovery Alert**.

- **Message body** - The text used in the body of the e-mail message. DeviceLock can send either the plain text body or an HTML version of the message body. The message body includes static text and macros. By default, the static text in the message body is as follows: **The following event has occurred**.

You can use the following predefined macros in the **Subject** line and/or the body of the e-mail message:

- `%EVENT_TYPE%` - The class of event: either **Success** if the action was successfully applied to the discovered content, or **Failure** if the action could not be applied.

- `%COMP_NAME%` - The name of the computer on which the file was discovered.

- `%COMP_FQDN%` - The fully-qualified domain name of the computer on which the file was discovered.

- `%COMP_IP%` - A comma-separated list of all network addresses (IPs) associated with the computer.

- `%DATE_TIME%` - The date and time that the discovery event occurred. The date and time are displayed based on the client computer's regional and language settings.

- `%ACTION%` - The action applied to the identified file.

- `%NAME%` - The name of the file to which the action was applied.

- `%REASON%` - The cause of the event (the name of the rule that was triggered by the file).

- `%SUMMARY_TABLE%` - A table detailing and visualizing individual events for consolidated alerts.

These macros are replaced with their actual values at the message generation time.

3. You may select the **Text** or **HTML** email format by using the **Message format** option.

4. You may restore the default template by clicking **Restore Defaults**, or load a template from a file by clicking the **Load** button.

   A template can be loaded from a tab-delimited text file containing plain text or HTML.

To configure syslog message for alerts

1. Double-click on the **Syslog Message for Alerts** item in the **Discovery Server Options** node.

   - OR -

   Right-click the **Syslog Message for Alerts** item in the **Discovery Server Options** node, and select **Properties** from the shortcut menu.

   The Syslog Message for Alerts dialog box appears.
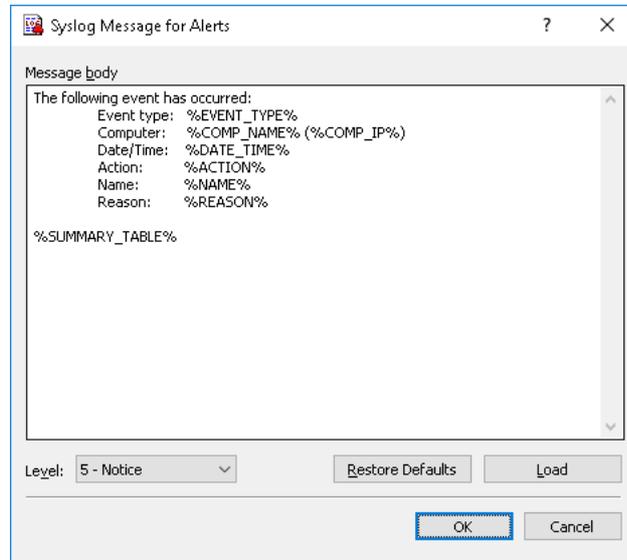
2. In the **Syslog Message for Alerts** dialog box, edit the template of the message, and click **OK**.

   The template contains the following information:

   - **Message body** - The text used in the body of the message. The message body includes static text and macros. By default, the static text in the message body is as follows: **The following event has occurred**.

   You can use the following predefined macros in the body of the syslog message:

   - %EVENT_TYPE% - The class of event: either **Success** if the action was successfully applied to the discovered content, or **Failure** if the action could not be applied.

   - %COMP_NAME% - The name of the computer on which the file was discovered.

   - %COMP_FQDN% - The fully-qualified domain name of the computer on which the file was discovered.

   - %COMP_IP% - A comma-separated list of all network addresses (IPs) associated with the computer.

   - %DATE_TIME% - The date and time when the discovery event occurred. The date and time are displayed based on the client computer's regional and language settings.

   - %ACTION% - The action applied to the identified file.

   - %NAME% - The name of the file to which the action was applied.

   - %REASON% - The cause of the event (the name of the rule that was triggered by the file).

   - %SUMMARY_TABLE% - A table detailing and visualizing individual events for consolidated alerts.

   These macros are replaced with their actual values at the message generation time.

3. You may select the message severity level using **Level** drop-down menu.

4. You may restore the default template by clicking **Restore Defaults**, or load a template from a file by clicking the **Load** button.

   A template can be loaded from a tab-delimited text file containing plain text.

To configure the discovery notification message

1. Double-click the **Discovery notification message** item in the **Discovery Server Options** node.

   The Discovery notification message dialog box appears.
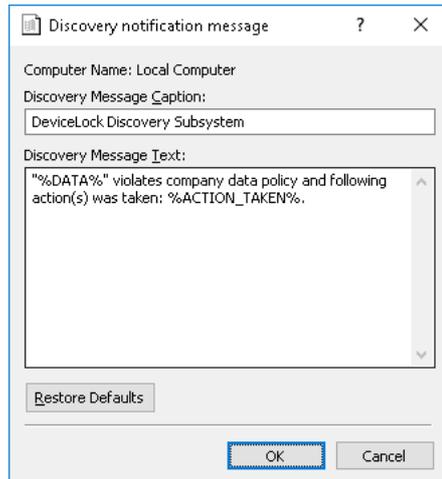
2. In the **Discovery notification message** dialog box, specify the **Caption** and **Text** of the notification message. This message pops up in the system notification area of a computer being scanned, and is visible to all users who are currently logged on to that computer.

   Along with static text, you can use the following predefined macros in the text of the notification message:

   - `%DATA%` - The name of the file that triggered the message.
   - `%ACTION_TAKEN%` - The name of the action(s) applied to that file.

Note: Notification messages are not displayed in case of agentless scanning. In case of scanning a terminal server, notification messages are displayed to all users connected to the terminal server.

Setting the data collection interval

You can configure the interval of discovery agents notifying the Discovery Server about new data. To change data collection settings, double-click the **Data collection interval** item in the **Discovery Server Options** node. The **Data collection interval** dialog box will appear.
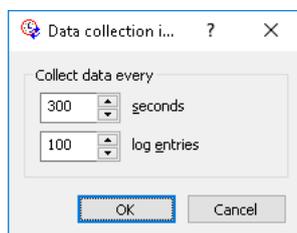
Under **Collect data every**, specify the time in seconds that should pass after a discovery task is started and before the scanning agents will start notifying the Discovery Server about new data. The default value is 300 seconds.

You can also specify the number of log entries to be accumulated before Discovery Agents will notify Discovery Server. Discovery Agent logs certain events during its work. Discovery Server users may specify additional logging rules, e.g. instructing the product to add a log entry if certain types of content are encountered. This setting configures the number of accumulated log entries that would cause Discovery Agents to notify the Discovery Server, after which the Discovery Server would collect information from the notifying Agent. The default value is 100 log entries.

The time in seconds and the number of log entries parameters are used concurrently. The data will be sent as soon as any one of the two conditions is met.

Managing Oracle IRM Server settings

Use the **Oracle IRM Server Settings** option to configure DeviceLock Discovery Server for Oracle IRM support. If you have configured Oracle IRM support, you will be able to analyze the content of files sealed by Oracle IRM.

Configuration settings are specified in the **Oracle IRM Server Settings** dialog box. To open that dialog box, right-click **Oracle IRM Server Settings** and then click **Properties**, or double-click **Oracle IRM Server Settings**.
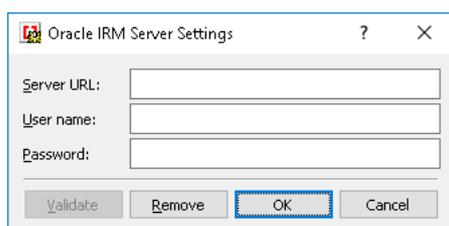
Complete the **Oracle IRM Server Settings** dialog box as follows:

- **Server URL** - Specify the URL of the IRM server used to seal documents for which access control by using DeviceLock is needed.
- **User name** - Specify the user account to use for authentication with the IRM server.
- **Password** - Specify the password corresponding to the user account to use for authentication with the IRM server.
- **Validate** - Click to attempt a connection to the IRM server using the specified server URL, user name and password.
- **Remove** - Click to remove the specified IRM server settings.

When configuring DeviceLock Discovery Server for Oracle IRM support, consider the following:

- The remote computer running the IRM server must be accessible from computers where the discovery task is being performed (by the Agent) or from the server (in case of agentless scanning).

- Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 5.0 must be installed on the IRM server. You can download this software from the Oracle Web site at www.oracle.com/technetwork/java/javasebusiness/downloads/java-archive-downloads-java-plat-419418.html.

- The IRM server you want to use must have a "device count" greater than 1.

- The IRM server certificate name must be the same as the IRM server name.

Enabling binary files content inspection

The **Binary Files Content Inspection** option allows for inspecting text content held in arbitrary binary files. When this option is disabled, DeviceLock performs keywords- and pattern-based content discovery for only Unicode text held in known file types. For a list of known file types, see "Expansive coverage of multiple file formats and data types" in the ContentLock and NetworkLock section of the DeviceLock User Manual at www.devicelock.com/support/docs.html.

When this option is enabled, DeviceLock performs keywords- and text pattern-based content discovery for text held in any binary files, regardless of text encoding (Unicode or non-Unicode). In this case, content discovery may take considerably longer to complete.

> **Note:** This option affects discovery rules that employ keywords groups, pattern groups and/or complex content groups containing those group types. For details regarding discovery rules, see Rules and Actions.

To enable or disable this option, double-click the **Binary Files Content Inspection** item in the **Discovery Server Options** list, or right-click that item and then choose **Enable** or **Disable**.

Alerts

The following alert options are available:

- **SNMP** - Allows you to configure SNMP transport for alerts.
- **SMTP** - Allows you to configure delivery of alerts via e-mail using an SMTP server.
- **Syslog** - Allows you to configure the forwarding of alerts to a syslog server.
- **Delivery retry parameters** - Allows you to configure server actions in case of alert delivery failure.

To start configuring an option, double-click that option, or right-click it and use commands on the shortcut menu that appears.

General Information

When scanning computers, DeviceLock Discovery can notify network administrators of certain events by issuing alerts. You can define alerts to automatically notify you if a scanning agent discovers content matching one of the defined discovery rules. Real-time alerting simplifies network administration and helps you respond faster and more efficiently to security incidents and policy violations.

Discovery Agents can send alerts notifying administrators of content discovery. Alerts can be sent to their intended recipients through e-mail or SNMP traps. Also, alerts can be sent to a syslog server.

To enable DeviceLock Content Security Server to send alert notifications, you should do the following:

- Decide how to be notified when alert conditions occur: through SNMP traps, e-mail or syslog.
- To be notified through SNMP traps, configure DeviceLock Content Security Server for SNMP support and specify the SNMP server to send traps to. For details, see Alerts Settings: SNMP.

  Note: This manual assumes a basic understanding of the Simple Network Management Protocol (SNMP) and related network management concepts.

- To be notified through e-mail, configure e-mail notifications by specifying SMTP Server and e-mail notification settings and defining the e-mail templates. For details, see Alerts Settings: SMTP.

- To be notified through syslog, configure DeviceLock Content Security Server for syslog and specify the syslog server to send alerts to. For details, see Alerts Settings: Syslog.

  Note: This manual assumes a basic understanding of syslog and related message logging concepts.

- Configure server actions in case of alert delivery failure, such as the delivery retry count, delivery retry interval, and the amount of time an undelivered notification is kept in the queue for delivery. For details, see Alerts Settings: Delivery retry parameters.

Alerts Settings: SNMP

Use the **SNMP** tab in the **Alerts Settings** dialog box to configure DeviceLock Content Security Server for SNMP support.

To open this dialog box, do either of the following:

- Right-click **Alerts** in the console tree, and then click **Manage**.

- Select **Alerts** in the console tree, and then click **Manage** 🗗 on the toolbar.

- Select **Alerts** in the console tree; then, in the details pane, right-click **SNMP** and click **Manage**.

- Select **Alerts** in the console tree, and then double-click **SNMP** in the details pane.

DeviceLock supports SNMPv1, SNMPv2c, and SNMPv3 protocols. You can configure DeviceLock Content Security Server to automatically send alert notifications to the specified SNMP server when alert conditions occur. These alerts are sent only when all of the following conditions are met:

- The SNMP server is set up to receive traps.

- The remote computer running the SNMP server is accessible from computers where the discovery task is being performed (by the Agent) or from the server (in case of agentless scanning).

- Alerts have been configured to be sent through SNMP traps.

Complete the **SNMP** tab as follows:

- **SNMP protocol version** - Choose the SNMP protocol version required by your SNMP server. Available options are: **SNMPv1**, **SNMPv2c**, and **SNMPv3**.

- **Connection** - Supply the SNMP server-related information:

  - **Server** - The SNMP sever to send traps to. In the **Server** box, type the SNMP server host name or IP address.

  - **Protocol** - The transport protocol for passing data between DeviceLock and the SNMP server. Available options are: **UDP** and **TCP**.

  - **Timeout** - The time (in seconds) that DeviceLock waits for the SNMP server to reply before retransmitting the data packet. The default is **1** second.

- **Port** - The port on which the SNMP server listens for traps. The default is **161**.

- **Retransmits** - The number of times a request is re-sent to the SNMP server, if the server is not responding (applies only to the **TCP** protocol). The default is **5**.

- **Security** - Configure SNMP security settings:

  - **Community** (if SNMPv1 or SNMPv2c is selected) - The SNMP community name to use for authentication with the SNMP server. The default is **public**.

  - **User name** (if SNMPv3 is selected) - The name of the user account to use for authentication with the SNMP server. To specify a user name, click the **Configure** button next to the **Security level** box. If authentication is not required, a user name may not be specified.

  - **Security level** (if SNMPv3 is selected) - A value indicating the security level of SNMP communication. Possible values:

    - **No security** - Communication using neither authentication nor encryption.

    - **Authentication** - Communication using authentication without encryption.

    - **Authentication and Privacy** - Communication using both authentication and encryption.

  - **Configure** (if SNMPv3 is selected) - Click the **Configure** button next to the **Security level** box, to specify the following settings:

    - **Security user name** - Supply the name of the user account to use for authentication with the SNMP server. If authentication is not required, this field can be left blank.

    - **Context name** - Supply the context name, as required by SNMP server.

    - **Context engine ID** - Supply the context engine ID, as required by SNMP server.

    - **Authentication protocol** - Choose the protocol used to encrypt the authentication with the SNMP server. Available options:

      - **None** - Security level of **No security**.

      - **HMAC-MD5** - Security level of **Authentication** or **Authentication and Privacy**, depending upon the **Privacy protocol** setting.

      - **HMAC-SHA** - Security level of **Authentication** or **Authentication and Privacy**, depending upon the **Privacy protocol** setting.

    - **Password/ Confirm password** - Supply the password of the user account to use for authentication with the SNMP server (applies to the **Authentication protocol** setting).

    - **Privacy protocol** - Choose the protocol used to encrypt data for SNMP communication. Available options:

      - **None** - Security level of **No security** or **Authentication**, depending upon the **Authentication protocol** setting.

      - **CBC-DES** - Security level of **Authentication and Privacy**, requires the **Authentication protocol** setting other than **None**.

      - **BC-AES-128** - Security level of **Authentication and Privacy**, requires the **Authentication protocol** setting other than **None**.

    - **Password/ Confirm password** - Supply the password for data encryption (applies to the **Privacy protocol** setting).

- **Threshold** - Specify the time interval (in hours, minutes or seconds) used for event consolidation when generating alerts. DeviceLock consolidates multiple similar events occurring within the threshold time and generates a summary in a single alert if all of the following conditions are true:

    a) The events are of the same type, either **Success** for actions successfully performed on discovered content, or **Failure** for failed actions.

    b) The **Reason** and **Computer** of the events being wrapped are the same.

  The default is **0** seconds.

- **Test** - Click to send a test SNMP trap to verify that DeviceLock is configured correctly. This test operation can have two different outcomes, each resulting in a different message being displayed:

    - The test can complete successfully, meaning that a test SNMP trap was successfully sent using the configured SNMP trap parameters. The resulting message states: "Test SNMP alert was successfully sent."

    - The test can fail, meaning that a test SNMP trap was not sent. The resulting message states: "Test SNMP alert was not sent due to error: <error_description>."

SNMP traps generated by DeviceLock are sent in the Management Information Base (MIB) format. The private DeviceLock MIB is represented by the object identifier (OID) **1.3.6.1.4.1.60000** or **iso.org.dod.internet.private.enterprise.DeviceLock**. The DeviceLock MIB contains the following branch nodes:

- **products(1)**

- **discoveryAgent(1)**

- **alerts(1)** - This node contains one instance of each of the following MIB objects:

    - **eventType(1)** - The class of an event: either **Success** for allowed access or **Failure** for denied access. Please note that the value of **eventType** is displayed as a numeric value instead of a text string: "**8**" indicates success, while "**16**" indicates failure.

    - **computerName(2)** - The name of the computer from which the event was received.

    - **action(3)** - The user's activity type.

    - **name(4)** - The name of the discovered object.

    - **reason(5)** - The cause of the event.

    - **datetime(6)** - The date and time (in the RFC3339 date/time format) when the content discovery event has occurred.

> **Note:** These MIB objects correspond to the column data in the Tasks Log Viewer.

A trap is sent just once each time an event associated with an alert occurs. Below is an example of the SNMP alert.

```
⌁ Specific: 1
      Message reception date: 21.02.2014
      Message reception time: 13:25:34.862
  🕐 Time stamp: 274 days 06h:37m:07s.29th
⌁ Message type: Trap (v1)
      Protocol version: SNMPv1
      Transport: IP/UDP
  🖥 Agent
      Address: 10.10.30.16
      Port: 59467
  🖥 Manager
      Address: 192.168.209.1
      Port: 0
  📂 Community: public
  🔎 SNMPv1 agent address: 10.10.30.16
  📊 Enterprise: enterprises.60000
  📁 Bindings (6)
      🟢 Binding #1: enterprises.60000.1.2.1.1 *** (gauge) 8
      🟢 Binding #2: enterprises.60000.1.2.1.2 *** (octet string) WIN7X64_DLADGLI
      🟢 Binding #3: enterprises.60000.1.2.1.3 *** (octet string) Log, Alert
      🟢 Binding #4: enterprises.60000.1.2.1.4 *** (octet string) C:\Documents\Research.docx
      🟢 Binding #5: enterprises.60000.1.2.1.5 *** (octet string) Rule: "Secret data" (Any keyword matched)
      🟢 Binding #6: enterprises.60000.1.2.1.6 *** (octet string) 2014-02-21T09:25:34Z
```

Alerts Settings: SMTP

Use the **SMTP** tab in the **Alerts Settings** dialog box to configure e-mail notifications.
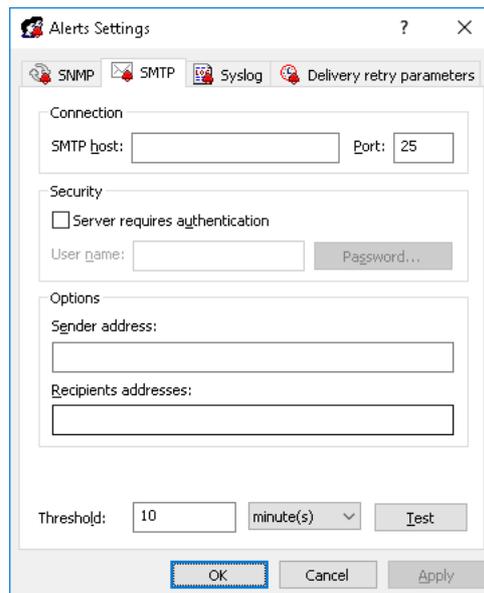
To open this dialog box, do either of the following:

- Right-click **Alerts** in the console tree, and then click **Manage**.

- Select **Alerts** in the console tree, and then click **Manage** 🗗 on the toolbar.

- Select **Alerts** in the console tree; then, in the details pane, right-click **SMTP** and click **Manage**.

- Select **Alerts** in the console tree, and then double-click **SMTP** in the details pane.

DeviceLock uses the Simple Mail Transfer Protocol (SMTP) for e-mail messaging. You can configure DeviceLock Content Security Server to automatically send notifications to the specified e-mail address(es) when alert conditions occur. To configure e-mail notifications, you'll have to specify SMTP server and configure e-mail notification settings.

Complete the **SMTP** tab as follows:

- **Connection** - Supply the mail sever-related information:
  - **SMTP host** - The name or IP address of the mail server.
  - **Port** - The port of the mail server. The default setting is **25**.

    Note: Both non-SSL (unencrypted) and SSL connections to the mail server are supported. DeviceLock automatically identifies and sets the required connection type.

- **Security** - If the mail server requires authentication, select the check box **Server requires authentication**, and supply the name and password of the mail server user in the **User name** and **Password** name, respectively.

- **Options** - Define the mail sender and recipients:
  - **Sender address** - You can supply the address of the mail sender. Normally, this is the name of the mail server user, such as user@mailserver.com. The sender address appears in the **From** field of the e-mail message.
  - **Recipients addresses** - Specify the e-mail addresses of alert recipients (those who will receive the e-mail notification of events). Multiple addresses must be separated by a comma (,) or semicolon (;).

- **Threshold** - Specify the time interval (in hours, minutes or seconds) used for event consolidation when generating alerts. DeviceLock consolidates multiple similar events occurring within the threshold time and generates a summary in a single alert if all of the following conditions are true:

  a) The events are of the same type, either **Success** for actions successfully performed on discovered content, or **Failure** for failed actions.

  b) The **Reason** and **Computer** of the events being wrapped are the same.

  The default is **10** minutes.

- **Test** - Click to send a test e-mail notification to verify that DeviceLock is configured correctly. This test operation can have two different outcomes, each resulting in a different message being displayed:

  - The test can complete successfully, meaning that a test e-mail notification was successfully sent using the configured e-mail notification parameters. The resulting message states: "Test SMTP alert was successfully sent."

  - The test can fail, meaning that a test e-mail notification was not sent. The resulting message states: "Test SMTP alert was not sent due to error: <error_description>."

Below is an example of the e-mail alert.

DeviceLock Alert

The following event has occurred:
Event type: Success (8)
Computer: WIN7X64_DLADGLI
Date/Time: 02/21/14 12:05:02
Action: Log, Alert
Name: C:\Documents\Research.docx
Reason: Rule: "Confidential data" (Matched: All keywords)

Note: Field names in an e-mail alert correspond to the column names in the Tasks Log Viewer.

Alerts Settings: Syslog

Use the **Syslog** tab in the **Alerts Settings** dialog box to configure DeviceLock Content Security Server for syslog.

To open this dialog box, do either of the following:

- Right-click **Alerts** in the console tree, and then click **Manage**.

- Select **Alerts** in the console tree, and then click **Manage** ⊞ on the toolbar.

- Select **Alerts** in the console tree; then, in the details pane, right-click **Syslog** and click **Manage**.

- Select **Alerts** in the console tree, and then double-click **Syslog** in the details pane.

You can configure DeviceLock Content Security Server to automatically send alert notifications to the specified syslog server when alert conditions occur. These alerts are sent only when all of the following conditions are met:

- The syslog server is set up to receive messages.

- The remote computer running the syslog server is accessible from computers where the discovery task is being performed (by the Agent) or from the server (in case of agentless scanning).

- Sending alerts to the syslog server is configured.

To configure sending alerts to the syslog server, complete the **Syslog** tab as follows:

- **Connection** - Supply the syslog server-related information:

  - **Server** - Specify the fully qualified domain name or IP address of the syslog server.

  - **Protocol** - Select **TCP** or **UDP** as the method of communication with the syslog server. The default is **UDP**.

  - **Port** - Specify the port number on which to send syslog messages. The default is **514**.

  - **Framing** - Specify the framing method for syslog messages when transported over TCP. DeviceLock supports these methods: **Zero byte**, **LF**, **CR+LF**, **Message length**.

- **Options** - View or change the following connection options:

    - **Name** - The unique name for the log channel. The default is **DeviceLockDiscoveryAlert**.

    - **Facility code** - A syslog standard value (between 0 and 23) to specify the type of program that is logging the message.

    - **Message size** - The syslog message size, in bytes. The default is **65535** bytes.

- **Threshold** - Specify the time interval (in hours, minutes and seconds) used for event consolidation when generating alerts. DeviceLock consolidates multiple similar events occurring within the threshold time and generates a summary in a single alert if all of the following conditions are true:

    a) The events are of the same type, either **Success** for actions successfully performed on discovered content, or **Failure** for failed actions.

    b) The **Reason** and **Computer** of the events being wrapped are the same.

    The default is **10** minutes.

- **Test** - Send a test syslog message to verify that DeviceLock is configured correctly. This test operation can have two different outcomes, each resulting in a different message being displayed:

    - The test can complete successfully, meaning that a test message was successfully sent using the configured syslog parameters. The resulting message states: "Test Syslog alert was successfully sent."

    - The test can fail, meaning that a test message was not sent. The resulting message states: "Test Syslog alert was not sent due to error: <error_description>."

Alerts Settings: Delivery retry parameters

Use the **Delivery retry parameters** tab in the **Alerts Settings** dialog box to configure server actions in case of alert delivery failure.
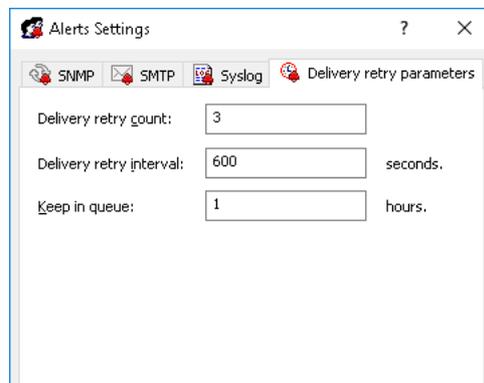
To open this dialog box, do either of the following:

- Right-click **Alerts** in the console tree, and then click **Manage**.

- Select **Alerts** in the console tree, and then click **Manage** on the toolbar.

- Select **Alerts** in the console tree; then, in the details pane, right-click **Delivery retry parameters** and click **Manage**.

- Select **Alerts** in the console tree, and then double-click **Delivery retry parameters** in the details pane.

DeviceLock generates and delivers alerts the moment the alert conditions are met. If alerts cannot be delivered on the first try, DeviceLock creates a queue to store undelivered alerts for a specified amount of time and sends them again. You can specify the maximum number of times DeviceLock attempts to send an alert, set the interval between delivery tries and also define the amount of time undelivered alerts are kept in the queue for delivery.

Complete the **Delivery retry parameters** tab as follows:

- **Delivery retry count** - Specify the maximum number of times DeviceLock attempts to send an alert if the first delivery attempt fails. If the first delivery attempt fails, the alert is deferred to the queue and marked as having had one delivery attempt. Thereafter, each time the queued alert is sent and delivery fails, the number of attempts is incremented.

  This parameter must contain a value between 0 and 1000. The default value is **3** retries.

  When the delivery retry count is reached and delivery fails, DeviceLock logs an error in the Discovery Tasks Log ("<channel_name> for alerts is unavailable and temporary disabled due to error: <error_code> - <error_description>") and temporarily stops further transmissions through the alert delivery channel (SNMP, SMTP and/or syslog).

  An attempt will be made to restore the delivery channel every time the agent successfully sends logs and status message to the Discovery Server.

- **Delivery retry interval** - Specify how many seconds DeviceLock waits before attempting next delivery of the alert, if the previous delivery failed. This parameter must contain a value between 10 and 3600. The default value is **600** seconds.

- **Keep in queue** - Define the amount of time in hours undelivered alerts are kept in the queue for delivery before they are deleted. The same queue is used for all delivery channels (SNMP, SMTP and/or syslog). This parameter must contain a value between 1 and 999. The default value is **1** hour.

Resetting Alert Settings to Defaults

At any time you can reset alert settings to their default state ("undefined"). To undefine all alert settings, right-click **Alerts** in the console tree, and then click **Undefine** on the shortcut menu. This command resets the alert settings to their default ("undefined") state.
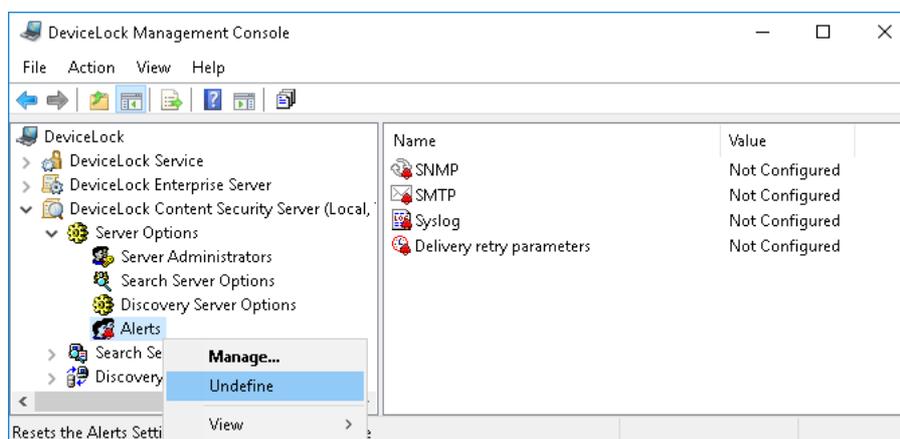
Resetting Individual Settings

You can also undefine individual options such as **SNMP**, **SMTP**, **Syslog** and **Delivery retry parameters**. In order to undefine any of these options, select **Alerts** in the console tree, and the right-click individual items appearing in the details pane. Click **Undefine** on the shortcut menu to reset the selected parameter.

4

Endpoint Scanning

In this chapter:

Discovery Server

DeviceLock Server scans user workstations and storage systems, looking for certain types of content according to configurable rules. Based on the results of the scan DeviceLock Server can perform various actions to grant or deny access to discovered content, alert the administrator, remove or encrypt discovered content or notify the computer user.

When scanning locations, DeviceLock Server operates with units. A unit lists all locations to be scanned. A single unit may consist of one or more computers, SMB shares or UNC paths. Each unit is assigned a set of content discovery rules as well as actions to be performed when content matching a certain rule is discovered.

After configuring one or more units with their corresponding rules and actions, a discovery task can be scheduled and deployed. Discovery tasks return scanning reports and logs, allowing administrators to review the results of the discovery job and see actions performed to the identified content.

A quick summary of configuring the discovery job is as follows:

1. Configure one or more units (locations to be scanned). For details, see Units.

2. Configure content discovery rules and actions applied to discovered content. For details, see Rules and Actions.

3. Set up and schedule one or more discovery tasks. For details, see Tasks.

Units

In DeviceLock Discovery, a unit is a basic entity for the purpose of content discovery. A unit is composed of one or more computers with either of the following properties:

- Common credentials

- Common scanning area settings (defined as pairs of Include and Exclude filters)

- Common scanning type

All units that currently exit on the server are listed in the console tree under **DeviceLock Content Security Server** > **Discovery Server** > **Units**.

When you select the **Units** node in the console tree, the details pane lists the units that currently exist on the server.
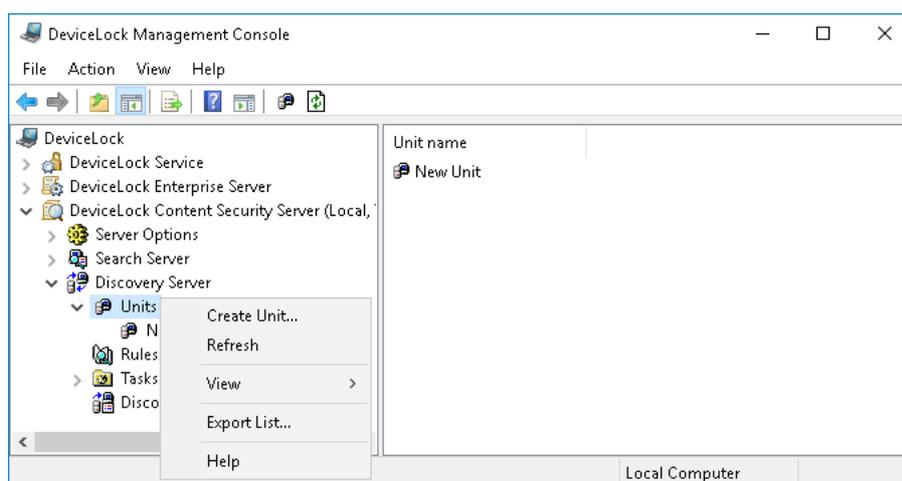
The list in the details pane displays the following information on each unit:

- **Unit name** - The name of the unit.

The shortcut menu on the **Units** node includes the following commands:

- **Create Unit** - Creates a new unit. You can specify the desired settings for the new unit in the dialog box that appears when you select this command.

- **Refresh** - Updates the list of units with the latest information.

The shortcut menu on a unit in the details pane includes the following commands:

- **Edit Unit** - Opens a dialog box where you can view or change the settings of the selected unit.

- **Duplicate Unit** - Creates a new unit with the settings copied from the selected unit. You can view or change the settings of the new unit in the dialog box displayed by this command.

  By default, the new unit name consists of the **Copy of** prefix followed by the name of the selected unit. When you create two or more copies of a unit, the new unit name includes a numeric suffix indicating the number of the copy.

- **Edit Computers List** - Opens a dialog box where you can view or change the list of computers included in this unit.

- **Delete Unit** - Deletes the selected unit.

- **Refresh** - Updates the list of units with the latest information.

Creating a Unit

To create a unit, open and complete the **Create Unit** dialog box. You can open that dialog box as follows:

1. In the console tree, expand **DeviceLock Content Security Server** > **Discovery Server** > **Units**.

2. Right-click the **Units** node, and then click **Create Unit** on the shortcut menu.

   - OR -

   Select the **Units** node, and then click **Create Unit** on the toolbar.

The **Create Unit** dialog box appears.
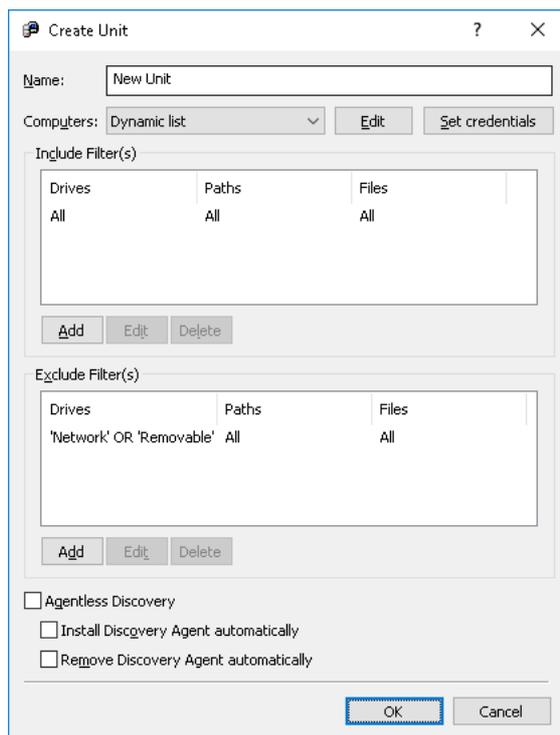
Complete the **Create Unit** dialog box as follows:

- **Name** - Specify a display name for the newly created unit.

- **Computers** - Specify the list of computers that are members of this unit. Two types of list are available: **Static list** and **Dynamic list**. You can choose the type of the list when creating a unit. Thereafter the list type cannot be changed.
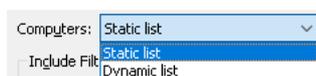
1. **Static list** - All computers are specified in the list by their names or IP addresses. Since this list is static, even if some computer no longer exists in the network, it will be scanned (and the error logged) until its record is deleted from the list manually.
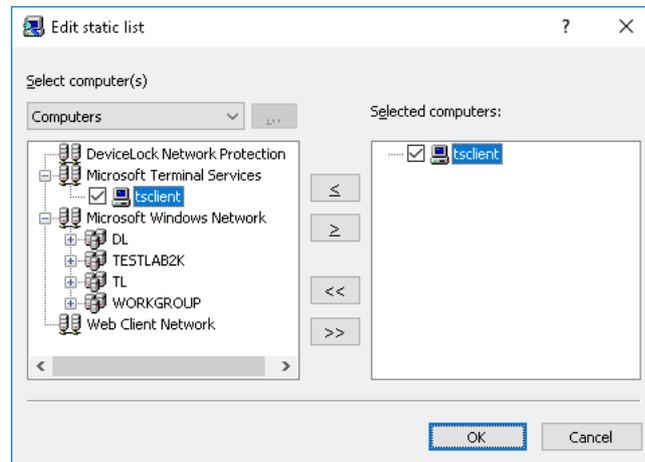
Computers that will be scanned must be specified in the list on the right. Select computers from the list on the left, and then move them to the list on the right by clicking the `>` button.

If you need to exclude some computers from the scanning job, select them in the list on the right and click the `<` button.

By using the `>>` and `<<` buttons, you can add and remove all available computers at the same time (no need to select computers in the list).

There are several ways to choose network computers from the left-hand list:
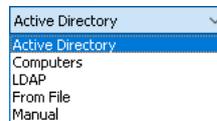
- **Active Directory** - Select computers from Active Directory folders (organizational units).

- **Computers** - Select computers that exist on the network.

- **LDAP** - Select computers from an LDAP-compatible directory.

- **From File** - Load a list of computers from a text file and then select computers. To open a text file, click the `...` button. In the file, each computer's name or IP address must be on a separate line.

- **Manual** - Type computer names manually to select the computers. Press ENTER as needed to type each computer's name or IP address on a separate line.

2. **Dynamic List** - Instead of computer names or IP addresses, you may specify a dynamic list containing path to the container (for example, an organizational unit) in the directory service tree such as Active Directory, Novell eDirectory, OpenLDAP and so on. Every time the task is executing, Discovery Server retrieves all the computers that currently exist in that container. Hence, if some computer was removed from the directory tree or moved to another container it will not be scanned anymore. And vice versa, if there is some new computer that did not exist in the container at the time the task was created/ modified, but was added to this container later, it will be retrieved and scanned at the time of executing the task. You can select one or more containers.
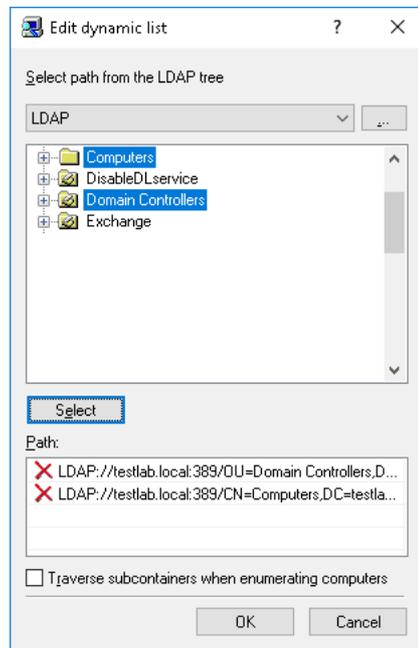
The path to the selected containers is specified in the **Path** field. Select containers in the tree by clicking while holding down the Shift or Ctrl key. Then click the **Select** button. To deselect the container, click the red X in the **Path** field.

Select the **Traverse subcontainers when enumerating computers** check box to allow Discovery Server to retrieve computers from all the nested containers located inside the selected container. Otherwise, if this check box is cleared all nested containers are ignored, and only computers located directly in the selected container are retrieved at the time of executing the task.

There are two modes to work with the directory service:

- **Active Directory** - You browse the Active Directory tree and select the needed container.

  While the Active Directory tree can also be displayed by choosing the **LDAP** option (see below), the Active Directory mode results in greater efficiency between the directory service and DeviceLock Discovery Server and thus resource savings.

  If you need to supply alternative credentials to access Active Directory, click the ... button and specify the needed user account and its corresponding password.

  > **Note:** If no alternative credentials are specified when accessing Active Directory, DeviceLock Discovery Server uses the credentials of the account under which the DeviceLock Content Security Server service is started. For more information, see Setting the service startup account.

Select the **Synchronization** check box to allow DeviceLock Discovery Server to use the synchronization feature of Active Directory. This will dramatically reduce the load on the domain controller and speed up the process of retrieving computers at the time of task execution.

> **Note:** To use the synchronization feature, DeviceLock Discovery Server must have access to Active Directory with domain administrator rights.

- **LDAP** - You browse the LDAP (Lightweight Directory Access Protocol) tree and select the needed container.

  To configure a connection to the LDAP server, click the ⋯ button and complete the **LDAP Settings** dialog box that appears.
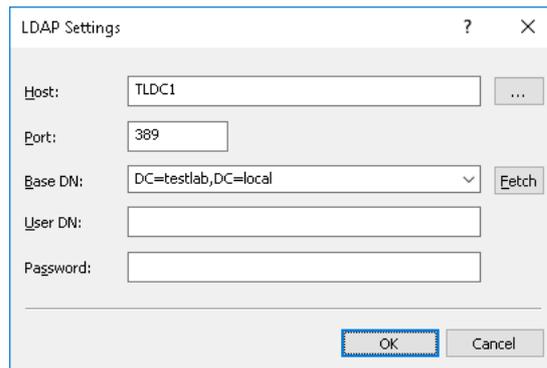
- **Host** - The name or the IP address of the LDAP server to connect to.

- **Port** - The TCP port on which the LDAP server accepts connections. The default port is 389.

- **Base DN** - The starting point for you to browse the directory tree. You must use the LDAP string representation for distinguished names (for example, cn=qa,o=SMARTLINE,c=US). Leave the **Base DN** box blank to start browsing from the root.

  By clicking the **Fetch** button, you can get all the published naming contexts.

- **User DN**, **Password** - The distinguished name (DN) and password of the directory user that allows connection to the directory. Use the LDAP string representation for distinguished name (for example, cn=admin,o=SMARTLINE,c=US).

> **Note:** If no user is specified when accessing the LDAP server, Discovery Server uses the credentials of the DeviceLock Content Security Server service's startup account. For more information, see Setting the service startup account.

- **Set Credentials** - Optionally, configure authorization credentials to access computers from the above list. Choosing credentials of an authorized user having administrative credentials on all endpoints is recommended.

> **Note:** In order to use alternative credentials and connect to remote DeviceLock Discovery agents, DeviceLock Content Security Server must be running under an account with administrative privileges.

The use of Credentials is optional. If no Credentials are specified, DeviceLock Discovery Server may use the DeviceLock Content Security Server service's startup account to access remote resources, or make use of the DeviceLock Certificate if the scanning is performed by DeviceLock Service with a corresponding public key installed.

> **Note:** If you are using an existing Discovery Server database used by a different Discovery Server, you will need to re-enter and apply your access credentials. All access passwords stored in the database are securely encrypted, and the encryption key is kept in the Protected Storage of the encrypting server. As a result, there is no way for a different Discovery Server to decrypt these passwords and thus the requirement to re-enter authorization credentials.

- **Include Filter(s) / Exclude Filter(s)** - Use include and exclude filters to specify which disks, folders and files you want the server to scan. By default, DeviceLock Discovery will scan all disks, files and folders except removable and network devices.

  Click **Add** under corresponding filter list to create a new filter. The **Add Exclude Filter** dialog will appear when adding an exclude filter. The **Add Include Filter** dialog appears when adding an include filter. For details, see Adding Filters. You can also change or delete filters by clicking the **Edit** or **Delete** button, respectively.

  The rules in each filter are stacked by using the logical OR operator. For example, by checking the **System**, **Non-system** and **Removable, Floppy & Optical** options in the **All Drives** section of the **Add Include Filter** dialog box, you will be specifying that only devices of these types will be scanned. If, in addition, you select the **Documents** check box, this will mean that only the Documents folders will be scanned on the drives matching the previously specified types. If you specify multiple filters, they will be combined with logical OR, meaning that a certain scanning area will be affected if it matches any of the filters. Include and exclude filters are combined by using the logical AND operator. For more information, see Creating a Filter: Example.

- **Agentless Discovery** - Select this check box if you want the server to scan remote computers without using Discovery Agent. The Agent is not installed on remote systems, and the scanning is performed via the SMB protocol. Depending on specified detection rules, the full content of the files being analyzed may be required. If this is the case, the files being analyzed will be transferred to the server for analysis, which may consume large amounts of bandwidth.

- **Install Discovery Agent automatically** - Select this check box if you want the server to install the Discovery Agent on the remote system if one is not yet installed, or if the remote system is not running DeviceLock Service with its bundled Discovery Agent.

- **Remove Discovery Agent automatically** - Select this check box if you want the server to remove the Discovery Agent from remote systems after the scanning task completes. Note that this option does not cause the server to remove DeviceLock Service and its bundled Discovery Agent.

   Note: If the DeviceLock Content Security Server service is configured to run under the Local System account, Discovery Server cannot install or remove Discovery Agents on remote computers.

The unit you have created appears in the console tree:
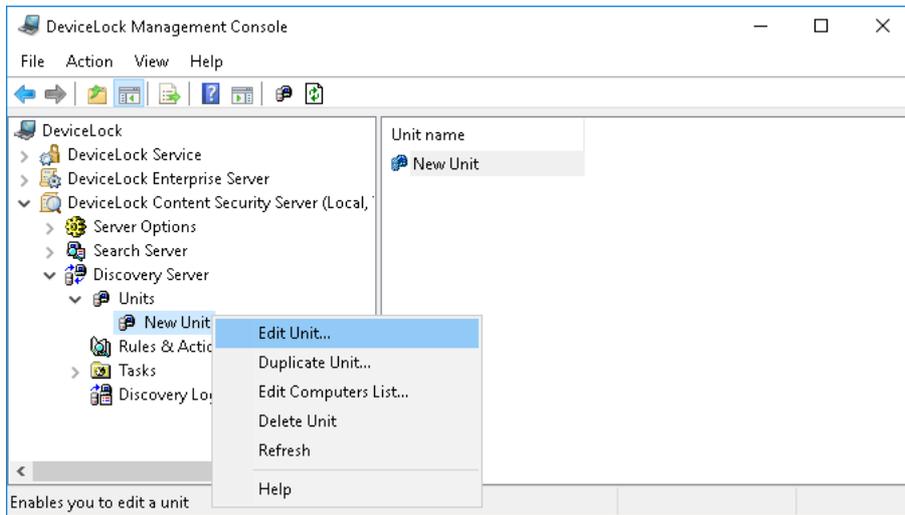
Adding Filters

To add a filter, use the **Add Include Filter** or **Add Exclude Filter** dialog box depending on the type of the filter.

Complete this dialog box as follows.

1. Specify the drives to include or exclude:

   - **All Drives** - Allows you to specify the types of storage devices to scan. These parameters are not supported in Agentless mode, in which case all disks will be scanned regardless of their type.

     Note: If the **All Drives** option is selected, the check boxes described below have no effect and the filter will include or exclude all disks.

     - **System** - Select to specify the logical disk where Windows is installed.

     - **Non-system** - Select to specify all other logical and physical disks that do not fall to other classifications.

     - **Network** - Select to specify mounted network disks. Multiple networks disks may exist for each logged in user. All network disks for all users will be scanned.

     - **Removable, Floppy & Optical** - Select to specify removable disks including floppy drives, optical drives (CD/DVD/BD-ROM). This also includes USB pen drives, attached memory cards, external storage devices connected via a USB cord etc.

2. Specify the paths to include or exclude:

- **All Paths** - Allows you to specify the paths on the disks to scan.

  > **Note:** If the **All Paths** option is selected, the check boxes described below have no effect and the filter will include or exclude all paths.

    - **Documents** - Select to specify the "My Documents" folder. Prior to Windows Vista, the path was defined as `%SystemDrive%\Documents and Settings\<user>\My Documents`. On Windows Vista or later, this path is defined as `%SystemDrive%\Users\<user>\Documents`. All document folders belonging to all users are scanned.

    - **Program Files** - Select to specify the "Program Files" folder. For 64-bit systems, both "Program Files" and "Program Files (x86)" will be scanned.

    - **System folder** - Select to specify the Windows installation folder.

    - **Temporary Folder** - Select to specify the system temp folder.

    - **Cloud storage folders** - Select to specify whether to scan the user's local synchronization directories for selected cloud storage services. The following services are supported: Amazon Cloud Drive, Box, Cloud Mail.ru, Copy, Dropbox, Google Drive, iCloud, MediaFire, OneDrive, SpiderOak, SugarSync, Yandex.Disk.

      > **Note:** The user (the owner of local synchronization directory) must be logged in for the **Box** cloud storage service directory to be scanned.

    - **Path** - Enter custom paths to scan. Multiple paths can be specified by using a semicolon (;) as a delimiter. UNC paths (e.g. `\\server\share`) are supported. You can use wildcards, such as asterisks (*) and question marks (?).

      See also Scanning a Network Share: Example.

    - **Including subfolders** - Specify whether to scan subfolders within the previously defined paths. If this option is not selected, only the files located in the specified folder will be scanned.

3. Specify the files to include or exclude:

- **All Files** - Allows you to specify the files to include or exclude.

  > **Note:** If the **All Files** option is selected, the check boxes described below have no effect and the filter will include or exclude all files.

    - **File name** - Specify the desired file names. Multiple file names must be separated by a semicolon (;); for example, `*.doc; *.docx`.

      You can use wildcards, such as asterisks (*) and question marks (?). An asterisk (*) replaces any group of characters. The question mark (?) replaces a single character. For example, type `*.txt` to specify all .txt files.

- **Modified** - Specify the desired last modification date/time of the file. To do so, choose from the following options in the **Modified** drop-down list:

    - **Not specified** (this option is selected by default)

    - **Before than** - The file's modified date/time must be earlier than the specified date/time.

    - **After than** - The file's modified date/time must be later than the specified date/time.

    - **Between** - The file's modified date/time must fall within the specified date/time range.

    - **Not older than** - The file's modified date/time must not be older than the specified number of seconds, minutes, hours, days, weeks, months, or years.

    - **Older than** - The file's modified date/time must be older than the specified number of seconds, minutes, hours, days, weeks, months, or years.

- **File size** - Specify the desired file size in bytes, kilobytes, megabytes, gigabytes or terabytes. To do so, choose from the following options in the **File size** drop-down list:

    - **Not specified** (this option is selected by default)

    - **Equal to** - The file must be exactly the specified size.

    - **Less than** - The file must be smaller than the specified size.

    - **More than** - The file must be larger than the specified size.

    - **Between** - The size of the file must fall within the specified range.

- **Attributes** - Specify the desired file attributes. The **System**, **Hidden** and **Encrypted** attributes are directly matched to the corresponding NTFS attributes.

Creating a Filter: Example

In the following example, we'll create a set of filters to scan all removable drives (including all currently inserted USB pen drives) as well as the folder `D:\Custom\`.

In order to create this unit, two Include filters must be specified, one enabling the scanning of all removable drives, and the other enabling the scanning of the custom folder. If we were to create a single filter combining both scanning parameters, the logical AND operator would be applied, and such filter would only enable the scanning of the `D:\Custom\` folder located on removable drives.

Create the first Include filter to scan all removable drives:

- **All Drives**: cleared
  Removable, Floppy & Optical: selected
  All other options in this category: cleared

- **All Paths**: selected

- **All Files**: selected

Create the second Include filter to scan the folder `D:\Custom\`:

- **All Drives**: selected

- **All Paths** and **all check boxes** in this category: cleared

- **Custom path**: enter `D:\Custom\`

- **All Files**: selected

Scanning a Network Share: Example

Suppose you need to scan a network share on a server or NAS device with an operating system on which DeviceLock cannot be installed (for example, a Linux OS). The network share is identified by a UNC path, such as `\\server\share`.

You can perform this task by configuring a unit as follows:

- Add a computer to the unit from which the network share can be accessed. This can be the computer running Discovery Server, or another computer with an operating system that allows DeviceLock installation (such as a Windows OS). For instructions, see Creating a Unit.

- Ensure that the user account under which Discovery Server performs a scan on that computer has sufficient rights to access the network share. At least read access is required. If during the scan Discovery Server needs to make changes on the network share (for example, encrypting files or setting permissions), appropriate access rights will be required.

  If the user account used by default to perform the scan does not have sufficient rights to access the network share, configure the unit to use alternative credentials. In the dialog box for creating or editing the unit, click the **Set Credentials** button, and specify the name and password of the user with the required access rights.

- Add an include filter to the unit. In the **Path** field of the filter, specify the UNC path of the network share.

Configure content discovery rules (see Rules and Actions), set up a discovery task based on the unit and rules you have configured (see Tasks), and run the task to perform the desired scan.

Managing Units

The console displays units in the console tree under **DeviceLock Content Security Server** > **Discovery Server** > **Units**.

When you select a unit in the console tree, the details pane displays the contents of that unit:
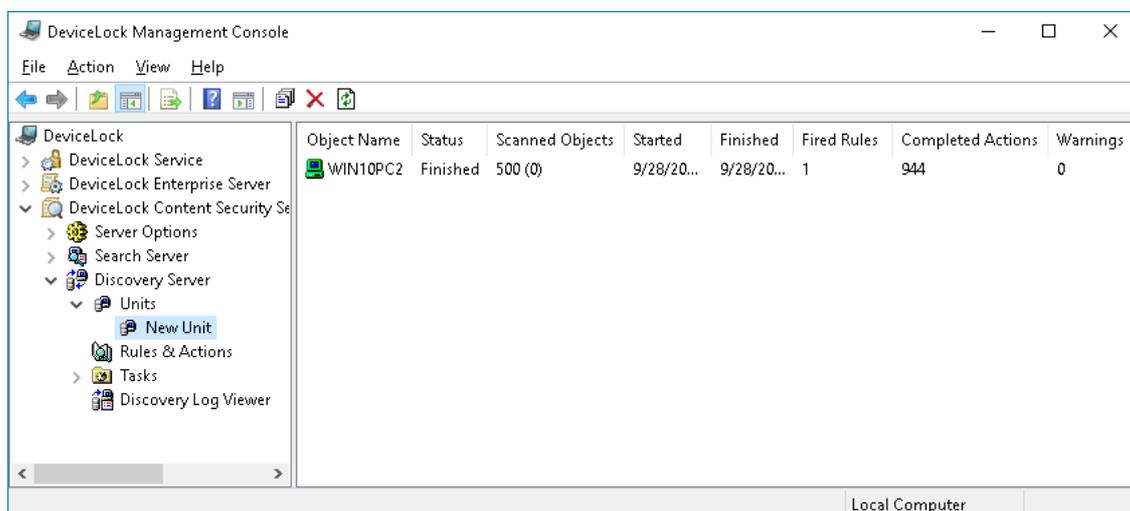
The details pane lists the following information about each computer held in the selected unit:

- **Object Name** - The name that identifies the computer.
- **Status** - The computer's status. The status can receive one of the following values:
    - **Waiting** - The computer is waiting for the scanning task to be run on that PC. This status is assigned when the applicable Task receives the status of **Running**.
    - **Scanning** - The computer is currently being scanned.
    - **Finished** - Indicates successful completion of the scanning task. The scanning of the computer has successfully completed.
    - **Expired** - Indicates a problem preventing the scanning task from completing. The task was initiated and began running, but the computer became unavailable (e.g. the computer was disconnected, or network configuration change prevented connectivity, or another problem prevented the Agent to successfully send logs and update status information to the server) and did not respond during the time period determined by the Keep-alive timeout parameter.

        The **Expired** status is also assigned if the scanning task exceeded the maximum scanning time as specified by the Stop task if runs longer than parameter, and was subsequently terminated.
    - **Access is denied** - Indicates a problem accessing the resource (e.g. computer). This can mean that the unit's specified credentials did not work (certificate or startup account error depending on configuration).
    - **Installation failed** - Indicates there was a problem installing Discovery Agent.
    - **No License** - Indicates that you don't have enough licenses to scan the computer.
    - **Canceling** - Indicates that the scanning task is being canceled.
    - **Canceled** - Indicates that the task has been canceled.

- **Computer is unavailable** - Indicates that either of the following issues has occurred after the number of attempts specified by the Number of retries parameter or on the expiry of the time period determined by the Retry timeout parameter:

  - Failed to connect to a remote computer in order to begin scanning (in agentless mode).

  - Failed to connect to a remote computer and communicate the scanning task to the Discovery agent. This can happen because the computer was unavailable (e.g. turned off or not connected to the network), or the Discovery agent was not installed or launched on that computer while the agent installation setting is not enabled in the unit properties (the **Install Discovery Agent automatically** flag is not set).

- **Scanned Objects** - Indicates the number of scanned objects. The bracketed value indicates the number of scanned nested objects.

  Example: "1 (20)" means 1 container (archive) with 20 files inside.

  > **Note:** The counter only adds up the number of objects processed during the last scanning. The counter resets every time a new scanning task is being run. The same applies to all other counters in this view.

- **Started** - Indicates the date and time when the server started scanning the resource.

- **Finished** - Indicates the date and time when the server finished scanning the resource.

- **Fired Rules** - The number of different rules that discovered a match. If a certain rule discovered more than one match, it will be still counted as 1.

- **Completed Actions** - Indicates the number of actions performed during the scan.

  Example: If a rule discovers a match, deleted a file, logged the event and sent a notification, this will count as 3 actions.

- **Warnings** - Indicates the number of scanning errors. This counter is increased if a matching object was discovered but it was impossible to take an action, or if content analysis was impossible (e.g. an attempt to analyze a corrupted or password-protected archive).

The shortcut menu on a unit in the console tree includes the following commands:

- **Edit Unit** - Opens a dialog box where you can view or change the settings of the selected unit.

- **Duplicate Unit** - Creates a new unit with the settings copied from the selected unit. You can view or change the settings of the new unit in the dialog box displayed by this command.

  By default, the new unit name consists of the **Copy of** prefix followed by the name of the selected unit. When you create two or more copies of a unit, the new unit name includes a numeric suffix indicating the number of the copy.

- **Edit Computers List** - Opens a dialog box where you can view or change the list of computers included in this unit.

- **Delete Unit** - Deletes the selected unit.

- **Refresh** - Updates the list in the details pane with the latest information.

  Since the console does not automatically update information displayed in the details pane, you need to update the list by using the **Refresh** command.

You can use the shortcut menu to manage computers held in the unit. To open the menu:

1. Expand **DeviceLock Content Security Server** > **Discovery Server** > **Units** in the console tree.

2. In the list under the **Units** node in the console tree, click the unit you want to manage.

   A list of computers will appear in the details pane.

3. Right-click a computer in the details pane.

   The shortcut menu will appear.
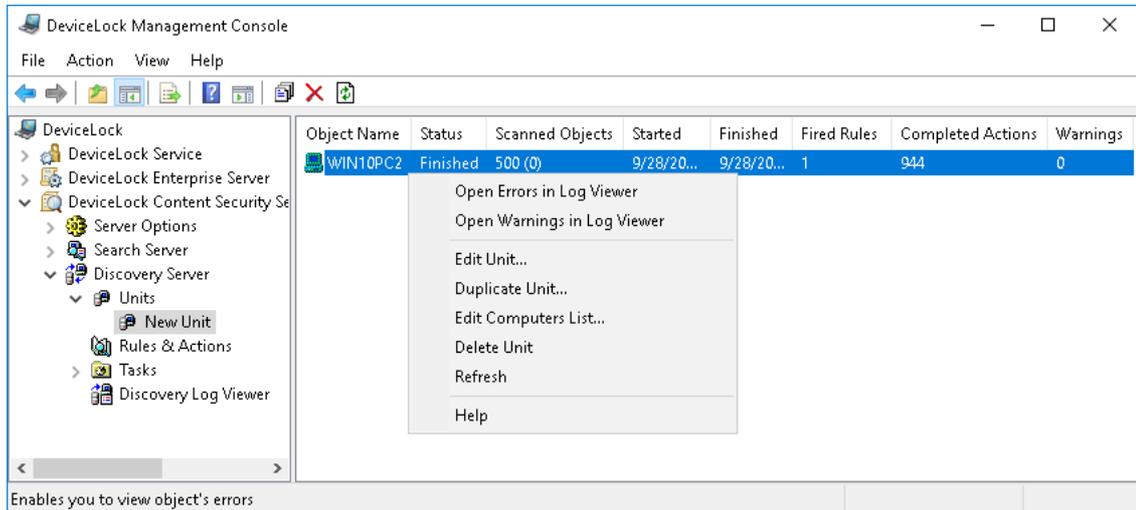
The shortcut menu on a computer in the details pane includes all commands that appear on the shortcut menu of the unit selected in the console tree as well as the following commands that apply to the selected computer:

- **Open Errors in Log Viewer** - Opens the Log Viewer with pre-defined filter settings to only display scanning errors for the selected computer. All errors occurred in all tasks and during the entire period of time will be displayed.

- **Open Warnings in Log Viewer** - Opens the Log Viewer with pre-defined filter settings to only display scanning warnings for selected computer. All warnings occurred in all tasks and during the entire period of time will be displayed.

Rules and Actions

By using content detection rules, you can define the type of content to discover and specify the actions to perform on the discovered data. Similar to DeviceLock Service's content-aware rules, content detection rules use content groups to determine the data to which a given rule should be applied.

Content detection rules are created based on content groups that enable you to centrally define the types of content to discover. Each rule employs a certain content group, and specifies the actions to apply to the discovered data. The rule's content group specifies the search criteria for the data to which those actions are to be applied.

All content groups are stored in the Content Database. The Content Database for DeviceLock Discovery is stored in the SQL database of the Discovery Server. As a result, all consoles communicating with the Server will operate with a single common Content Database.

> **Note:** Groups stored in the Content Database of the DeviceLock Service can be imported to the DeviceLock Discovery Server. For instructions, see Importing and Exporting Rules.

The following content group types are available:

- **File Type Detection** - Identify files by using file type-specific signatures.
- **Keywords** - Look for specific keywords or phrases in data/files.
- **Pattern** - Look for specific text fragments by using Perl regular expressions.
- **Document Properties** - Look for specific document properties, such as size, name, etc.
- **Digital Fingerprints** - Check digital fingerprints of data/files.
- **Complex** - Compose a logical expression of multiple group types.
- **Oracle IRM groups** - Identify files by using their IRM contexts.

For more information about content groups, refer to the Configuring Content Groups section in the DeviceLock User Manual at www.devicelock.com/support/docs.html.

Rules & Actions Node

When you select **DeviceLock Content Security Server** > **Discovery Server** > **Rules & Actions** in the console tree, the details pane lists all the content detection rules that currently exist on the server.
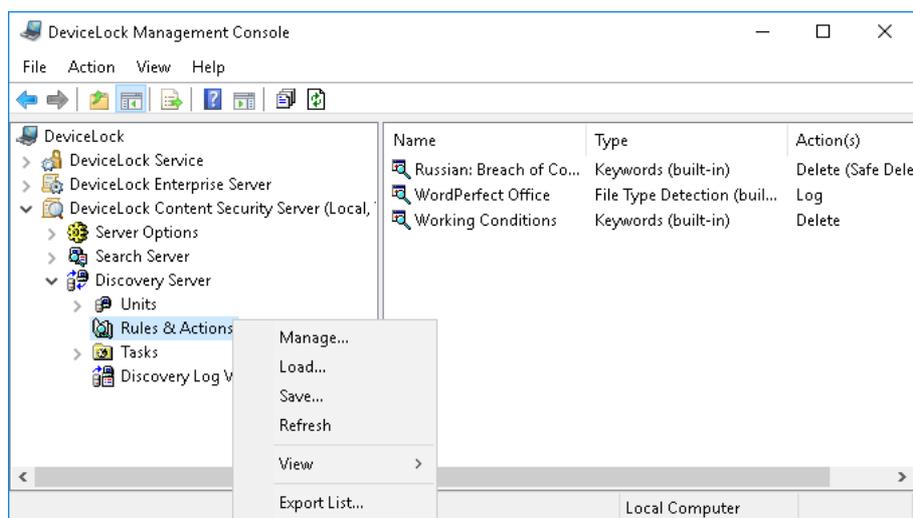
In the details pane, the following information is displayed on each rule:

- **Name** - The name that identifies the rule. By default, the rule has the same name as its content group.

- **Type** - The type of the content analysis. Possible values:

  - **File Type Detection** - Recognition and identification of files is based on their characteristic signatures.

  - **Keywords** - Recognition and identification of data/files is based on the specified keywords or phrases.

  - **Pattern** - Recognition and identification of data/files is based on the specified patterns of text described by Perl regular expressions.

  - **Document Properties** - Recognition and identification of files is based on their properties.

  - **Digital Fingerprints** - Recognition and identification of data/files is based on their digital fingerprints.

  - **Complex** - Recognition and identification of data/files is based on the specified content described by a Boolean expression.

  - **Oracle IRM** - Recognition and identification of files is based on their IRM contexts.

- **Action(s)** - The action of the rule. Possible actions:

  - **Delete** - Deleting the detected content.

  - **Safe Delete** - Deleting the detected content with the use of a secure erase procedure as defined in US DoD 5220.22-M.

  - **Encrypt** - Encrypting the detected content by using Windows EFS (Encrypted File System).

  - **Set permissions** - Setting certain file system permissions on the detected files.

  - **Apply to Containers** - Means that the action can be applied to archive files, such as ZIP or RAR files, that hold the detected content.

  - **Log** - Recording an event to the Discovery Tasks Log that informs about the detected content.

  - **Send Alert** - Sending an alert that informs about the detected content.

  - **Notify User** - Notifying the computer user about the detected content.

The shortcut menu on the **Rules & Actions** node includes the following commands:

- **Manage** - Opens a dialog box where you can create, view, modify or delete content detection rules and content groups.

- **Load** - Loads rules from an export file. You can use this command to import content detection rules of Discovery Server as well as content-aware rules and content groups exported from DeviceLock Service.

- **Save** - Saves all rules to an export file.

  You can export rules to a file and then load them from the export file. This function may be useful, for example, when you need to copy rules to another server.

- **Refresh** - Updates the list in the details pane with the latest information.

  Since the console does not automatically update information displayed in the details pane, you need to update the list by using the **Refresh** command.

The shortcut menu on a rule in the details pane includes the following commands:

- **Manage** - Opens a dialog box where you can create, view, modify or delete content detection rules and content groups.

- **Edit Rule** - Opens a dialog box where you can view or change the action of the rule. You can also change the name of the rule.

- **Duplicate Rule** - Creates a new rule with the settings copied from the selected rule. You can change the action and the name of the new rule in the dialog box displayed by this command.

  By default, the new rule name is composed of the **Copy of** prefix followed by the name of the selected rule. When you create two or more copies of a rule, the new unit name includes a numeric suffix indicating the number of the copy.

- **Delete Rule** - Deletes the selected rule.

- **Refresh** - Updates the list in the details pane with the latest information.

  Since the console does not automatically update information displayed in the details pane, you need to update the list by using the **Refresh** command.

Defining and Editing Rules and Actions

Content detection rules are defined and edited by using the **Rules & Actions** dialog box.

To define a content detection rule

1. Open the DeviceLock Management Console.

2. In the console tree, expand **DeviceLock Content Security Server** > **Discovery Server**.

3. Under **Discovery Server**, do one of the following:

   - Right-click **Rules & Actions**, and then click **Manage**.

     - OR -

   - Select **Rules & Actions**, and then click **Manage** 🗗 on the toolbar.

Configuring content detection rules in DeviceLock Discovery is similar to configuring content-aware rules in ContentLock. For details, refer to the Content-Aware Rules (Regular Profile) section in the DeviceLock User Manual at www.devicelock.com/support/docs.html.

To edit, duplicate or delete a content detection rule

1. Open the DeviceLock Management Console.

2. In the console tree, expand **DeviceLock Content Security Server** > **Discovery Server**.

3. Under **Discovery Server**, select **Rules & Actions**.

4. In the details pane, right-click the rule you want to edit, duplicate or delete, and then use the commands from the shortcut menu that appears:
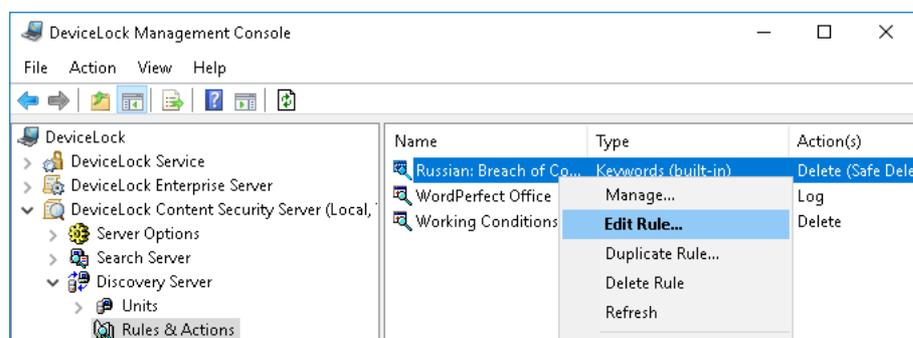
Using the "Rules & Actions" Dialog Box

You can define and edit content detection rules by using the **Rules & Actions** dialog box. Right-click **Rules & Actions** in the console tree, and then click **Manage** to open that dialog box. The **Rules & Actions** dialog box provides the tools for managing content groups and content discovery rules for Discovery Server.

Content detection rules are created based on content groups that enable you to centrally define the types of content to discover. You can use the built-in content groups as they are, create their editable copies (duplicates) or create your own content groups to suit your particular organization's needs.

To view a content group

- In the upper pane of the dialog box, under **Content Database**, select a content group, and then click **View Group**.

You cannot edit built-in content groups but you can create and edit their copies to suit the needs of your organization.

To copy a content group

1. In the upper pane of the dialog box, under **Content Database**, select a content group, and then click **Duplicate**.

2. In the dialog box that appears, edit the content group as required, and then click **OK**. The content group you created is added to the list of content groups under **Content Database** in the upper pane of the **Rules & Actions** dialog box.

You can modify or delete custom content groups at any time.

To modify or delete a custom content group

1. In the upper pane of the dialog box, under **Content Database**, select a custom group.

2. To modify the selected group, click **Edit Group**. In the dialog box that appears, make the necessary changes, and then click **OK**.

   - OR -

   To delete the selected group, click **Delete Group** or press the DELETE key.

3. In the **Rules & Actions** dialog box, click **OK** or **Apply** to save the changes.

You can test any built-in or custom content group to see whether specified files match with it. By using these tests, you can verify that the rules that are created based on the content groups meet your specific business requirements.

To test a content group

1. In the upper pane of the dialog box, under **Content Database**, select a content group, and then click **Test Group**. You can test only one group at a time.

2. In the dialog box that appears, locate and open the file to use for testing the selected content group.

   The console displays the **Result** message box. If the file matches the content group, the message box contains the following text: "Selected file matches with the group." If the file does not match the content group, the message box contains the following text: "Selected file does not match with the group."

   Note: When testing is in progress, the console stops responding (hangs).

Content detection rules are created based on either the built-in or custom content groups.

To define a content detection rule

1. In the upper pane of the dialog box, under **Content Database**, select the desired content group, and then click **Add**.

   > **Note:** For each rule, you can choose only one content group.

2. In the **Add Rule** dialog box that appears, specify the rule properties, and then click **OK**.

   The rule you created is displayed under **Rules & Actions** in the lower pane of the **Rules & Actions** dialog box.

3. Click **OK** or **Apply** to save the rule.

You can modify rule properties such as **Name** and **Actions**.

To modify rule properties

1. In the lower pane of the dialog box, under **Rules & Actions**, select a rule, and then click **Edit**.

   - OR -

   Right-click a rule, and then click **Edit**.

2. In the **Edit Rule** dialog box that appears, modify the rule properties as required to meet your needs.

3. Click **OK** to save the changes.

You can export all your current content detection rules to a .dra file that you can import and use on another computer. You can also import content detection rules from a .dra file, as well as import DeviceLock Service's content-aware rules from a .cwl file. Exporting and importing can also be used as a form of backup.

To export content detection rules

1. In the lower pane of the dialog box, under **Rules & Actions**, click **Save**.

2. In the dialog box that appears, specify the export file. When you export rules, they are saved in a file with a .dra extension.

To import content detection rules or content-aware rules

1. In the lower pane of the dialog box, under **Rules & Actions**, click **Load**.

2. In the dialog box that appears, locate and open the file containing the earlier-exported rules.

   You can import only one .dra or .cwl file at a time.

You can delete content detection rules when they are no longer required.

To delete a content detection rule

- In the lower pane of the dialog box, under **Rules & Actions**, select the rule and then click **Delete** or right-click the rule, and then click **Delete**.

Using the "Edit Rule" Dialog Box

When having detected any content that matches a given rule, DeviceLock performs the action specified by that rule. Use the **Edit Rule** dialog box to view or change the action of a particular rule:

1. Open the DeviceLock Management Console, and then, in the console tree, select **DeviceLock Content Security Server** > **Discovery Server** > **Rules & Actions**.

2. In the details pane, right-click the rule, and then click **Edit Rule** on the shortcut menu to open the **Edit Rule** dialog box:
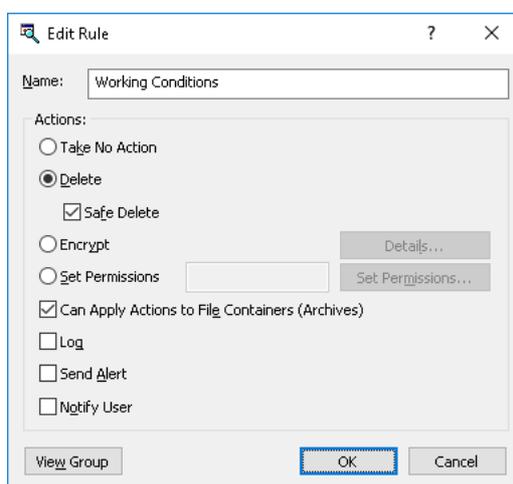
3. Use the following settings provided in the **Edit Rule** dialog box:

   - **Name** - View or change the name of the rule.

     By default, the rule has the same name as its content group. The name of the rule can be changed if needed.

     To view this rule's content group, click the **View Group** button in the bottom left corner of the dialog box. The console displays the properties of the group in a separate dialog box, allowing property values to be viewed but not modified.

   - **Take No Action** - Select to leave the detected content intact. This option should be used when configuring the rule to log a discovery event, alert or notify about the discovery.

   - **Delete** - Select to delete the detected content. The following option is available:

     - **Safe Delete** - Deletes the detected content using a secure erase procedure as defined in US DoD 5220.22-M.

   - **Encrypt** - Select to encrypt the detected content using Windows EFS (Encrypted File System). To enable this action, you have to configure file encryption as follows:

     a) Select the **Encrypt** option, and then click the **Details** button.

     b) In the **Encryption Details** dialog box that appears, click **Add**.

     c) In the dialog box that appears, select a certificate from the list of available encryption certificates.

     > **Note:** The list of available encryption certificates corresponds to the list of Personal Certificates of the user under whose account the management console is launched. You can view Personal Certificates in the **Certificates** console. For details, see Microsoft's article at technet.microsoft.com/library/cc512680.aspx.
     >
     > During the encryption, a Recovery Agent EFS certificate is added.

Encryption does not function when using a remote file system in agentless scanning or when SMB resource scanning is performed. This limitation is specific to EFS and not to DeviceLock Discovery.

> **Note:** If a file matches multiple rules with the **Encrypt** action, it will be encrypted with all certificates specified in all matching rules.

- **Set Permissions** - Select to set file access permissions on the detected content. Click the **Set Permissions** button to open the standard file permissions dialog provided by the operating system.

> **Note:** If a file matches multiple rules with the **Set Permissions** action, the resulting permission settings on the file will be determined by joining all access control lists (ACL) from all matching rules.

Permission conflict resolving: If a file matches multiple rules that specify mutually exclusive permissions, the resulting ACL on that file will be configured by setting individual access parameters. For example, suppose a given file matches two rules, one of which specifies `Allow Full Control` while the other one specifies `Deny Write` for the same user. In this case, the resulting ACL will be as follows: `Allow Read, Read & Execute; Deny: Write`.

If the different rules specify different users or user groups, any access control rights specified by these rules are joined together, and the resulting ACL is determined by Windows.

- **Can Apply Actions to File Containers (Archives)** - Select to allow applying an action (**Delete**, **Set Permissions**, **Encrypt**) to the entire compressed archive (such as a ZIP or RAR file) in which the matching content was discovered. If this option is not selected, the action will not be applied to the container.

> **Note:** This option also affects saved emails (EML), Adobe Portable Document Format (PDF) files, Rich Text Format (RTF), AutoCAD files (.dwg, .dxf), and Microsoft Office documents (.doc, .xls, .ppt, .vsd, .docx, .xlsx, .pptx, .vsdx).

- **Log** - Select to have the rule record a discovery event to the tasks Log (see Tasks Log Viewer).
- **Send Alert** - Select to have the rule alert the administrator about the detected content.
- **Notify User** - Select to have the rule notify the user with a message displayed in the system tray.

> **Note:** User notification is not available in Agentless mode.

Importing and Exporting Rules

You can export all your current Discovery Rules and Actions to a .dra file that you can import and use on another computer. You can also import Discovery Rules and Actions from a .dra file, as well as import content-dependent detection rules from a Content-Aware Rules .cwl file. Exporting and importing can also be used as a form of backup.

You can export Discovery Rules and Actions by using the **Save** button in the **Rules & Actions** dialog box. The **Load** button in that dialog box imports Discovery Rules and Actions from either a .dra or .cwl file.

Another option is to use the **Save** and **Load** commands on the **Rules & Actions** node in the DeviceLock Management Console.

To export Discovery Rules and Actions

1. In the console tree, expand **DeviceLock Content Security Server** > **Discovery Server** > **Rules & Actions**, right-click the **Rules & Actions** node, and then click **Save**.

2. In the **Save As** dialog box that appears, specify the export file to hold the exported rules.

   When you export rules, they are saved in a file with the .dra file name extension.

To import Discovery Rules and Actions

1. In the console tree, expand **DeviceLock Content Security Server** > **Discovery Server** > **Rules & Actions**, right-click the **Rules & Actions** node, and then click **Load**.

2. In the **Open** dialog box that appears, select the .dra or .cwl file that holds the exported rules.

   You can import only one .dra or .cwl file at a time.

Content-dependent detection rules in .cwl format can be loaded from a file. When loading rules from a .cwl file, **Log Event** and **Send Alert** parameters are automatically converted into **Log** and **Send Alert** respectively. If the source rule does not have these parameters, you will need to specify the required action. Such rules will be displayed with an exclamation point icon as shown in the screen below.
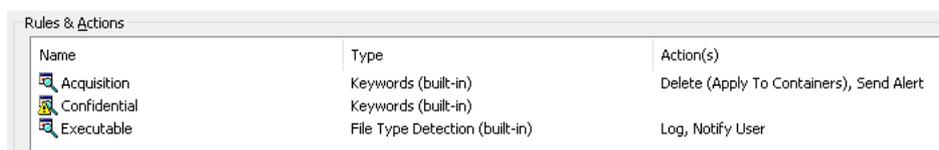
Rules & Actions		
Name	Type	Action(s)
Acquisition	Keywords (built-in)	Delete (Apply To Containers), Send Alert
Confidential	Keywords (built-in)	
Executable	File Type Detection (built-in)	Log, Notify User

Important: It is not possible to use a list of imported rules in which there is a rule marked with an exclamation point. Such rules must be re-configured by hand in order to assign an action or set up logging, alerting, or notification. Once all rules are correctly configured, the list is ready to use.

Tasks

In DeviceLock Discovery, all actions (computers scanning, content checking and applying actions to discovered content) are performed by tasks.

A single DeviceLock Discovery license can support an unlimited number of tasks. The maximum number of tasks is only limited by available memory, CPU and network's bandwidth capacity. Please keep in mind that the server should have sufficient resources to communicate with at least 10 remote computers simultaneously.

DeviceLock Discovery Server imposes the following limits on concurrent communications:

- For scanning with DeviceLock Discovery Agent:

  - The Server sends tasks to remote agents in up to 5 threads. This number cannot be changed.

  - The Server collects scanning logs and status updates from remote agents in up to 10 threads. This value can be changed by modifying the following registry value:

    - Key: `HKEY_LOCAL_MACHINE\SOFTWARE\SmartLine Vision\DeviceLockContentSecurityServer\DiscoverySettings`

    - Value: `MaxConcurrentAgents=dword:<number_of_threads>`

    In this value, `<number_of_threads>` must be an integer between 1 and 64.

- For agentless scanning:

  - The Server scans remote computers in up to 10 threads. This value can be changed by modifying the following registry value:

    - Key: `HKEY_LOCAL_MACHINE\SOFTWARE\SmartLine Vision\DeviceLockContentSecurityServer\DiscoverySettings`

    - Value: `MaxConcurrentLocalAgents=dword:<number_of_threads>`

    In this value, `<number_of_threads>` must be an integer between 1 and 64.

The following activities occur during task execution:

1. Write status information to the tasks Log (Tasks Log Viewer), including data about computers being scanned with DeviceLock Discovery.

2. Perform actions on discovered content (as defined in the Rules & Actions).

3. Create a report containing all relevant information about the task execution.

The tasks are controlled with the management console as described below.

Action	Description
View Log	To view Discovery tasks log: 1. In the management console tree, expand **DeviceLock Content Security Server** > **Discovery Server** > **Tasks**. 2. Under the **Tasks** node, click **Log Viewer**. The log view will appear in the details pane. The log view is common to all tasks.
Edit Task	To view or change task parameters: 1. In the management console tree, expand **DeviceLock Content Security Server** > **Discovery Server** > **Tasks**. 2. Under the **Tasks** node, right-click the task, and then click **Edit Task** on the shortcut menu. You can view or change the task parameters in the wizard that appears.

Action	Description
View Report	To view the report of a certain task:

1. In the management console tree, expand **DeviceLock Content Security Server** > **Discovery Server** > **Tasks**.
2. Under the **Tasks** node, expand the task whose report you want to view.
3. Click the report under the task node in the console tree.

The report view appears in the details pane. Reports are task-specific; in order to view reports produced by multiple tasks, you will have to expand each task and view each task's corresponding report.

Tasks Node

All discovery tasks along with their log and reports are available in the console tree under **DeviceLock Content Security Server** > **Discovery Server** > **Tasks**.
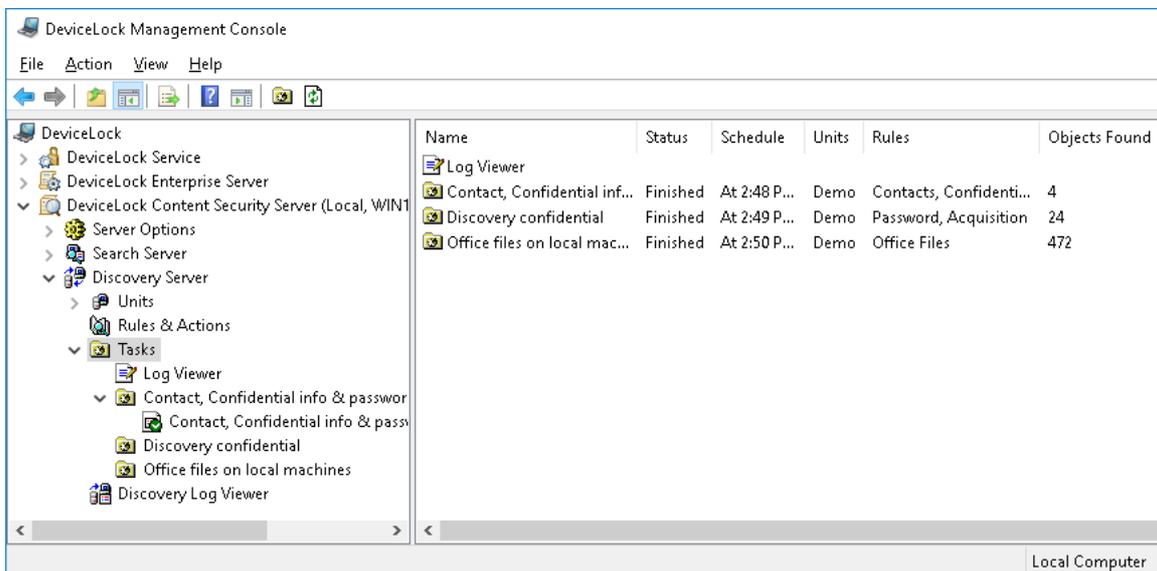
Select the **Tasks** node in the console tree to view a list of discovery tasks. The list in the details pane displays the following information on each task:

- **Name** - The name of the task.

- **Status** - One of the following:

  - **Canceled** - The task was launched and manually canceled via the task's shortcut menu. No report is created for canceled tasks.

  - **Expired** - The task was launched but never reported back, and was discarded after the expiration of Keep-alive timeout for one or more computers specified in the task.

    The **Expired** status is also assigned for tasks terminated after the time specified in Stop task if runs longer than has expired.

    If the task is expired, reports are created based on all information received from the agents prior to expiration.

  - **Failed** - The task failed to execute on all computers scheduled to be scanned by the task (for example, if all computers were unavailable).

    The report will be created containing the **Failed to scan** table listing the computers that failed to scan and including the failure reason.

- **No License** - The task was launched, but the installed license was insufficient to scan at least one resource. The report will be created.
- **Finished** - The task has successfully completed and will not be recurred. The report will be created.
- **Running** - The task is running.
- **Waiting** - The task was not and will not be launched (e.g. the **Active** flag is not set).
- **Scheduled** - The task is scheduled to run in the future. This status does not specify whether or not the task was ever executed in the past.
- **Schedule** - Identifies the task schedule.
- **Units** - Lists the units specified in the task.
- **Rules** - Lists the rules specified in the task.
- **Objects Found** - The number of objects discovered by the task.
- **Warnings** - The number of warnings issued by the task.
- **Errors** - The number of scanning errors the task encountered.

The shortcut menu on the **Tasks** node includes the following commands:

- **Create Task** - Creates a new task. You can specify the desired task settings in the dialog boxes that appear when you select this command.
- **Refresh** - Updates the list of tasks with the latest information.

The shortcut menu on a task in the details pane includes the following commands:

- **Edit Task** - Opens the dialog boxes where you can view or change the settings of the selected task.
- **Duplicate Task** - Creates a new task with the settings copied from the selected task. You can view or change the settings of the new task in the dialog boxes displayed by this command.

    By default, the new task name is composed of the **Copy of** prefix followed by the name of the selected task. When you create two or more copies of a task, the new task name includes a numeric suffix indicating the number of the copy.
- **Delete Task** - Deletes the selected task.

    If a given task was ever run, and thus has any reports, then the console prevents deletion of that task. To delete such a task, you first need to delete the task's reports.
- **Run Task** - Causes immediate execution of the selected task. You can run any task except of those already running.
- **Stop Task** - Causes immediate stop of the selected task. This command replaces the **Run Task** command for the tasks that are currently running.
- **Generate New Report** - Initiate report generation. Depending on the context, this command can be used as follows:
    - During task execution - If the task is currently running and has some progress, report generation is not possible.
    - After task finished - You can re-create reports in some time after the task finished.

        This can be used to produce the complete report if some tasks finished after the Keep-alive timeout has expired. Is this is the case, agents that took longer than that to finish their jobs will report back to the server; the server will collect logs from these agents, but the report will not re-generate automatically. By using **Generate New Report**, you will produce the most complete report using all available information.
- **Refresh** - Updates the list of tasks with the latest information.

Creating a Task

Tasks are created with a wizard. To create a task, do the following:

1. Open the task creation wizard:

   - In the DeviceLock Management Console, expand **DeviceLock Content Security Server** > **Discovery Server** > **Tasks**, right-click **Tasks**, and then click **Create Task** on the shortcut menu.

2. In the **Select Units** dialog box that appears, select the units that will be scanned by the task:

   - Select one or more units in the **Available Units** list, and then click **Add**. You can select multiple units by holding down the SHIFT or CTRL key while clicking them. The units you have added will appear in the **Selected Units** list.

     Note: You may review unit properties by clicking the **View** button while a unit is selected. In the **View Unit** dialog box that appears, you will not be able to change any unit settings.

3. Click **Next** to continue.

4. In the **Select Rules & Actions** dialog box that appears, select the rules that will be applied by the task:

   - Select one or more rules in the **Available Rules & Actions** list, and then click **Add**. You can select multiple rules by holding down the SHIFT or CTRL key while clicking them. The rules you have added will appear in the **Selected Rules & Actions** list.

     Note: You may review rule properties by clicking the **View** button while a rule is selected. In the **View Rule** dialog box that appears, you will not be able to change any rule settings.

5. Click **Next** to continue.

6. In the **Set Task Schedule & Advanced Settings** dialog box that appears, you can change the name of the task, configure the task to run on a scheduled basis, and specify additional settings that affect execution of the task:

   - **Task Name** - Identifies the name of the task. The task will appear under that name in the management console.

   - **Active** - Select this check box to activate the task according to the schedule, or clear to deactivate it.

     If the **Active** check box is not selected, the task will not be executed by the schedule.

   - **Schedule** - To configure a schedule for the task, use the following options:

     - **One Time** - The task will be launched once on the time and date specified. Choose the date and time to run the task, or select the **Now** check box to run the task right after it has been created or modified.

       Note: If you specify a date/time in the past, the following message is displayed when you click **Next**: "The specified date is earlier than the current date."

     - **Hourly** - The task will be executed on an hourly basis. The task will recur after the specified number of hours. You will be able to specify the number of hours to pass between scheduled scanning attempts.

     - **Daily** - The task will be executed on a daily basis. The task will recur after the specified number of days. You will be able to specify the number of days to pass between scheduled scanning attempts.

- **Weekly** - The task will be executed on a weekly basis. The task will recur after the specified number of weeks. You will be able to specify the number of weeks to pass between scheduled scanning attempts, and set days of weeks on which the scanning task will be executed.

- **Monthly** - The task will be executed every month on a specified day. You will be able to specify calendar months on which the task will be executed. You will be also able to specify calendar days of month or days of week on which the scanning task will be executed.

> **Note:** If you configure a recurrent task, the task will run periodically according to a set schedule. If, however, a task execution does not finish before a next run of the task upon schedule, the next run of that task is delayed until the preceding execution of the task has finished.

- **Advanced Settings** - Use these settings to control the task's behavior during execution:

  - **Stop task if runs longer than** - Specifies that the task will be force stopped if it takes longer than a specified period of time to complete.

    This setting is used to ensure successful automated operation even if the rules are too complex or the scanned data set too big to complete on a timely basis.

  - **Scan priority** - Specifies process priority and sets the amount of simultaneous scanning threads depending on the number of available processors and/or processor cores.

    - The **Below Normal** or **Low** setting will only use one processor/core for scanning and set the "Below Normal" or "Low" process priority, respectively.

    - The **Above Normal** or **Normal** setting will use one half of all available processors/cores and set the "Above Normal" or "Normal" process priority, respectively.

    - The **High** setting will use all available processors/cores except one, and set the "High" process priority.

    - The **Realtime** setting will devote all available processors/cores to the scanning task, and set "Realtime" priority to the process.

  - **Number of retries** - The number of times that will be performed if the scanning attempt returns status indicating an error. The value of **0** means that no retries will be performed if the first attempt fails.

- **Retry timeout** - Specifies how many seconds DeviceLock waits before attempting to perform the next scanning attempt in the case the previous attempt failed.

Number of retries:	5
Retry timeout:	1200 sec

- **Keep-alive timeout** - Specifies the number of hours the server will wait for each agent to collect scanning logs. If no logs were collected after the timeout has passed, the server will stop waiting for that agent.

Keep-alive timeout:	24 hour(s)

If the agent reports later on and after the timeout has passed, the logs will be collected and processed as usual.

7. Click **Next**. The confirmation dialog will appear listing parameters of the newly created task. Click **Finish** to complete the wizard. The newly created task will be saved and scheduled.

You can edit, delete, duplicate or run tasks, refresh task list or generate a new report by using the task's shortcut menu. For description of the menu, see Tasks Node earlier in this document.

Task and Its Reports

The console displays discovery tasks in the console tree under **DeviceLock Content Security Server** > **Discovery Server** > **Tasks**.

The shortcut menu on a discovery task in the console tree includes the same commands as the task's shortcut menu in the details pane (for description of commands, see Tasks Node earlier in this document).

When you select a discovery task in the console tree, the details pane lists the reports produced by that task. The list in the details pane displays the following information on each report:

- **Name** - Report name. By default, includes the task name followed by the date and time of the task run.

- **Type** - One of the following:

    - **Scheduled** - Report generated automatically upon task completion.

    - **Manual** - Report generated by hand, using the **Generate New Report** command.

- **Status** - One of the following:

    - **Generating** - Report creation is in progress.

    - **Ready** - Report created successfully.

    - **Error** - Report encountered an error.

- **Objects Found** - The number of objects discovered by the task.

- **Warnings** - The number of warnings issued by the task.

- **Errors** - The number of scanning errors the task encountered.

- **Started** - Date and time that the report creation started.

- **Finished** - Date and time that the report creation was completed.

- **Scheduled by** - Identifies the user account that started the task (in case of report type of **Scheduled**) or generated the report (in case of report type of **Manual**).

- **Scheduled from** - Identifies the computer from which the task was started (in case of report type of **Scheduled**) or the report was generated (in case of report type of **Manual**).

The shortcut menu on a report in the details pane includes the following commands:

- **Open** - Displays the report in the details pane. This command is available for reports with the status of **Ready** (green icon).

    Another way to open a task's report is by selecting the report under the node representing that task in the console tree.

- **Show error** - Displays error information about the report. This command is available for reports with the status of **Error** (red icon).

- **Rename** - Changes the name of the selected report. You can specify a new name in the dialog box displayed by this command.

- **Delete Report** - Deletes the selected report.

    You can delete multiple reports at a time: Click while holding down Shift or Ctrl to select reports, right-click the selection, and then click **Delete Reports**.

- **Generate New Report** - Appears on the menu when you select multiple reports. Generates a single aggregated report by using information available in all selected reports.

- **Refresh** - Updates the list of reports with the latest information.

Viewing Report List

Each task produces reports detailing the scanning results in a human-readable form. To access reports, do the following:

1. Open the DeviceLock Management Console.

2. In the console tree, expand **DeviceLock Content Security Server** > **Discovery Server** > **Tasks**.

3. Under the **Tasks** node, select and expand the node that represents the task whose report you want to access.

    The list of the given task's reports appears in under the task node in the console tree as well as in the details pane on the right of the console tree:
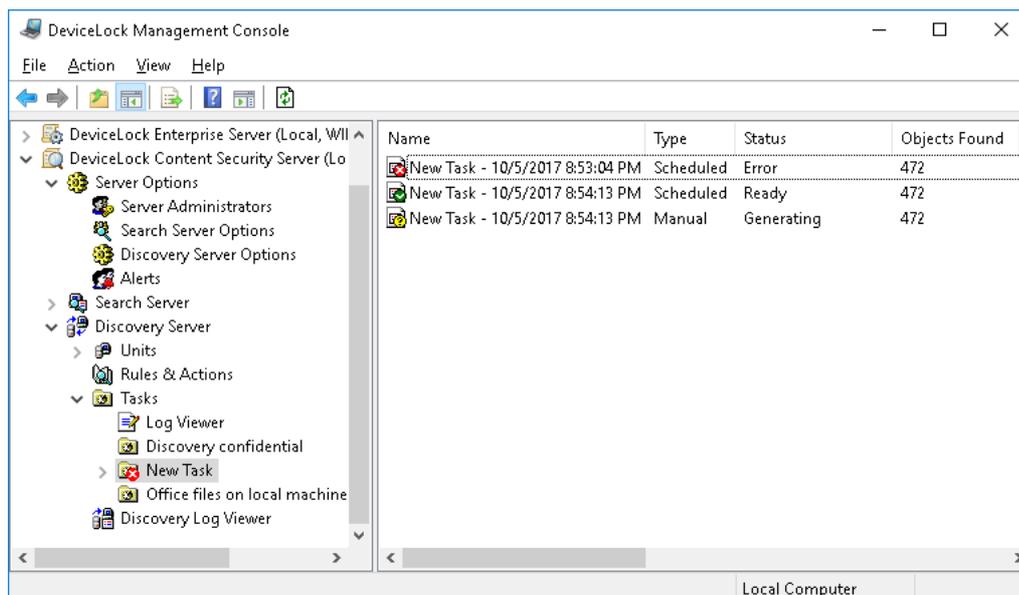
The following types of report are available:

- **Scheduled** - Reports automatically generated after the task finishes.
- **Manual** - Reports manually generated by the user via the **Generate New Report** command.

The icon in the first column represents report status. The following statuses are available:

- **Generating** - A yellow icon. The report is being generated. Wait for the generation to finish before opening the report.
- **Ready** - A green icon. Double-click on the report to open.
- **Error** - A red icon. Double-click on the report to view details about the error.

For more information, see description of the report list in the Task and Its Reports section.

To manage reports, select one or more reports in the details pane, right-click the selection, and use the commands from the shortcut menu. Description of commands can be found in the Task and Its Reports section earlier in this document.

> **Tip:** To select multiple reports, click while holding down the Shift or Ctrl key.

Viewing a Report

When you expand the node representing a discovery task in the console tree, and select a report under that node, the details pane displays report pages. Another way to view a report is by using the **Open** command on the shortcut menu or by double-clicking the report list item in the details pane.

The shortcut menu on a report in the console tree includes the following commands:

- **Open** - Displays the report in the details pane.
- **Rename** - Changes the name of the report. You can specify a new name in the dialog box that appears.
- **Delete Report** - Deletes the selected report.
- **Refresh** - Updates the report in the details pane.

DeviceLock Discovery Server generates multi-page reports in HTML format.

> **Note:** If JavaScript is not enabled in your Web browser, the following error appears when viewing a report: "For full functionality of this page it is necessary to enable JavaScript. See your web browser manual or help on how to enable JavaScript."
>
> To view reports, enable JavaScript in your Web browser. For instructions, see the "How to enable JavaScript in your browser" guide at http://www.enable-javascript.com.

Discovery Server allows automatic or manual generation of reports using data returned by scanning agents. Use reports to arrange and display information about discoveries and actions performed by the scanning agents.

Reports are created automatically by the tasks. You can also generate reports manually by using DeviceLock Management Console.

The report contains detailed information about the results of the scan.

The first page of the report may contain the following information:

- **Header** - Displays the name of the report, and contains information about the beginning and end of the scan, the name of the user who requested the report, and the name of the computer that initiated the reporting.

- **Discovery results** - Contains a summary of discovery results and actions performed on the discovered content. If the discovery task did not make any discoveries, this section displays **Discovery results: None**.

  Information in this section includes:

  - **Object Name** - Lists the rules and units within which the rule made a discovery.

  In the list of rules and units, the report displays the following information:

  - **Log** - Indicates how many discovery events have been logged.
  - **Alert** - Indicates how many administrator alert about the discovery have been sent.
  - **Notify** - Indicates how many user notifications about the discovery have been displayed.
  - **Delete** - Indicates the number of occurrences where detected content has been deleted.
  - **Encrypt** - Indicates the number of occurrences where detected files have been encrypted.
  - **Set Permissions** - Indicates the number of occurrences where file access permissions on detected content have been modified.
  - **Warnings** - Indicates the number of file access errors, content analysis errors and errors applying actions to discovered files.

- **Rules** - This section contains descriptions of all rules specified in the task, including those not included into the **Discovery results** table.

- **Failed to scan** - If there are one or more computers that failed to scan, this report will contain an error summary. The following information is available:

  - **Unit/Computer** - Lists units containing computers that failed to scan.

  - **Error message** - Description of the error preventing the computer from being scanned.

  - **Date/Time** - The date and time of error.

> **Note:** It is essential to note that many items in the report are clickable links. Clicking a certain element may transfer you to a different page in the report (opening detailed view for the item you clicked), or open the **Log Viewer** with pre-filled filter to display all records relevant to the item that was clicked. For example, clicking the number in the **Total** line opens the **Log Viewer**, and displays all actions calculated in the referring table.
>
> For more information and instructions on how to work with reports, see Navigating Reports.

You may click the plus sign **[+]** on the left of each object to expand. If you want to expand all objects, click the plus sign **[+]** on the left of the **Object Name** heading.

Subsequent pages contain detailed information, including:

- **Header** - Displays the name of the report, and contains information about the beginning and end of the scan, the name of the user who requested the report, and the name of the computer that initiated the reporting.

- **Discovery results** - Contains the list of scanned computers. You can click a computer name to expand the list. When expanded, the table will show the names of the files that were detected.

  > **Note:** You can switch the order in which computers and files are displayed, making file names appear as expandable branches and computer names as items. The order depends on the type of the link you clicked to get to this report.
  >
  > For more information on switching the computer/file display order, see Navigating Reports.

  Information in this section includes:

  - **Object Name** - Lists computer names and file names, depending on viewing mode. Displays either all computers containing discovered files matching the appropriate rule and unit, or all discovered files matching the appropriate rule and unit, with the list of computers on which they were found.

  In the list of computers and files, the report displays the following information:

  - **Log** - Indicates how many discovery events have been logged.

  - **Alert** - Indicates how many administrator alert about the discovery have been sent.

  - **Notify** - Indicates how many user notifications about the discovery have been displayed.

  - **Delete** - Indicates the number of occurrences where detected content has been deleted.

  - **Encrypt** - Indicates the number of occurrences where detected files have been encrypted.

  - **Set Permissions** - Indicates the number of occurrences where file access permissions on detected content have been modified.

  - **Warnings** - Indicates the number of file access errors, content analysis errors and errors applying actions to discovered files.

Note: Certain items in the Detailed Report are clickable. Clicking a file name or computer name will expand the list of linked computers (or files), whereas clicking an underlined number will open the **Log Viewer**.

For more information and instructions on how to work with reports, see Navigating Reports.

Flat table view is also available, listing all files discovered during the scan by the rule, or all computers on which at least one discovery was made by the rule. There are no sub-items in flat view. Clicking a file opens the list of computers on which it was discovered (according to the rule). Clicking a computer opens the list of files discovered on that computer (according to the rule).

In the flat table view, the following information is available:

- **Header** - Displays the name of the report, and contains information about the beginning and end of the scan, the name of the user who requested the report, and the name of the computer that initiated the reporting.

- **Discovery results** - Contains the list of files and computers discovered by the combination of units and rules. This list may be displayed in one of the following views depending on the link used to get to the flat table view.

    - **Object Name**:

        - **Computers for** <FileName> **for** <UnitName> **and** <RuleName> - Lists all computers on which a certain file was discovered by a certain rule in a certain unit.

          - OR -

        - **Computers for** <FileName> **for** <RuleName> - Lists all computers on which a certain file was discovered by a certain rule.

          - OR -

        - **Files for** <ComputerName> **for** <UnitName> **and** <RuleName> - Lists all files discovered on a certain computer by a certain rule for a certain unit.

          - OR -

        - **Files for** <ComputerName> **for** <RuleName> - Lists all files discovered on a certain computer by a certain rule. If a file has more than one name (has different aliases), the number of aliases will be displayed in parenthesis after the file name.

    In all of these views, the file, computer, rule, and unit names are specified by the <FileName>, <ComputerName>, <RuleName> and <UnitName> variables, respectively.

    In the list of computers and files, the report displays the following information:

    - **Log** - Indicates how many discovery events have been logged.

    - **Alert** - Indicates how many administrator alert about the discovery have been sent.

    - **Notify** - Indicates how many user notifications about the discovery have been displayed.

    - **Delete** - Indicates the number of occurrences where detected content has been deleted.

    - **Encrypt** - Indicates the number of occurrences where detected files have been encrypted.

    - **Set Permissions** - Indicates the number of occurrences where file access permissions on detected content have been modified.

    - **Warnings** - Indicates the number of file access errors, content analysis errors and errors applying actions to discovered files.

The final report type is alias view. If the same file has different names, these names are called aliases. On this report page, the first table lists file names that triggered a discovery rule. Clicking a file name expands the list of computers that contained a file with that name during the scan. You can also expand the list by clicking the plus sign **[+]** to the left of the file name, opening the list of computers on which a file with a given name was discovered.

The alias view has two tables. The first table is the alias table; the second table lists computers that contain a given file known under aliases listed in the first table. In the alias view, the following information is available:

- **Header** - Displays the name of the report, and contains information about the beginning and end of the scan, the name of the user who requested the report, and the name of the computer that initiated the reporting. In addition, the header contains information about the computer, unit and rule for the flat table.

- **Aliases** - Contains the list of aliases (different names of the same file) discovered by the combination of units and rules on a given computer. This information includes:

  - **Object Name** - Lists all names of the file that was discovered by one of the detection rules. Under each file name you can find a list of all computers where the file was discovered.

  In the list of files, the report displays the following information:

  - **Log** - Indicates how many discovery events have been logged.

  - **Alert** - Indicates how many administrator alert about the discovery have been sent.

  - **Notify** - Indicates how many user notifications about the discovery have been displayed.

  - **Delete** - Indicates the number of occurrences where detected content has been deleted.

  - **Encrypt** - Indicates the number of occurrences where detected files have been encrypted.

  - **Set Permissions** - Indicates the number of occurrences where file access permissions on detected content have been modified.

  - **Warnings** - Indicates the number of file access errors, content analysis errors and errors applying actions to discovered files.

- **Discovery results** - Lists computers that contain a file known under the names listed in the **Aliases** table above. This information includes:

  - **Object name** - All computers containing a given file are listed under the corresponding file name.

  In the list of computers and files, the report displays the following information:

  - **Log** - Indicates how many discovery events have been logged.

  - **Alert** - Indicates how many administrator alert about the discovery have been sent.

  - **Notify** - Indicates how many user notifications about the discovery have been displayed.

  - **Delete** - Indicates the number of occurrences where detected content has been deleted.

  - **Encrypt** - Indicates the number of occurrences where detected files have been encrypted.

  - **Set Permissions** - Indicates the number of occurrences where file access permissions on detected content have been modified.

  - **Warnings** - Indicates the number of file access errors, content analysis errors and errors applying actions to discovered files.

If you click a file name in the **Aliases** table, the report displays a full list of computers containing the discovered file with a matching name. In other words, the report will list the files matching both the hash (checksum) and the particular file name.

Navigating Reports

DeviceLock Discovery Server generates dynamic reports with comprehensive navigation structure. These reports enable you to receive detailed information about most items in the report by clicking an item. Most elements in the report are clickable links. Clicking a certain element may transfer you to a different page in the report (opening detailed view for the item you clicked), or open the Log Viewer with pre-filled filter to display all records relevant to the item you clicked.

Discovery results

The first column of the **Discovery results** table contains a number of clickable items. Clicking a rule or unit displays a shortcut menu.

If you click a rule, the following items are available on the shortcut menu:

- **Computers for Rule** - Displays a list of all computers on which content matching the rule was discovered.
- **Files for Rule** - Displays a list of all files in which content matching the rule was discovered.

If you expand a rule and click one of the units, the following items are available on the shortcut menu:

- **Computers for Unit and Rule** - Displays a list of computers held in the selected unit on which content matching the rule was discovered.
- **Files for Unit and Rule** - Displays a list of files from computers held in the selected unit in which content matching the rule was discovered.

Certain numbers in the table are clickable. If you hover a mouse over such numbers, they become underlined. Clicking an underlined number in the table opens the **Log Viewer** as described in the Links to Log Viewer section.

Failed to scan

Report section **Failed to scan** lists all units containing computers that failed to scan. Clicking a unit opens a list of computers accompanied with corresponding error messages and date and time of the error. You may encounter the following error messages:

- **Computer is unavailable** - The computer was not available during the scan (e.g. turned off or not connected to the network).
- **Installation failed** - The installation of the scanning agent was not successful.
- **Access is denied** - There was a problem with configured access credentials or certificate.
- **No License** - You have exceeded the number of computers to scan permitted by your license. You may wish to upgrade your license to cover additional computers.

Details Table

When you click one of the four menu items described in the Discovery results section above, you are transferred to the corresponding **Details Table**. If you click a computer, you are presented with all files discovered by the corresponding rule. If you click a file, you will be viewing all computers on which that file has been discovered by the corresponding rule. Which particular view is displayed is indicated in the **Discovery results** line.

Certain numbers in the table are clickable. If you hover a mouse over such numbers, they become underlined. Clicking an underlined number in the table opens the **Log Viewer** as described in the Links to Log Viewer section.

The number of entries for all tables can be adjusted by changing the following registry values:

- Key: `HKEY_CURRENT_USER\SOFTWARE\SmartLine Vision\DLManager\Manager`

    - Value: `DisplayRootCount=dword:<number_of_root_elements>`

      The default value is 500.

    - Value: `DisplayChildCoun=dword:<number_of_child_elements>`

      The default value is 50.

By default, at most 500 root elements (nodes) and 50 sub-nodes of each node will be listed.

Rules Section

The **Rules** section lists the rules used in this scan. Clicking a rule name opens the **Rules & Actions** view, with that rule being selected in the details pane.

Links to Log Viewer

If you need more details about a certain item in one of the report tables, you may click an underlined item in the header or an underlined number in the table. This will open the **Log Viewer**, with the **Filter** options set to ensure that only relevant records are displayed.

The filtering rule is a logical AND of all relevant fields, and is generated as follows:

<ReportID> AND <ColumnName> AND <RuleName> (if available) AND <UnitName> (if available).

The resulting filter is applied to the **Log View**, and you will see only those entries that match the filtering rule. As a result, you will always have **Log Viewer** display information that is relevant to your click. You can reset the filter and view full log results by using the **Reset Filter** command.

Tasks Log Viewer

This viewer allows you to retrieve the log files produced by discovery tasks. Discovery tasks use this log to write information about scanning activities, discoveries and actions taken to discovered content.

To access the tasks log, do the following:

1. Open the DeviceLock Management Console.

2. In the console tree, expand **DeviceLock Content Security Server** > **Discovery Server** > **Tasks**, and then select **Log Viewer** under the **Tasks** node.
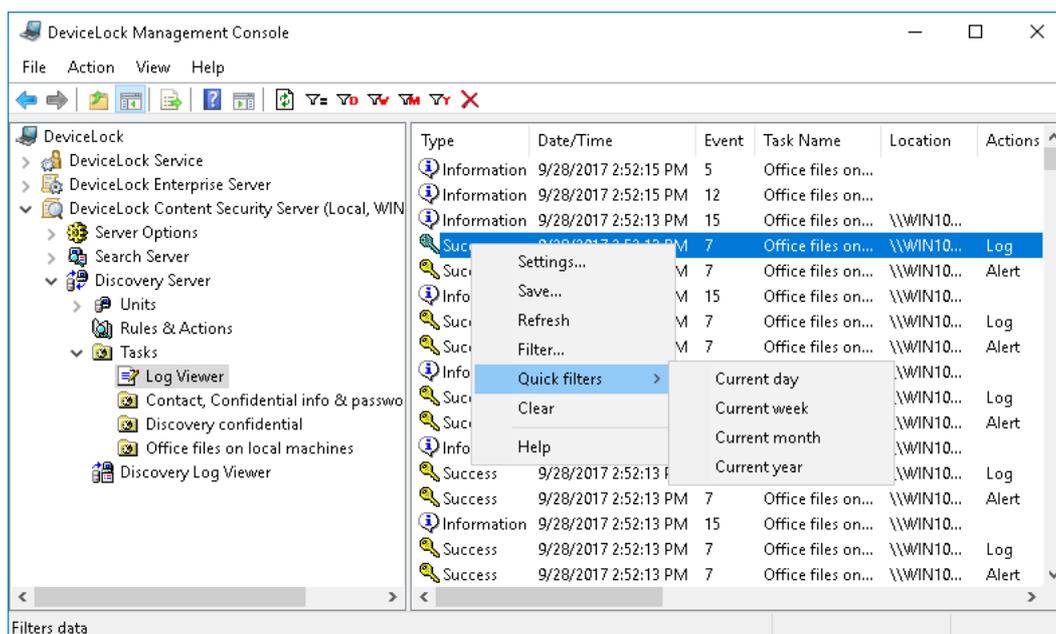
The details pane displays a list of events, with the following information on each event:

- **Type** - Event type indicates one of the following:

  - **Success** - Task or operation completed successfully.

  - **Information** - Certain action performed.

  - **Warning** - A problem might occur unless action is taken.

  - **Error** - A problem has occurred.

- **Date/Time** - Date and time that the event occurred.

- **Event** - ID number of the event.

- **Task Name** - Identifies the discovery task that caused the event.

- **Location** - The name of the resource the event is related to.

- **Actions** - Identifies the action performed by the task on the detected content, such as:

  - **Alert** - Sending an alert that informs about the detected content.

  - **Delete** - Deletion of the detected content.

  - **Delete (Safe Delete)** - Deletion using a secure erase procedure as defined in US DoD 5220.22-M.

  - **Encrypt** - Encrypting the detected content by using Windows EFS (Encrypted File System).

  - **Log** - Recording an event to the Discovery tasks log that informs about the detected content.

  - **Notify** - Notifying the computer user about the detected content.

  - **Set Permissions** - Setting certain file system permissions on the detected files.

- **Name** - The name of discovered file.

- **Reason** - The cause of the event, such as:

  - **Completed** - Completion of the discovery task.

  - **Content-Aware Rule error** - Discovery rule application error.

  - **On request** - Discovery task started by hand.

  - **On schedule** - Discovery task started by a schedule.

  - **Rule** - Discovery rule triggered. The reason specifies the name of the rule followed by a brief description of the content matches, keywords, and/or file types that led to the rule triggering.

- **Information** - Detailed description of the event that includes details of the actions performed and errors encountered.

- **Unit** - The name of the unit that invoked the event.

- **Received Date/Time** - The date and time when the event was received by DeviceLock Discovery Server.

Managing the Tasks Log

You can manage the log by using commands from the shortcut menu:

- In the console tree, expand **DeviceLock Content Security Server** > **Discovery Server** > **Tasks**, and then right-click **Log Viewer** under the **Tasks** node.

    - OR -

    In the console tree, select **DeviceLock Content Security Server** > **Discovery Server** > **Tasks** > **Log Viewer**, and then right-click any list record in the details pane.

The shortcut menu provides the following log management commands (next to the command name is the toolbar button corresponding to that command):

- **Settings** 🗗 - View or change the settings that limit the maximum number of event records the log may contain. For instructions, see To view or change Discovery tasks log settings.

- **Save** - Saves the log to the file you specify.

- **Refresh** 🗐 - Updates the list of events with the latest information.

- **Filter** ▽▫ - Displays only the events that match the conditions set. For instructions, see To configure the Discovery tasks log filter.

- **Quick filters** - Choose from the following options to display only records for a certain period of time:

    - Current day ▽ᴅ
    - Current week ▽ᴡ
    - Current month ▽ᴍ
    - Current year ▽ʏ

    Note: To cancel the selected quick filter option, choose that option again. A regular filter applied by the **Filter** command disables the quick filters and removes the current quick filter, if any applied. Remove the regular filter to use a quick filter.

- **Clear** ✕ - Delete all records that currently exist in the log.

    This command also adds a deletion record to the log, indicating how many records have been deleted as well as who performed the deletion and from what computer.

To view or change Discovery tasks log settings

1. Click **Settings** on the shortcut menu.

2. View or change log settings in the dialog box that appears.

The following log settings are available:

- **Control log size** - Select this check box to allow the server to control the number of records in the log and delete outdated records. If this check box is cleared, the server uses all available database space to store the log.

- **Keep events for last** <number> **days** - Store records no older than a certain number of days. Then, specify the desired number of days. The default setting is 365 days.

- **Maximum log size:** <number> **records** - Store no more than a certain number of records. If you select this option, specify the desired number of records, and select the server action to be performed when the log reaches the maximum size:

  - **Overwrite events as needed** - New event records continue to be stored when the maximum log size is reached. Each record of a new event replaces the oldest record in the log.

  - **Overwrite events older than** <number> **days** - New event records replace only records stored longer than the number of days specified. The supported setting is up to 32,767 days.

  - **Do not overwrite events (clear log manually)** - New event records are not added when the maximum log size is reached. To enable the server to add new records, the log must be cleared by hand.

> **Important:** If the log has no space for new records and log settings do not allow the deletion of old records, then the server does not add any new records to the log.

To use the default log size, select the option **Maximum log size** and click **Restore Defaults**. The default log size settings are as follows:

- Maximum log size: 10,000 records

- Overwrite events older than 7 days

To configure the Discovery tasks log filter

1. Click **Filter** on the shortcut menu.

2. View or change filter settings in the dialog box that appears.

Two filter types are available:

- **Include** - The console displays only the events that match these conditions. To set up and apply these conditions, select the **Enable filter** check box on the **Include** tab.

- **Exclude** - The console does not display the events that match these conditions. To set up and apply these conditions, select the **Enable filter** check box on the **Exclude** tab.

The filter can be temporarily disabled by clearing the **Enable filter** check box.

> **Note:** The mark next to the tab name turns green if the filter on that tab is enabled. Otherwise, the mark is gray.

When the filter enabled, its conditions are defined by entering values into the following fields:

- **Event types** - Select check boxes to filter events by type:

    - **Success** - Task or operation completed successfully.

    - **Information** - Certain action performed.

    - **Warning** - A problem might occur unless action is taken.

    - **Error** - A problem has occurred.

- String fields that allow you to include or exclude events depending upon whether event data matches the filter string specified. For example, to filter events by the name of the task that caused the event, specify a filter string in the **Task name** field. To filter events with certain IDs, enter ID numbers separated by a semicolon in the **Event ID** field.

  The following string fields are available:

  - **Event ID** - ID number of the event.

  - **Task name** - The name of the task that caused the event.

  - **Location** - The name of the resource the event is related to.

  - **Action** - The name of the action that caused the event. You can type or select a name from the following list:

    - **Alert** - Means sending an alert that informs about the detected content.

    - **Delete** - Indicates deletion of the detected content.

    - **Delete (Safe Delete)** - Means deletion using a secure erase procedure as defined in US DoD 5220.22-M.

    - **Encrypt** - Indicates encrypting the detected content by using Windows EFS (Encrypted File System).

    - **Log** - Means recording an event to the Discovery tasks log that informs about the detected content.

    - **Notify** - Means notifying the computer user about the detected content.

    - **Set Permissions** - Indicates setting certain file system permissions on the detected files.

  - **Name** - The name of the discovered file.

  - **Reason** - The reason that triggered the event. You can type or select a reason from the following list:

    - **Completed** - Completion of the discovery task.

    - **Content-Aware Rule error** - Discovery rule application error.

    - **On request** - Discovery task started by hand.

    - **On schedule** - Discovery task started by a schedule.

    - **Rule** - Discovery rule application.

  - **Information** - Detailed description of the event that includes details of the actions performed and errors encountered

  - **Unit** - The name of the unit that invoked the event.

Note: To assist with configuring a filter, string setting fields store previous entries and suggest matches for what is being typed. Previous entries are also available on the drop-down list of options for the setting field.

- **Generated Date/Time** - In this area, the following fields can be used to specify the event range by the date and time that the event occurred:
  - **From** - The beginning of the event range to match. Possible values: **First Record** (selected by default) and **Records On**. Select **First Record** to match events starting from the first one recorded in the log. Select **Records On** to match events that occurred later than a specific date and time.
  - **To** - The end of the event range to match. Possible values: **Last Record** (selected by default) and **Records On**. Select **Last Record** to match events up to the last one recorded in the log. Select **Records On** to match events that occurred earlier than a specific date and time.
- **Received Date/Time** - In this area, the following fields can be used to specify the event range by the date and time when the event was received by Discovery Server:
  - **From** - The beginning of the event range to match. Possible values: **First Record** (selected by default) and **Records On**. Select **First Record** to match events starting from the first one recorded in the log. Select **Records On** to match events that were received later than a specific date and time.
  - **To** - The end of the event range to match. Possible values: **Last Record** (selected by default) and **Records On**. Select **Last Record** to match events up to the last one recorded in the log. Select **Records On** to filter events that were received earlier than a specific date and time.

When configuring a filter, consider the following:

- Filter conditions are combined by AND logic, that is, a given record matches the filter if it matches each of the filter conditions. Clear the fields that are not to be used in the filter conditions.
- Filter string fields may include wildcards, such as an asterisk (*) or a question mark (?). An asterisk represents zero or more characters; a question mark represents any single character.
- A filter string field may include multiple values separated by a semicolon (;). In this case, the values are combined by OR logic, that is, a given record matches the filter condition on a particular field if it matches at least one of the values specified in that field.
- The **Clear** button in the **Filter** dialog box provides the option to remove all the defined filter conditions and start setting up a new filter from scratch.
- The **Save** and **Load** buttons in the **Filter** dialog box are used to save the filter conditions to a file and to load previously saved filter conditions from a file.

Discovery Log Viewer

This viewer allows you to retrieve DeviceLock Discovery Server's internal log. The server uses this log to record errors, warnings and other important information (such as configuration changes, start/stop events, and so on). Unlike the Tasks Log, the Discovery Log contains information that has no direct relation to scanning tasks.

You may use the information from this log to diagnose problems (if any), to monitor changes in the server's configuration and to see who has cleared logs and when.

To access the DeviceLock Discovery Server log, do the following:

1. Open the DeviceLock Management Console.

2. In the console tree, expand **DeviceLock Content Security Server** > **Discovery Server**, and then select **Discovery Log Viewer** under the **Discovery Server** node.
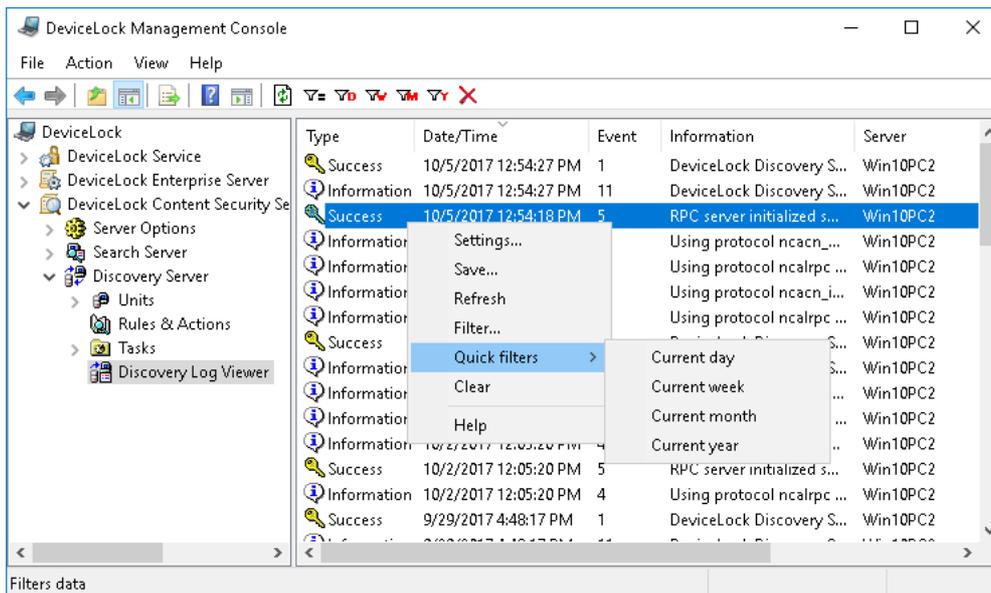
The details pane displays a list of events, with the following information on each event:

- **Type** - Event type indicates one of the following:

  - **Success** - Task or operation completed successfully.

  - **Information** - Certain action performed.

  - **Warning** - A problem might occur unless action is taken.

  - **Error** - A problem has occurred.

- **Date/Time** - The date and time that the event occurred.

- **Event** - ID number of the event.

- **Information** - Detailed description of the event that includes details of the actions performed and errors encountered.

- **Server** - Identifies the computer on which the event has occurred.

- **Record N** - Sequence number of the event record in the list.

Managing the Discovery Log

You can manage the log by using commands from the shortcut menu:

- In the console tree, expand **DeviceLock Content Security Server** > **Discovery Server**, and then right-click **Discovery Log Viewer** under the **Discovery Server** node.

  - OR -

- In the console tree, select **DeviceLock Content Security Server** > **Discovery Server** > **Discovery Log Viewer**, and then right-click any list record in the details pane.

The shortcut menu provides the following log management commands (next to the command name is the toolbar button corresponding to that command):

- **Settings** - View or change the settings that limit the maximum number of event records the log may contain. For instructions, see To view or change Discovery log settings.

- **Save** - Saves the log to the file you specify.

- **Refresh** - Updates the list of events with the latest information.

- **Filter** - Displays only the events that match the conditions set. For instructions, see To configure the Discovery log filter.

- **Quick filters** - Choose from the following options to display only records for a certain period of time:

  - Current day
  - Current week
  - Current month
  - Current year

  > **Note:** To cancel the selected quick filter option, choose that option again. A regular filter applied by the **Filter** command disables the quick filters and removes the current quick filter, if any applied. Remove the regular filter to use a quick filter.

- **Clear** - Delete all records that currently exist in the log.

  This command also adds a deletion record to the log, indicating how many records have been deleted as well as who performed the deletion and from what computer.

To view or change Discovery log settings

1. Click **Settings** on the shortcut menu.

2. View or change log settings in the dialog box that appears.

The following log settings are available:

- **Control log size** - Select this check box to allow the server to control the number of records in the log and delete outdated records. If this check box is cleared, the server uses all available database space to store the log.

- **Keep events for last** <number> **days** - Store records no older than a certain number of days. Then, specify the desired number of days. The default setting is 365 days.

- **Maximum log size:** <number> **records** - Store no more than a certain number of records. Then, specify the desired number of records, and select the server action to be performed when the log reaches the maximum size:

  - **Overwrite events as needed** - New event records continue to be stored when the maximum log size is reached. Each record of a new event replaces the oldest record in the log.

  - **Overwrite events older than** <number> **days** - New event records replace only records stored longer than the number of days specified. The supported setting is up to 32,767 days.

  - **Do not overwrite events (clear log manually)** - New event records are not added when the maximum log size is reached. To enable the server to add new records, the log must be cleared by hand.

    Important: If the log has no space for new records and log settings do not allow the deletion of old records, then the server does not add any new records to the log.

To use the default log size, select the option **Maximum log size** and click **Restore Defaults**. The default log size settings are as follows:

- Maximum log size: 10,000 records

- Overwrite events older than 7 days

To configure the Discovery log filter

1. Click **Filter** on the shortcut menu.

2. View or change filter settings in the dialog box that appears.

Two filter types are available:

- **Include** - The console displays only the events that match these conditions. To set up and apply these conditions, select the **Enable filter** check box on the **Include** tab.

- **Exclude** - The console does not display the events that match these conditions. To set up and apply these conditions, select the **Enable filter** check box on the **Exclude** tab.

The filter can be temporarily disabled by clearing the **Enable filter** check box.

> **Note:** The mark next to the tab name turns green if the filter on that tab is enabled. Otherwise, the mark is gray.

When the filter enabled, its conditions are defined by entering values into the following fields:

- **Event types** - Select check boxes to filter events by type:

  - **Success** - Task or operation completed successfully.

  - **Information** - Certain action performed.

  - **Warning** - A problem might occur unless action is taken.

  - **Error** - A problem has occurred.

- **Information**, **Server**, **Event ID** - Include or exclude events depending upon whether event data matches the filter string specified. For example, to filter events by the name of the computer on which the event occurred, specify a filter string in the **Server** field. To filter events with certain IDs, enter ID numbers separated by a semicolon in the **Event ID** field.

- **From** - The beginning of the range of events to filter. Possible values: **First Record** (selected by default) or **Records On**. Select **First Record** to filter events starting with the first one recorded in the log. Select **Records On** to filter events that occurred starting with a specific time and date.

- **To** - The end of the range of events to filter. Possible values: **Last Record** (selected by default) or **Records On**. Select **Last Record** to filter events up to the last one recorded in the log. Select **Records On** to filter events that occurred ending with a specific time and date.

> **Note:** To assist with configuring a filter, string setting fields store previous entries and suggest matches for what is being typed. Previous entries are also available on the drop-down list of options for the setting field.

When configuring a filter, consider the following:

- Filter conditions are combined by AND logic, that is, a given record matches the filter if it matches each of the filter conditions. Clear the fields that are not to be used in the filter conditions.

- Filter string fields may include wildcards, such as an asterisk (*) or a question mark (?). An asterisk represents zero or more characters; a question mark represents any single character.

- A filter string field may include multiple values separated by a semicolon (;). In this case, the values are combined by OR logic, that is, a given record matches the filter condition on a particular field if it matches at least one of the values specified in that field.

- The **Clear** button in the **Filter** dialog box provides the option to remove all the defined filter conditions and start setting up a new filter from scratch.

- The **Save** and **Load** buttons in the **Filter** dialog box are used to save the filter conditions to a file and to load previously saved filter conditions from a file.