Security Management Server Virtual v10.2.11 AdminHelp

Table of Contents

Welcome

About Online Help

Version: **10.2.11**

Attributions & Copyrights

Third Party Software

I. OpenSSL License - Copyright (c) 1998-2011 The OpenSSL Project. All rights reserved.

LICENSE ISSUES

==========

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

==========

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

A. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

B. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

C. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)".

D. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

E. Products derived from this software may not be called "OpenSSL" * nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

F. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)" THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE

FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved. This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL. This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com). Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

a. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

b. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

c. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related.

d. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)" THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.].

II. Portions of this product use Commons IO, Commons DBCP, and Commons LANG. You may obtain a copy of the licenses at http://www.apache.org/licenses/LICENSE-2.0.

III. Portions of this product use OrientDB. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

IV. Portions of this product use Apache Wink. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

V. Portions of this product use Jackson JSON. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

VI. Portions of this product use Jetty. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

VII. Portions of this product use ActiveMQ. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

VIII. Portions of this product use jasypt. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

IX. Portions of this product make use of zlib. You may obtain a copy of the license at http://www.zlib.net/zlib_license.html.

/* zlib.h -- interface of the 'zlib' general purpose compression library version 1.2.7, May 2nd, 2012 Copyright (C) 1995-2012 Jean-loup Gailly and Mark Adler This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

A. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

B. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

C. This notice may not be removed or altered from any source distribution. Jean-loup Gailly Mark Adler jloup@gzip.org madler@alumni.caltech.edu.

X. Portions of this product make use of Apache Tomcat (www.apache.org). You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.txt.

XI. Portions of this product make use of Apache Commons HTTPClient. You may obtain a copy of the license at http://opensource.org/licenses/apache2.0.

XII. Portions of this product make use of log4net. You may obtain a copy of the license at http://logging.apache.org/log4net/license.html.

XIII. Portions of this product make use of MVVM Light Toolkit. You may obtain a copy of the license at http://mvvmlight.codeplex.com/license.

XIV. Portions of this product make use of Apache JDBCLog, Apache Software Foundation. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.txt.

XV. Portions of this product make use of Apache Log4J, Apache Software Foundation. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.txt.

XVI. Portions of this product make use of Apache Struts, Apache Software Foundation. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.txt.

XVII. Portions of this product make use of Struts2. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

XVIII. Portions of this product make use of Struts Beanutils, Apache Software Foundation. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.txt.

XIX. Portions of this product make use of Struts Digester, Apache Software Foundation. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.txt.

XX. Portions of this product make use of Apache xmlrpc, Apache Software Foundation. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.txt.

XXI. Portions of this product make use of Bean Scripting Framework (http://commons.apache.org/bsf/), Apache License, Version 2.0, January 2004 http://commons.apache.org/license.html.

XXII. Portions of this product make use of Apache Commons CLI (http://commons.apache.org/cli/), Apache License, Version 2.0, January 2004 http://commons.apache.org/license.html.

XXIII. Portions of this product make use of Apache Commons EL (http://commons.apache.org/el/), Apache License, Version 2.0, January 2004 http://commons.apache.org/license.html.

XXIV. Portions of this product make use of Groovy. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.html.

XXV. Portions of this product make use of H2. You may obtain a copy of the license at http://www.h2database.com/html/license.html.

XXVI. Portions of this product make use of Spring.net Application Framework. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.html.

XXVII. Portions of this product make use of Java Service Wrapper (http://www.tanukisoftware.com/en/index.php). You may obtain a copy of the license at http://wrapper.tanukisoftware.com/doc/english/licenseOverview.html.

XXVIII. Portions of this product make use of Xalan. You may obtain a copy of the license at http://xml.apache.org/xalan-j/.

XXIX. Portions of this product make use of FreeMarker. You may obtain a copy of the license at http://freemarker.sourceforge.net/docs/app_license.html.

XXX. Portions of this product make use of Velocity. You may obtain a copy of the license at http://velocity.apache.org/.

XXXI. Portions of this product make use of MSV. You may obtain a copy of the license at http://opensource.org/licenses/apache2.0.

XXXII. Portions of this product make use of FLIB. You may obtain a copy of the license at http://opensource.org/licenses/artistic-license.html.

XXXIII. Portions of this product makes use of libraries developed by Boost (http://www.boost.org/users/license.html), under the following license: Boost Software License - Version 1.0 - August 17th, 2003.

XXXIV. Portions of this product make use of ANTLR. You may obtain a copy of the license at http://antlr.org/license.html.

XXXV. Portions of this product make use of BIRT. You may obtain a copy of the license at http://www.eclipse.org/org/documents/epl-v10.php.

XXXVI. Portions of this product make use of the getopt function, Copyright © 1987-2002 The Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

A. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

B. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

C. Neither the names of the copyright holders nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

XXXVII. Portions of this product make use of the SHA-2 algorithm, Copyright © 2002, Dr. Brian Gladman (brg@gladman.me.uk), Worcester, UK. All rights reserved.

A. LICENSE TERMS

The free distribution and use of this software in both source and binary form is allowed (with or without changes) provided that:

1. Distributions of this source code include the above copyright notice, this list of conditions and the following disclaimer;

2. Distributions in binary form include the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other associated materials;

3. The copyright holder's name is not used to endorse products built using this software without specific written permission.

DISCLAIMER

This software is provided "as is" with no explicit or implied warranties in respect of its properties, including, but not limited to, correctness and/or fitness for purpose.

XXXVIII. Portions of this product make use of STLport. A copy of the license may be obtained at http://www.stlport.org/doc/license.html.

A. License Agreement:

Boris Fomitchev grants Licensee a non-exclusive, non-transferable, royalty-free license to use STLport and its documentation without fee.

By downloading, using, or copying STLport or any portion thereof, Licensee agrees to abide by the intellectual property laws and all other applicable laws of the United States of America, and to all of the terms and conditions of this Agreement.

Licensee shall maintain the following copyright and permission notices on STLport sources and its documentation unchanged:

Copyright 1999,2000 Boris Fomitchev

This material is provided "as is", with absolutely no warranty expressed or implied. Any use is at your own risk.

Permission to use or copy this software for any purpose is hereby granted without fee, provided the above notices are retained on all copies. Permission to modify the code and to distribute modified code is granted, provided the above notices are retained, and a notice that the code was modified is included with the above copyright notice.

The Licensee may distribute binaries compiled with STLport (whether original or modified) without any royalties or restrictions.

The Licensee may distribute original or modified STLport sources, provided that:

- The conditions indicated in the above permission notice are met;
- The following copyright notices are retained when present, and conditions provided in accompanying permission notices are met :

Copyright 1994 Hewlett-Packard Company - Permission to use, copy, modify, distribute and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Hewlett-Packard Company makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Copyright 1996,97 Silicon Graphics Computer Systems, Inc. - Permission to use, copy, modify, distribute and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Silicon Graphics makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Copyright 1997 Moscow Center for SPARC Technology - Permission to use, copy, modify, distribute and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Moscow Center for SPARC Technology makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

XXXIX. Portions of this product make use of The Legion of Bouncy Castle Software. Copyright (c) 2000 - 2016 The Legion Of The Bouncy Castle. You may obtain a copy of the license at http://www.bouncycastle.org/license.html.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Note: Our license is an adaptation of the MIT X11 License and should be read as such.

License

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

XL. Portions of this product make use of ResizableLib. You may obtain a copy of the license at http://opensource.org/licenses/artistic-license-1.0.

XLI. Portions of this product make use of Spring Framework. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

XLII. Portions of this product use $File:

A. LEGAL NOTICE,v 1.15 2006/05/03 18:48:33 christos Exp $. Copyright (c) Ian F. Darwin 1986, 1987, 1989, 1990, 1991, 1992, 1994, 1995. Software written by Ian F. Darwin and others; maintained 1994-Christos Zoulas. This software is not subject to any export provision of the United States Department of Commerce, and may be exported to any country or planet. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice immediately at the beginning of the file, without modification, this list of conditions, and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

XLIII. Portions of this product use UFSD – Paragon NTFS for Windows Driver based on Paragon Universal File System Driver (UFSD) Technology. Copyright (C) 2008 Paragon Technologie GmbH. All rights reserved. This software is provided 'as-is', without any express or implied warranty.

XLIV. Portions of this product use JDBC drivers - licensed from DataDirect Technologies.

XLV. Portions of this product make use of DIMime, available at http://www.zeitungsjunge.de/delphi/mime/.

XLVI. Portions of this product make use of RSA Security Inc. PKCS #11 Crypto Token Interface (Cryptoki).

XLVII. This software uses following 3rd party libraries:

1. urwid

Copyright (C) 2004-2012 Ian Ward

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it is useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

GNU LESSER GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General Public License, supplemented by the additional permissions listed below.

1. Additional Definitions.

   As used herein, "this License" refers to version 3 of the GNU Lesser General Public License, and the "GNU GPL" refers to version 3 of the GNU General Public License.

   "The Library" refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

   An "Application" is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

   A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

   The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

   "Corresponding Application Code" for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

   You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

   If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

   a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

   b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

   The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

   a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

   b) Accompany the object code with a copy of the GNU GPL and this license document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license document.

c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions is similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

XLVIII. Portions of this product use DropNet. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

XLIX. Portions of this product use Hardcodet WPF NotifyIcon 1.0.8. You may obtain a copy of the license at http://www.codeproject.com/info/cpol10.aspx.

L. Portions of this product use MahApps.Metro 1.2.4.0. You may obtain a copy of the license at http://opensource.org/licenses/ms-pl.

LI. Portions of this product use Microsoft Practices Enterprise Library 6.0.1304.0. You may obtain a copy of the license at http://opensource.org/licenses/ms-pl.

LII. Portions of this product use Microsoft Practices Prism 4.1. You may obtain a copy of the license at http://opensource.org/licenses/ms-pl.

LIII. Portions of this product use Microsoft Practices Unity 2.1. You may obtain a copy of the license at http://opensource.org/licenses/ms-pl.

LIV. Portions of this product use RestSharp 105.2.3. You may obtain a copy of the license at https://github.com/restsharp/RestSharp/blob/master/LICENSE.txt.

Copyright 2009 RestSharp

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License.

You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

See the License for the specific language governing permissions and limitations under the License.

LV. Portions of this product use System.Data.SQLite 1.0.102.0. You may obtain a copy of the copyright statement at http://www.sqlite.org/copyright.html.

LVI. Portions of this product use android-passwordsafe 0.6.0. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LVII. Portions of this product use Dropbox.NET 3.4.0. You may obtain a copy of the license at https://github.com/dropbox/dropbox-sdk-dotnet/blob/master/LICENSE.

LVIII. Portions of this product use Newtonsoft JSON 9.0.1. You may obtain a copy of the license at https://raw.githubusercontent.com/JamesNK/Newtonsoft.Json/master/LICENSE.md.

The MIT License (MIT)

Copyright (c) 2007 James Newton-King

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LIX. Portions of this product use NT Security Classes for .NET. You may obtain a copy of the license at http://www.codeproject.com/info/cpol10.aspx.

LX. Portions of this product use Prism Core 6.1. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXI. System.IdentityModel.Tokens.Jwt 4.0.2. You may obtain a copy of the license at https://github.com/AzureAD/azure-activedirectory-identitymodel-extensions-for-dotnet/blob/master/LICENSE.txt.

LXII. Portions of this product use Unity 4.0.1. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXIII. Portions of this product use the Dropbox Android SDK 1.6.3. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

LXIV. Portions of this product use the Dropbox json_simple-1.1.jar. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

LXV. Portions of this product use the Box Android Library V2. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXVI. Portions of this product use the Box Java Library V2. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXVII. Portions of this product use Apache HttpClient Cache 4.2.5. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXVIII. Portions of this product use Apache HttpClient 4.2.5. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXIX. Portions of this product use Apache HttpCore 4.2.4. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXX. Portions of this product use Apache HttpClient Mime 4.2.5. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXXI. Portions of this product use Apache Commons IO 2.4. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXXII. Portions of this product use Apache Commons Lang 2.6. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXXIII. Portions of this product use JUnit 4.11. You may obtain a copy of the license at https://www.eclipse.org/legal/epl-v10.html.

LXXIV. Portions of this product use EasyMock 3.1. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXXV. Portions of this product use Jackson Databind 2.4.4. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXXVI. Portions of this product use Jackson Core 2.4.4. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXXVII. Portions of this product use Jackson Annotations 2.4.4. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXXVIII. Portions of this product use Apache Maven Wagon 2.2. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXXIX. Portions of this product use Scribe OAuth Library 1.3.0. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

LXXX. Portions of this product use JSON Web Token Support for the JVM 0.6.0. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXXXI. Portions of this product use OneDrive SDK Android 1.2.2. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

LXXXII. Portions of this product use Microsoft Services MSA Auth 0.8.4. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

LXXXIII. Portions of this product use Adal 1.1.7. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXXXIV. Portions of this product use Google API Client Library for Java with Android Platform Extensions and GSON Extensions 1.20.0. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXXXV. Portions of this product use Google Drive API V3 Rev 170 1.22.0. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXXXVI. Portions of this product use Backport Util Concurrent 3.1. You may obtain a copy of the license at https://creativecommons.org/publicdomain/zero/1.0.

LXXXVII. Portions of this product use Apache Commons Logging 1.1.3. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

LXXXVIII. Portions of this product use Flurry Analytics 4.1.0. You may obtain a copy of the license at https://developer.yahoo.com/flurry/legal-privacy/terms-service/flurry-analytics-terms-service.html.

LXXXIX. Portions of this product use kSOAP2 3.4.0. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

XC. Portions of this product use FindBugs Jsr305. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

XCI. Portions of this product use Google Gson 2.3.1. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

XCII. Portions of this product use Hockey SDK 3.0.2. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

XCIII. Portions of this product use Picasso 2.5.2. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

XCIV. Portions of this product use Circular Floating Action Menu Library 1.0.2. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

XCV. Portions of this product use Apache Commons Codec 1.8. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

XCVI. Portions of this product use Apache Commons Compress 1.1. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

XCVII. Portions of this product use One Password App Extension 1.8. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

XCVIII. Portions of this product use Azure Active Directory Authentication Library 1.2.9. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

XCIX. Portions of this product use AF Networking 2.6.3. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

C. Portions of this product use Box iOS SDK 1.0.11. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

CI. Portions of this product use CT Assets Picker Controller 2.9.5. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

CII. Portions of this product use Google API Objective C Client 1.0.422. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

CIII. Portions of this product use Google GTM HTTP Fetcher 1.0.141. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

CIV. Portions of this product use Google GTM OAuth 2 1.0.126. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

CV. Portions of this product use Hockey SDK iOS 3.8.6. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

CVI. Portions of this product use libextobjc 0.4.1. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

CVII. Portions of this product use libPhoneNumber iOS 0.8.11. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

CVIII. Portions of this product use MBProgressHUD 0.9.2. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

CIX. Portions of this product use NSData Base64 1.0.0. You may obtain a copy of the license at http://opensource.org/licenses/Zlib.

CX. Portions of this product use OneDrive SDK iOS 1.1.2. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

CXI. Portions of this product use RNCryptor 3.0.1. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

CXII. Portions of this product use SSZipArchive 1.1. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

CXIII. Portions of this product use SVProgressHUD 2.0.2. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

CXIV. Portions of this product use WEPopover 1.0.0. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

CXV. Portions of this product use XMLDictionary. You may obtain a copy of the license at http://opensource.org/licenses/Zlib.

CXVI. Portions of this product use NHNetworkTime 1.7. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

CXVII. Portions of this product use the Dropbox iOS SDK. You may obtain a copy of the license at http://opensource.org/licenses/MIT.

CXVIII. Portions of this product use Flurry iOS SDK 5.3.0. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0.

CXIX. Portions of this product make use of the Mono and the Mono runtime, under MIT, BSD, and Apache licenses. You may obtain a copy of the licenses at http://www.mono-project.com/docs/faq/licensing/.

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

See the License for the specific language governing permissions and limitations under the License.

CXX. Portions of this product make use of the Mono .NET assemblies under MIT and BSD licenses. You may obtain a copy of the licenses at https://mit-license.org/ and https://opensource.org/licenses/BSD-3-Clause.

The MIT License (MIT)

Copyright © 2018 Microsoft

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

The BSD License

Copyright 2018 Microsoft

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the copyright holder nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING

NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

CXXI. Portions of this product make use of mkbundle in Mono under GNU LESSER GENERAL PUBLIC LICENSE v3. You may obtain a copy of the license at https://www.gnu.org/licenses/lgpl.txt.

GNU LESSER GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <https://fsf.org/>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General Public License, supplemented by the additional permissions listed below.

0. Additional Definitions.

As used herein, "this License" refers to version 3 of the GNU Lesser General Public License, and the "GNU GPL" refers to version 3 of the GNU General Public License.

"The Library" refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

An "Application" is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library.

Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The "Corresponding Application Code" for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

a. under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

b. under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

   The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

a. Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

b. Accompany the object code with a copy of the GNU GPL and this license document.

4. Combined Works.

   You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

a. Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

b. Accompany the Combined Work with a copy of the GNU GPL and this license document.

c. For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.

d. Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e. Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. Combined Libraries.

   You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a. Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b. Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

CXXII. Portions of this product make use of minizip, memcheck.h, freebsd-dwarf.h, freebsd-elf_common.h, freebsd-elf64.h, freebsd-elf32.h, bsearch.c, w32file-unix-glob.c, and w32file-unix-glob.h in Mono under BSD license. You may obtain a copy of the license at https://opensource.org/licenses/BSD-3-Clause.

The BSD License

Copyright 2018 Microsoft

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the copyright holder nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

CXXIII. Portions of this product make use of RabbitMQ.Client in Mono under dual license in Apache v2 and Mozilla Public License 1.1. You may obtain a copy of the licenses at http://www.apache.org/licenses/LICENSE-2.0 and https://www.mozilla.org/MPL/.

License Information:

This software and associated documentation (if any) is furnished under a license and may only be used or copied in accordance with the terms of the license.

Dell elects to use only the Apache license for any software where a choice of Apache v2, and Mozilla Public License 1.1 license versions are made available with the language indicating that Apache v2, and Mozilla Public License 1.1 “or any later version may be used, or where a choice of which version of the Apache v2, and Mozilla Public License 1.1" is applied is unspecified.

CXXIV. Portions of this product make use of Compat.ICSharpCode.SharpZipLib and ICSharpCode.SharpZipLib in Mono under GNU LESSER GENERAL PUBLIC LICENSE v3. You may obtain a copy of the license at https://www.gnu.org/licenses/lgpl.txt, although the full text is available below.

GNU LESSER GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General Public License, supplemented by the additional permissions listed below.

1. Additional Definitions.

   As used herein, "this License" refers to version 3 of the GNU Lesser General Public License, and the "GNU GPL" refers to version 3 of the GNU General Public License.

   "The Library" refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

   An "Application" is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library.

   Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

   A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

   The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

   The "Corresponding Application Code" for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

2. Exception to Section 3 of the GNU GPL.

   You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

3. Conveying Modified Versions.

   If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

a. under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

b. under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

4. Object Code Incorporating Material from Library Header Files.

   The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

a. Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

b. Accompany the object code with a copy of the GNU GPL and this license document.

5. Combined Works.

   You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

a. Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

b. Accompany the Combined Work with a copy of the GNU GPL and this license document.

c. For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.

d. Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e. Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

6. Combined Libraries.

   You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a. Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b. Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

7. Revised Versions of the GNU Lesser General Public License.

   The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

   Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

   If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

   Classpath is distributed under the terms of the GNU General Public License with the following clarification and special exception.

   Linking this library statically or dynamically with other modules is making a combined work based on this library. Thus, the terms and conditions of the GNU General Public License cover the whole combination.

   As a special exception, the copyright holders of this library give you permission to link this library with independent modules to produce an executable, regardless of the license terms of these independent modules, and to copy and distribute the resulting executable under terms of your choice, provided that you also meet, for each linked independent module, the terms and conditions of the license of that module. An independent module is a module which is not derived from or based on this library. If you modify this library, you may extend this exception to your version of the library, but you are not obligated to do so. If you do not wish to do so, delete this exception statement from your version.

   As such, it can be used to run, create and distribute a large class of applications and applets. When GNU Classpath is used unmodified as the core class library for a virtual machine, compiler for the java languge, or for a program written in the java programming language it does not affect the licensing for distributing those programs directly.

   Source code for this component can be found at http://opensource.dell.com.

CXXV. Portions of this product make use of TimeZoneInfo.Android.cs in Mono under Apache License, Version 2.0. You may obtain a copy of the license at http://www.apache.org/licenses/LICENSE-2.0

Copyright 2018 Microsoft

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License.

You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS,

WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

See the License for the specific language governing permissions and limitations under the License.

CXXVI. Portions of Advanced Threat Prevention are licensed under GNU LESSER GENERAL PUBLIC LICENSE v3. You may obtain a copy of the license at https://www.gnu.org/licenses/lgpl.txt or request information at www.cylance.com.

Get Started

Get Started with Dell Data Security

- Once your environment has been configured in the Server Configuration Tool, ensure that Dell services are .
- Log in to the Management Console.
- Add Client Access Licenses, as needed.
- Add domains from your directory server.
- If you require that users receive non-default policies upon activation, modify policies at the appropriate level.
- Add groups and users, as necessary.
- Assign administrators, as necessary.
- Deploy clients.

Log In

To perform a given administrative procedure, an administrator must first log in to the Management Console using an appropriate Dell administrator account.

The Dell Server installs with a default super administrator user name (superadmin) and password (changeit) that you can use to add additional Dell administrator accounts.

1. Open a supported browser and type **http://<server.domain.com>:8443/webui/login**.
2. If you are logging in for the first time, in the *Username*, enter **superadmin**. In the *Password*, enter **changeit**.

   If you are not logging in for the first time, enter your u**ser name** in one of the formats listed below. In *Password,* enter **<your_case-sensitive_password>**.

   user@domain.com (preferred format)

   sAMAccountName, such as jsmith

   <DOMAIN>\<Username> - You must specify your domain name as an alias to use this format. For more information, refer to Add Domains.
3. Click **Sign in**.

To log out, see Log Out.

Log Out

If you are an account administrator and make changes to your own account, you must log out and log back in to see the results.

- Click the gear icon in the top right corner of the Management Console and select **Log out** from the menu.

Dashboard

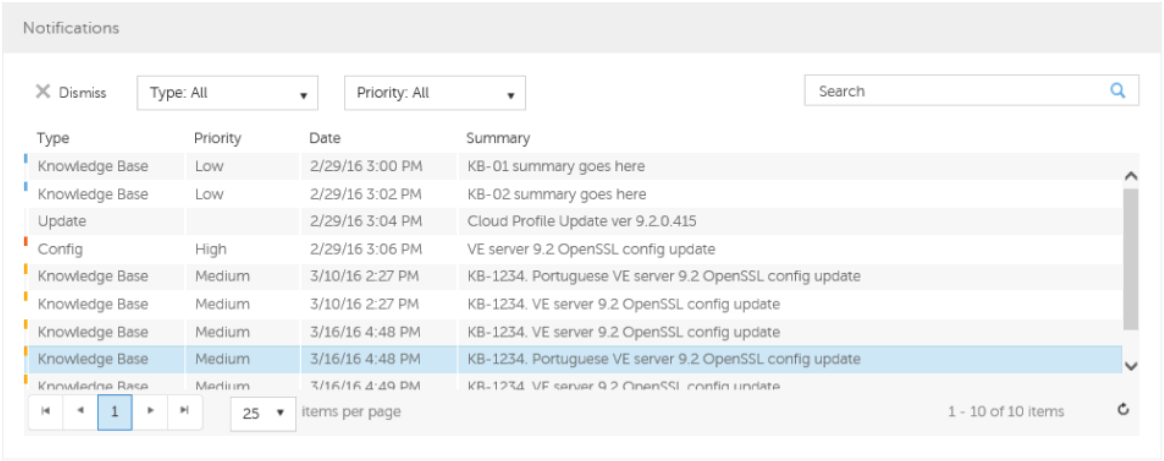
The dashboard displays an overview of status information for your enterprise. Access more detailed information directly from the dashboard by clicking its statistics, graphs, and chart legends.

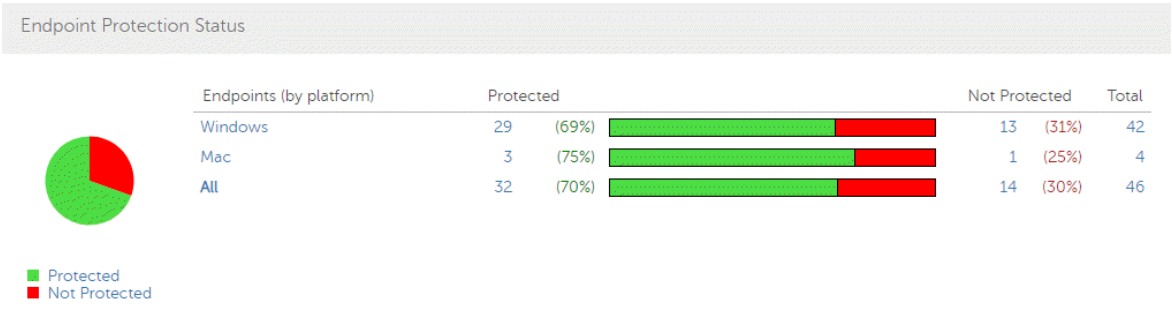
In the top right, select the **Widgets** menu to add or remove the following widgets:

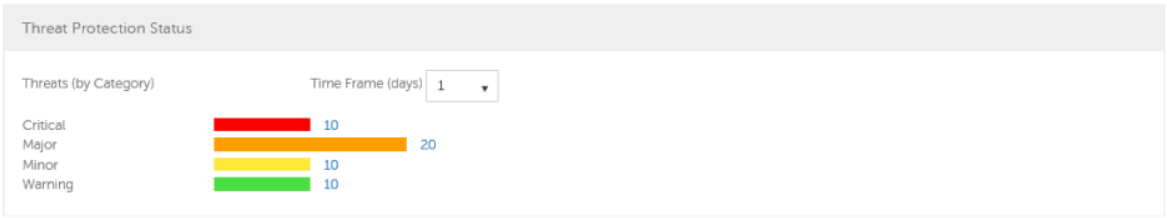
- Notifications
- Protection Status
- Threat
- Protection History
- Inventory History
- Summary Statistics

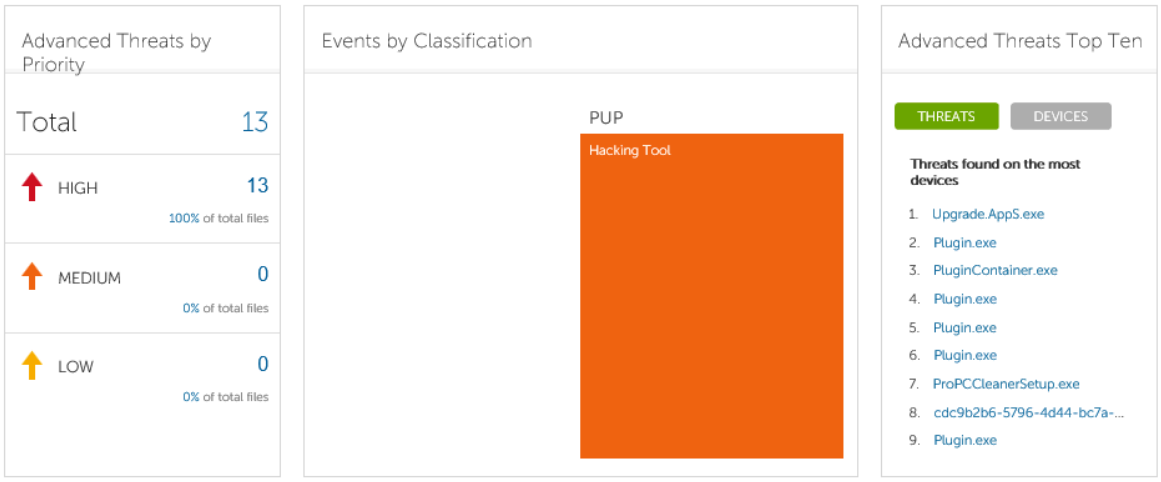
The images below reflect what may be seen in the dashboard, depending on widgets enabled. Content may vary based on the features installed and enabled on your Dell Server and endpoints.

Click an area below to view a description of the detail accessible by clicking the same area in the dashboard.

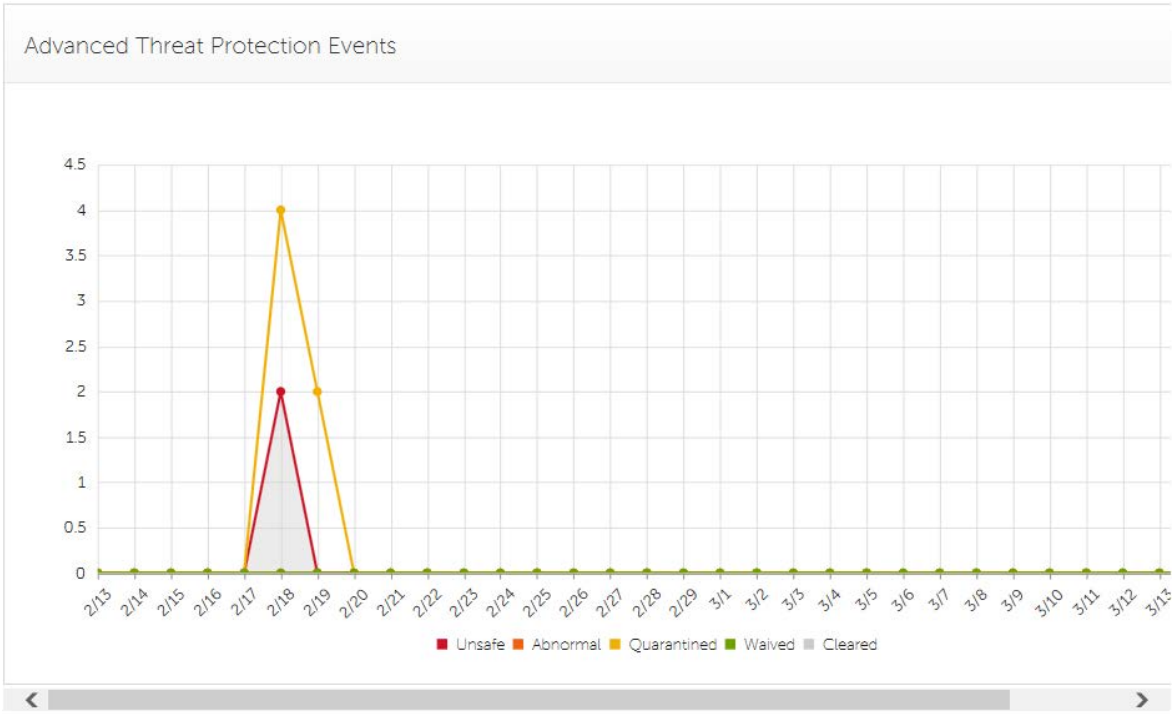


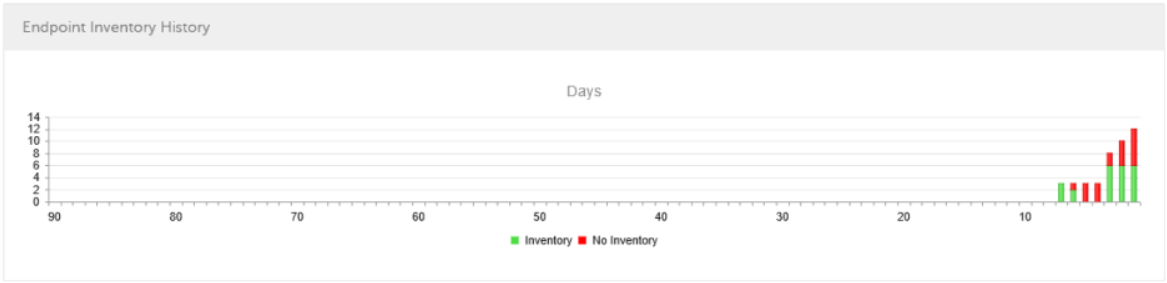






An Advanced Threat Prevention event is not necessarily a threat. An event is generated when a recognized file or program is quarantined, safe listed, or waived. Threats are a category of events that are newly detected as potentially unsafe files or programs and require guided remediation.





Summary Statistics

Details	
Domains	2
User Groups	18
Endpoint Groups	14
AD Users	127
Local Users	417
Endpoints	46
Protected	32
Not-Protected	14
Shields	23
Managers	37
Modified Policies	0

Endpoints (by platform)	
Windows	42
Mac	4
All	46

Change Superadmin Password

1. In the masthead at the top of the screen, click the gear icon and select **Change superadmin password**.
2. Enter the current password.
3. Enter the new password.

   The new password must be at least 6 characters, contain at least one capital letter and one of these characters: **~@#$%^*()|?!{}[]**.
4. Confirm the new password.
5. Click **Update**.

After three failed login attempts, the superadmin account is locked for five minutes. To change these settings, see Set or Change Account Lockout Settings.

Components

Default Port Values

Compatibility Server: TCP/1099 (closed)

Compliance Reporter: HTTP(S)/8084

Identity Server: HTTPS/8445

Core Server: HTTPS/8888

Policy Proxy: TCP/8000/8090

Security Server: HTTPS/8443

Forensic Server: HTTPS/8448

Client authentication: HTTPS/8449 (If using Dell Encryption on a server operating system)

Management Console: HTTPS/8443

Client communication if using Advanced Threat Prevention: HTTPS/TCP/443

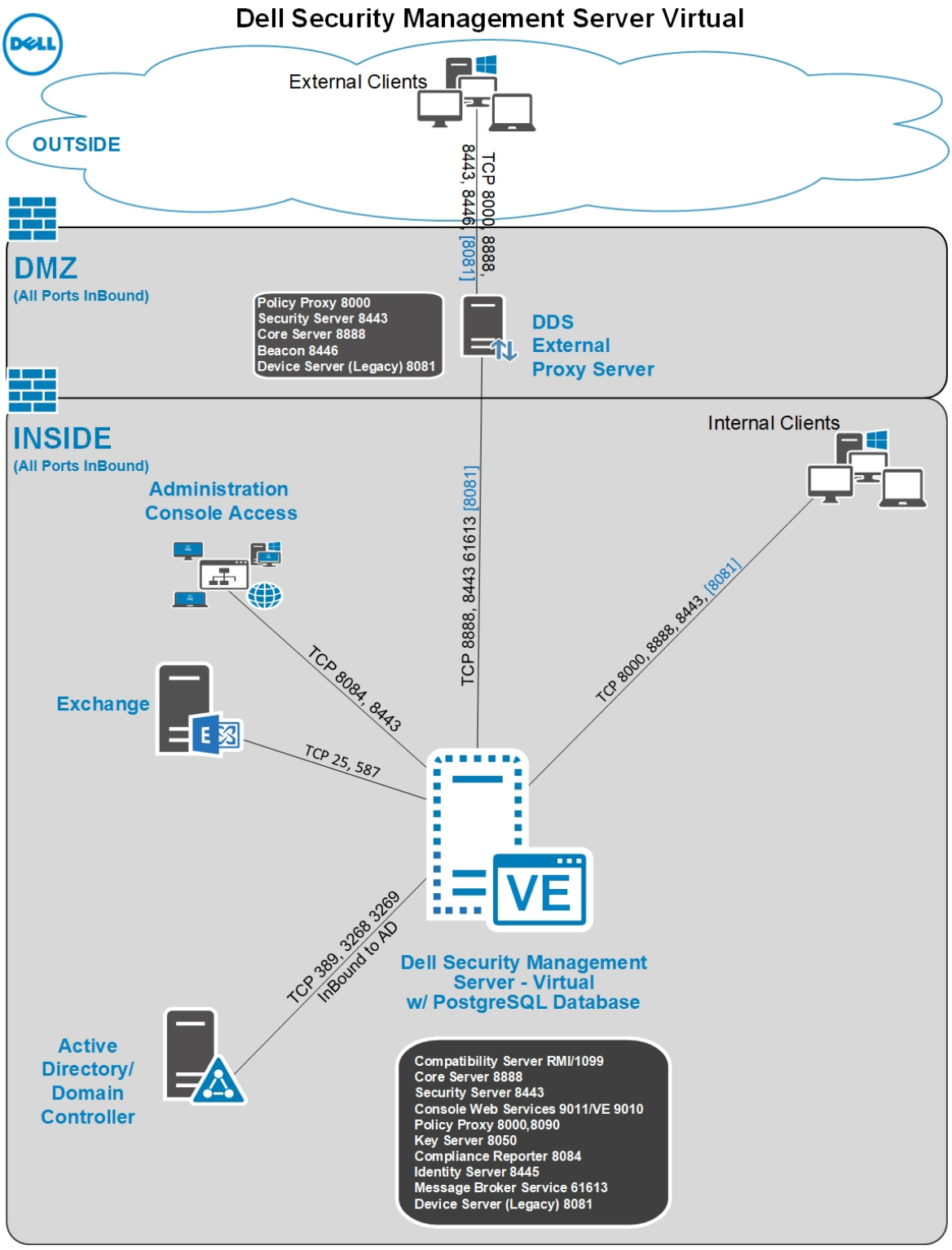
NTP time synchronization: TCP and UDP/123 (for more information, refer to https://help.ubuntu.com/10.04/serverguide/NTP.html.)

Proxy Servers

The proxy server installation, implementation, and deployment are fast and easy. The proxy server is a simplified web server with a single web application.

Types of Proxy Servers

- Security Server (defaults to 8443)
- Core Server (defaults to 8888)
- Device Server (defaults to 8081) see **Note**



Note: The purpose of Device Server proxy is to support legacy Encryption clients (pre-v8.0) that communicate with port 8081. Newer Encryption clients (v8.0 and later) are configured by the client installer to communicate with the Security Server (or Security Server proxy) on port 8443. The full Device Server is not installed in v8.1. The Device Server proxy forwards all communications to the Security Server behind the firewall.

Policy Proxy

Policy Proxy serves as intermediary between Dell Server and Encryption client, delivering information from each to the other.

Time Slotting

To prevent Dell Server traffic jams, Policy Proxies use a time slotting mechanism that allows them to independently choose well-distributed time slots for communicating with the Dell Server.

Polling

On every poll, the endpoint authenticates, checks for policy updates, and uploads inventory. A successful authentication is required for the process to begin.

Poll Triggers

A user must be logged in to poll. On the next user login, another poll occurs. The poll information needed is only available per user, and when that user is logged in.

Other times a poll occurs:

- Immediately upon login, after encryption keys are unlocked.
- When a network status update is signaled by the operating system (cable plugged in, wireless network connected, VPN becomes active).
- When the polling period elapses, as specified by policy.

Failed Poll Attempts

Policy Proxy poll attempts are based on a timer. When a poll attempt fails, the timer is reset. The length of time set for the next attempt is based on when the attempt failed. If the device misses a poll when powered off, the timer is triggered when the device is next powered on.

If the poll attempt failed while making the attempt, the time is set to one tenth the policy value for the polling interval. For example, if the polling interval is 100 minutes, then the next interval after a failed attempt is 10 minutes. If it fails again, the next interval is still 10 minutes. The interval remains 10 minutes until a successful poll, after which it returns to 100 minute intervals.

General Information

- Policy Proxy is generally installed on only a few computers.
- Creates inventory information for the Dell Server.
- Passes on to the Dell Server device inventory it receives when the Encryption client successfully retrieves policies.
- Securely distributes security policies and encryption keys to devices via the network when contacted.
- May be in your DMZ.
- Always belongs to a group. By default, all Policy Proxies belong to the same group.

Navigate the Dell Server

Navigation

The Management Console is a central control center that the administrator can use to deploy and monitor security for the organization. It consists of security and configuration settings that are applied through policy to groups called Populations.

The menu pane allows access to the following:

Dashboard

The Management Console opens to the dashboard. The dashboard provides graphs and statistics on endpoints and threat protection as well as summary statistics on populations and operating systems.

Populations

A population is a grouping for which security policies, settings, and actions can be configured. For example, security policies can be applied at the Enterprise, Domain, User Group, User, Endpoint Group, and Endpoint levels. See Populations. See Manage Security Policies.

Reporting

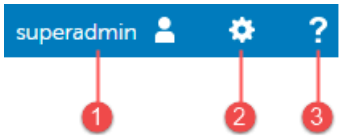
Reporting menu items provide reports on the protection state of the environment and endpoints, deployment issues that require action, and devices within the network. Create and manage reports with the Manage Reports tool or by launching Compliance Reporter. This menu allows you to collect, view, and export audit events to a SIEM server.

Management

Commit policies, manage licenses, services, and alerts.

Masthead Icons

The following icons display on the masthead:



(1) Logged in user - The user icon and name of the user that is currently logged on.

(2) Gear icon - From the gear icon, you can Change the Superadmin Password, view information about the Dell, get Dell ProSupport contact information, and log out.

(3) Question mark icon - Open a help topic that explains the current screen in the Management Console.

Disconnected Mode

Disconnected mode allows a Dell Server to manage Advanced Threat Prevention endpoints without client connection to the Internet or external network. Disconnected mode also allows the Dell Server to manage clients without Internet connection or a provisioned and hosted Advanced Threat Prevention service. The Dell Server captures all event and threat data in Disconnected mode.

To determine if a Dell Server is running in Disconnected mode, click the gear icon at the top right of the Management Console and select **About**. The About screen indicates that a Dell Server is in Disconnected mode, below the Dell Server version.

Disconnected mode is different than a standard connected installation of Dell Server in the following ways.

Client Activation

An install token is generated when the administrator uploads an Advanced Threat Prevention license, which allows the Advanced Threat Prevention client to activate.

Management Console

The following items are ***not available*** in the Management Console when Dell Server is running in Disconnected mode:

The following areas specific to Advanced Threat Prevention: Advanced Threats by Priority, (Advanced Threat) Events by Classification, Advanced Threats Top Ten, and Advanced Threat Prevention Events.

Enterprise > Advanced Threats tab, which provides a dynamic display of detailed events information for the entire enterprise, including a list of the devices on which events occurred and any actions taken on those devices for those events.

(Left navigation pane) **Services Management**, which allows enabling of the Advanced Threat Prevention service and product notifications enrollment.

The following item ***is available*** to the Management Console when Dell Server is running in Disconnected mode:

Enterprise > Advanced Threat Events tab, which list events information for the entire enterprise based on information available in the Dell Server, even when running in Disconnected mode.

Functionality

The following functionality is ***not available*** in the Management Console when Dell Server is running in Disconnected mode:

Security Management Server upgrade, update, and migration

Security Management Server Virtual auto update - an update must be done manually

Advanced Threat Prevention auto update

Upload of Unsafe or Abnormal Executable files for Advanced Threat Prevention analysis

Advanced Threat Prevention file upload and log file upload

The following functionality differs:

The Dell Server sends the Global Safe List, Quarantine List, and Safe List to client computers.

The Global Safe List is imported to the Dell Server through the Global Allow policy. For more information, see the Global Allow policy.

The Quarantine List is imported through Quarantine List policy. For more information, see the Quarantine List policy.

The Safe List is imported through Safe List policy. For more information, see the Safe List policy.

Dashboard

Dashboard

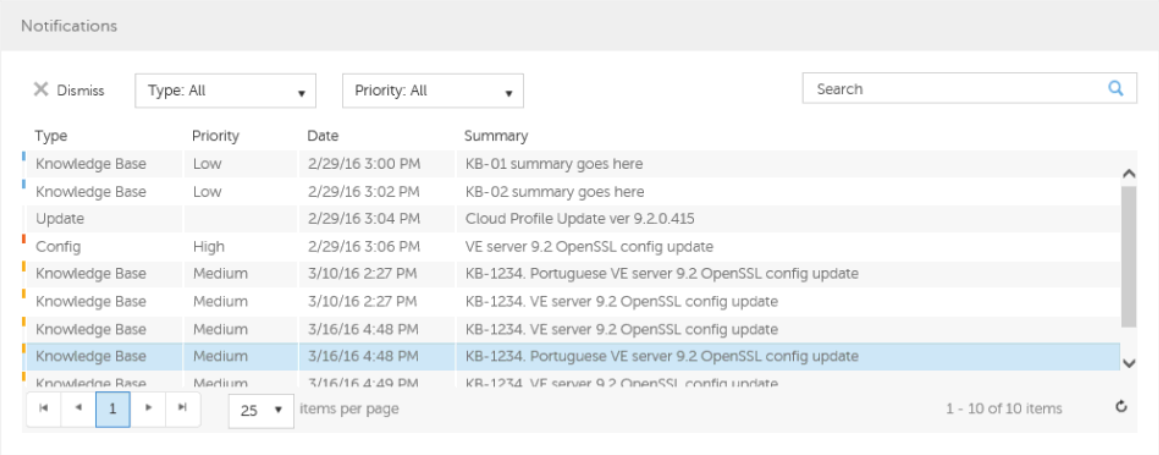
The dashboard displays an overview of status information for your enterprise. Access more detailed information directly from the dashboard by clicking its statistics, graphs, and chart legends.

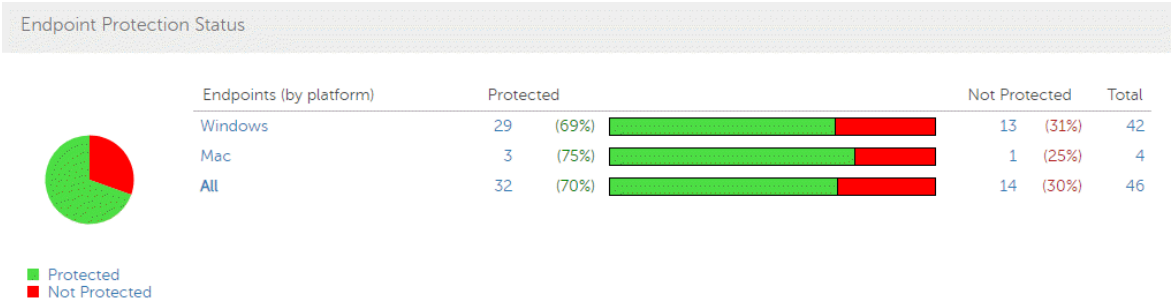
In the top right, select the **Widgets** menu to add or remove the following widgets:

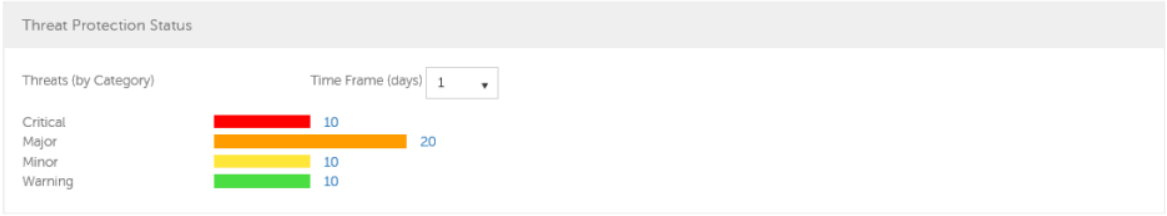
- Notifications
- Protection Status
- Threat
- Protection History
- Inventory History
- Summary Statistics

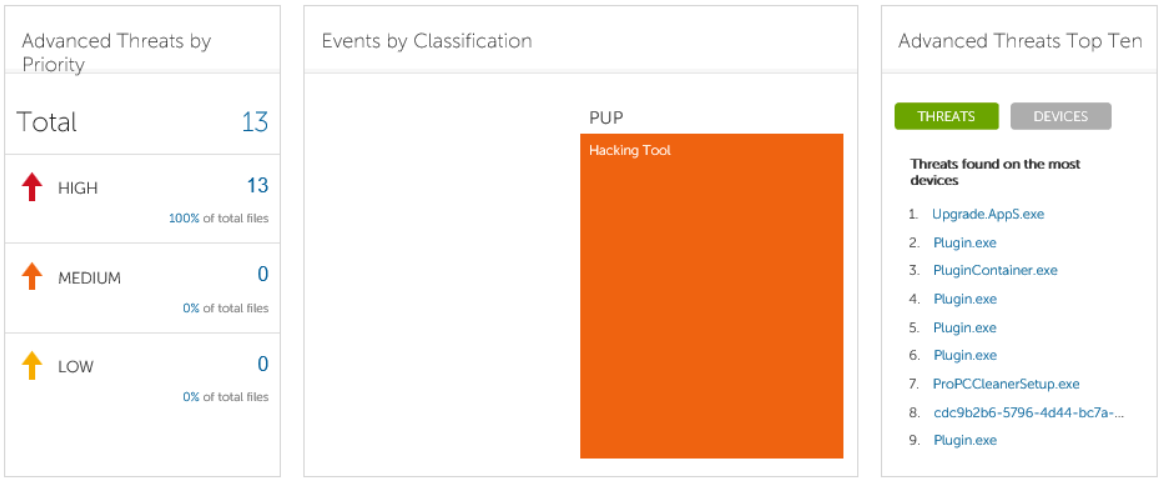
The images below reflect what may be seen in the dashboard, depending on widgets enabled. Content may vary based on the features installed and enabled on your Dell Server and endpoints.

Click an area below to view a description of the detail accessible by clicking the same area in the dashboard.

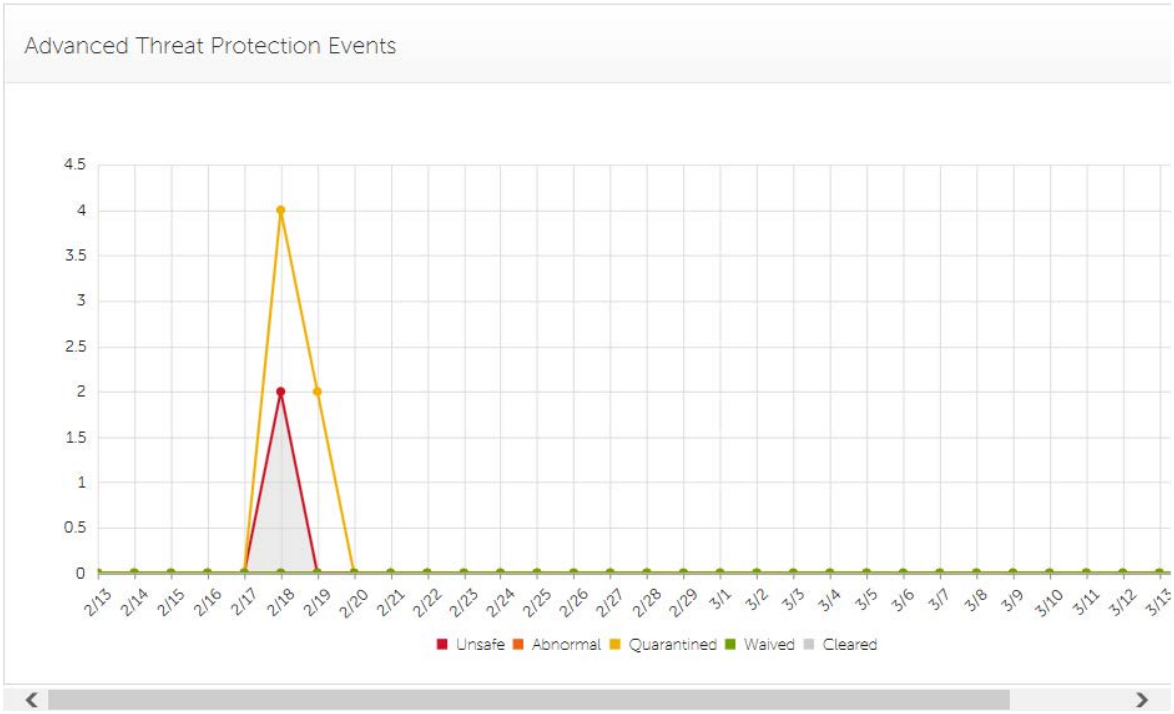


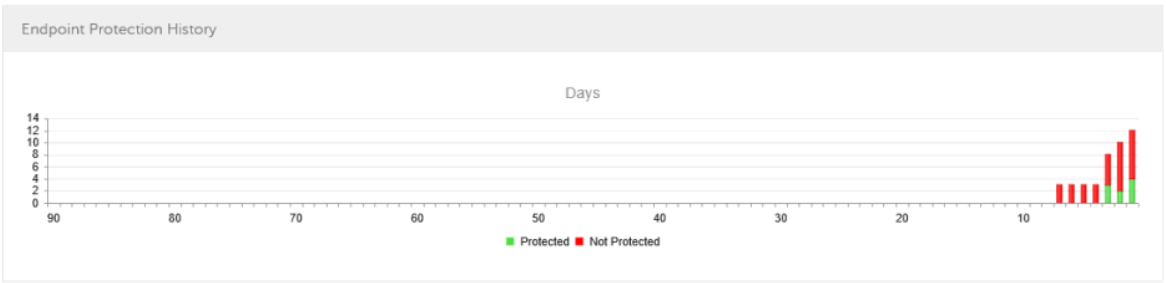






An Advanced Threat Prevention event is not necessarily a threat. An event is generated when a recognized file or program is quarantined, safe listed, or waived. Threats are a category of events that are newly detected as potentially unsafe files or programs and require guided remediation.





Summary Statistics

Details	
Domains	2
User Groups	18
Endpoint Groups	14
AD Users	127
Local Users	417
Endpoints	46
Protected	32
Not-Protected	14
Shields	23
Managers	37
Modified Policies	0

Endpoints (by platform)	
Windows	42
Mac	4
All	46

Notifications List

The notifications list provides a configurable summary of news, alerts, and events to display on the dashboard or to be sent as email notifications. For more information, see Dashboard Field Descriptions and Notification Management.

Notification Types

Select the notification types to include in the list. Notifications of the remaining types are hidden.

Types include:

Update - News of upcoming product updates. To view and receive product updates, you must enroll to receive them. Select **Services Management > Product Notifications**, click **On**, then click **Save Preferences**.

Config - News about configuration changes.

Knowledge Base - Summaries and links to knowledge base articles with in-depth technical information such as work arounds and configuration methods.

- Alerts when your volume license is low, or when your client access license count has been exceeded.

Announcement - News of upcoming releases and new products.

Threat Protection - A threat alert from Advanced Threat Prevention.

Advanced Threat Event - An event detected by Advanced Threat Prevention. The summary contains a listing of Critical, Major, Minor, Caution, and Information events, with links to more detailed information.

Threat Event - An event detected by Threat Protection.

Certificate - Certificate expiration notification.

Server Exceptions - A Dell Server communication issue is impacting deliveries of the following notifications: Threat Protection, Update, Config, Knowledge Base, and Announcement.

After selecting one or more types, click in the neutral space above the list to apply the selections.

Select **Clear selected items** to reset the selections in this list.

Priority Levels

Notification priority levels are not related to priority levels displayed on the dashboard other than in the notifications area.

Priorities are Critical, High, Medium, and Low. These priority levels are only relative to one another within a type of notification.

Select the priority levels of notifications to include in the dashboard notifications area or email notifications lists. Notifications of the remaining priority levels are not included in the dashboard or email notifications lists.

In the dashboard, after selecting one or more priority levels, click in the neutral space above the list to apply selections.

Select **Clear selected items** to reset the selections in this drop down list. All notifications will display (unless filtered elsewhere).

Endpoint Protection Status

In the Endpoint Protection Status section of the dashboard, view endpoint status by platform: Windows, Mac, and All Platforms with a numeric value and bar chart that shows the numbers of protected and unprotected endpoints. A pie chart representing total protected and unprotected endpoints displays on the left.

Click a value to display a list of the endpoints represented in the value.

Protection Status

To access this page, click a link in the dashboard's Endpoint Protection Status graph. Click a specific platform type or **All**. The page provides protection details on the endpoints within that platform.

Platform - Windows, Mac, All, Protected, or Not Protected

Endpoint ID - Value that uniquely identifies the endpoint.

Protected - A green check mark indicates the endpoint is protected. The protection status of a Windows workstation is derived from the current encryption policies and encryption states of the Encryption client users, as well as the current device encryption policy and state of the endpoint. On the dashboard's Endpoint Protection Status graph, select endpoints by platform, protected endpoints, non-protected endpoints, or all endpoints. See Protected.

Shield Inventory Received - The date and time that the inventory was received and placed in the queue.

Shield Inventory Processed - The date and time that the inventory was picked up from the queue and processed. (**Note**: If the server is under load, the Processed and Received times may be different, but usually they are the same.)

Agent Inventory Received - The date and time that the inventory was received and placed in the queue.

Agent Inventory Processed - The date and time that the inventory was picked up from the queue and processed (**Note**: If the Dell Server is under load, the Processed and Received times may be different, but usually they are the same.)

Shield - If encryption is installed on the endpoint, an icon displays.

Manager (Windows only) - If installed on the endpoint, an icon displays. This includes endpoints with activated PBA, SED, or BitLocker Manager.

Threat Protection Status

Threat Protection monitors the network for viruses, spyware, unwanted programs, suspicious communications through the firewall, and unsafe websites and downloads.

The Threat Protection Status pane shows threats by category: Critical, Major, Minor, and Caution. Each category is listed in a colored bar chart with a numerical value for the corresponding number of threats found during the time frame.

The time frame is selectable, in days: 1, 7, 14, 30, 60, and 90 days.

Click a Threat Category value to display a detailed list of threats included in the category.

Threat Protection Status for Severity Level

To access this page, click a value on the dashboard's Threat Protection Status graph.

This page provides a detailed view of threats based on individual severity levels and devices that have a threat within that severity level. The columns list the specific counts for each type of threat event on a device.

List of severity levels - Select a another option from the list (Critical, Major, Minor, Caution, Information). **Critical** is the most dangerous threat to the endpoint, and **Information** is a notification of an event that is unlikely to harm the endpoint.

List of days - Select a time frame option: 1, 7, 14, 30, 60, and 90 days.

Platform - The platform type

Device ID - Value that uniquely identifies the target device. Click a link to view information about that endpoint.

Event Count columns - For each device, lists the number for each of the following threat events:

Malware/Exploit - Includes counts for viruses, spyware, and unwanted programs. This could be exploited buffer overflows that seek to execute arbitrary code on a device or attempts to exploit browser vulnerabilities. Counts may include malware that executes from within memory space.

Web Filter - Includes threats related to web browsing and downloads.

Web Protection - Includes threats related to web browsing and downloads.

Firewall - Includes suspicious communications related to incoming or outgoing traffic and any attacks.

Uncategorized - Lists the number of threats that do not belong in other event counts.

Advanced Threat Prevention Events

The Advanced Threat Prevention Events pane displays a time line of Advanced Threat events over the course of a month, by file type as assigned by Advanced Threat Prevention.

Click a file type for details of the events of that type.

File types include:

Unsafe - A suspicious file with a high score (-60 to –100) likely to be malware

Abnormal - A suspicious file with a lower score (-1 to –59) less likely to be malware

Quarantined - A file that is moved from its original location, stored in the Quarantine folder, and prevented from executing on a specific device.

Waived - A file allowed to execute on a specific device.

Cleared - A file that has been cleared within the organization. Cleared files include files that are Waived, added to the Safe list, and deleted from the Quarantine folder on a device.

For more detail about events, see Advanced Threat Prevention Classifications and Advanced Threats Top Ten

Advanced Threats by Priority

Advanced Threats by Priority classifies suspicious files by priority levels of High, Medium, and Low. This prioritization helps administrators determine which threats and devices to address first. To view a list of threats with the corresponding priority level, click a value in *Advanced Threats by Priority* on the dashboard.

Files are analyzed for the following attributes:

- The file has a Cylance score greater than 80.

  A score is assigned to each file that is deemed Abnormal or Unsafe. The score represents the confidence level that the file is malware. The higher the number, the greater the confidence.
- The file is currently running.
- The file has been run previously.
- The file is set to auto run.
- The file is detected by Execution Control.

Files are prioritized based on the number of the above attributes it has:

Low = 0-1 attributes

Medium = 2-3 attributes

High = 4-5 attributes

As an example, following is the analysis of three threats:

Threat 1

Attribute	Attribute Value	Score
Cylance score	90	+1
Currently running on any device	True	+1

Ever run on any device	True	+1
Set to auto run on any device	True	+1
Detected by Execution Control	False	+0
	Total score	**5: High Priority**

Threat 2

Attribute	Attribute Value	Score
Cylance score	20	+0
Currently running on any device	True	+1
Ever run on any device	False	+0
Set to auto run on any device	True	+1
Detected by Execution Control	False	+0
	Total score	**2: Medium Priority**

Threat 3

Attribute	Attribute Value	Score
Cylance score	20	+0
Currently running on any device	False	+0
Ever run on any device	False	+0
Set to auto run on any device	False	+0

Detected by Execution Control	True	+5
	Total score	**5: High Priority**

Advanced Threat Prevention Classifications

Advanced Threat Prevention can provide details on the static and dynamic characteristics of files. This allows administrators to not only block threats, but also to understand threat behavior to further mitigate or respond to threats.

Type of Threat

Threats are classified by the type of threat - Malware, Dual Use, and Potentially Unwanted Program.

Malware

If the file is identified as a piece of malware, the file should be removed or quarantined as soon as possible. Verified malware can be further subclassified as one of the following:

Subclass	Definition	Examples
Backdoor	Malware that provides unauthorized access to a system, bypassing security measures.	Back Orifice, Eleanor
Bot	Malware that connects to a central Command and Control (C&C) botnet server.	QBot, Koobface
Downloader	Malware that downloads data to the host system.	Staged-Downloader
Dropper	Malware that installs other malware on a system.	
Exploit	Malware that attacks a specific vulnerability on the system.	
FakeAlert	Malware that masquerades as legitimate security software to trick the user into fixing fake security problems at a price.	Fake AV White Paper
Generic	Any malware that does not fit into an existing category.	
InfoStealer	Malware that records login credentials and/or other sensitive information.	Snifula
Ransom	Malware that restricts access to system or files and demands payment for removal of restriction, thereby holding the system for ransom.	CryptoLocker, CryptoWall
Remnant	Any file that has malware remnants post removal attempts.	
Rootkit	Malware that enables access to a computer while protecting itself or other files to avoid detection and/or removal by administrators or security technologies.	TDL, Zero Access Rootkit
Trojan	Malware that disguises itself as a legitimate program or file.	Zeus

Virus	Malware that propagates by inserting or appending itself to other files.	Sality, Virut
Worm	Malware that propagates by copying itself to another device.	Code Red, Stuxnet

Dual Use

Dual Use indicates the file can be used for malicious and non-malicious purposes. Caution should be used when allowing the use of these files in your organization. For example, while PsExec can be a useful tool for executing processes on another system, that same benefit can be used to execute malicious files on another system.

Subclass	Definition	Examples
Crack	Technologies that can alter (or crack) another application to bypass licensing limitations or Digital Rights Management protection (DRM).	
Generic	Any Dual Use tool that does not fit into an existing category.	
KeyGen	Technologies which can generate or recover/reveal product keys that can be used to bypass Digital Rights Management (DRM) or licensing protection of software and other digital media.	
MonitoringTool	Technologies that track a user's online activities without awareness of the user by logging and possibly transmitting logs of one or more of the following: • user keystrokes • email messages • chat and instant messaging • web browsing activity • screenshot captures • application usage	Veriato 360, Refog Keylogger
Pass Crack	Technologies that can reveal a password or other sensitive user credentials either by cryptographically reversing passwords or by revealing stored passwords.	l0phtcrack, Cain & Abel
RemoteAccess	Technologies that can access another system remotely and administer commands on the remote system, or monitor user activities without user notification or consent.	Putty, PsExec, TeamViewer
Tool	Programs that offer administrative features but can be used to facilitate attacks or intrusions.	Nmap, Nessus, P0f

Potentially Unwanted Programs

The file has been identified as a **P**otentially **U**nwanted **P**rogram. This indicates that the program may be unwanted, despite the possibility that users consented to download it. Some PUPs may be permitted to run on a limited set of systems in your organization (EX. A VNC application allowed to run on domain administrator devices). A Dell Server administrator can choose to waive or block PUPs on a per device

basis or globally quarantine or safelist based on company policies. Depending on how much analysis can be performed against a PUP, further subclassification may be possible. Those subclasses are shown below and will aid an administrator in determining whether a particular PUP should be blocked or allowed to run:

Subclass	Definition	Examples
Adware	Technologies that provide annoying advertisements (example: pop-ups) or provide bundled third-party add-ons when installing an application. This usually occurs without adequate notification to the user about the nature or presence of the add-on, control over installation, control over use, or the ability to fully uninstall the add-on.	Gator, Adware Info
Corrupt	Any executable that is malformed and unable to run.	
Game	Technologies that create an interactive environment with which a player can play.	Steam Games, League of Legends
Generic	Any PUP that does not fit into an existing category.	
HackingTool	Technologies that are designed to assist hacking attempts.	Cobalt Strike, MetaSp0it
Portable Application	Program designed to run on a computer independently, without needing installation.	Turbo
Scripting Tool	Any script that can run as if it were an executable.	AutoIT, py2exe
Toolbar	Technologies that place additional buttons or input fields on-screen.	Nasdaq Toolbar, Bring Me Sports

Score

A **Score** is assigned to each file. Negative scores, from -1 to -100 denote files that are deemed Abnormal or Unsafe. The score represents the confidence level that the file is malware. The higher the negative number, the greater the confidence.

File Type

The file is assigned a type, based on the score.

File Types:

- Unsafe: A file with a score ranging from -60 to -100. An Unsafe file is one in which the Advanced Threat Prevention agent finds attributes that greatly resemble malware.
- Abnormal: A file with a score ranging from -1 to -59. An Abnormal file has a few malware attributes but fewer than an unsafe file, thus is less likely to be malware.

Note: Occasionally, a file may be classified as Unsafe or Abnormal even though the score displayed doesn't match the range for the classification. This could result from updated findings or additional file analysis after the initial detection. For the most up-to-date analysis, enable **Auto Upload** in the Device Policy.

Priority Level

The file is given a p**riority level**. The priority level helps administrators determine which threats and devices to address first. For more information, see Advanced Threats by Priority.

Advanced Threats Top Ten

Click **Threats** to view the threats found on the largest number of devices.

- Click a threat to display additional information about the threat. Details display on a new page.

Click **Devices** to view a list of devices that have the largest number of threats.

- Click a device to display additional information about the device. Details display on a new page.

Endpoint Protection History

This graph gives a time line snapshot of the past 90 days of the total number of endpoints that are protected and total number that are not protected. This graph is especially useful during initial deployment, when moving toward complete protection.

The green bars represent the total number of protected endpoints. The red bars represent the total number of endpoints that are not protected.

Endpoint Inventory History

This graph gives a time line snapshot of the past 90 days of the total number of endpoints that have communicated with and sent inventory to the Dell Server and the total number that have not sent inventory.

Summary Statistics

Summary Statistics provides a breakdown of the following:

- Domains
- User groups
- Endpoint groups
- AD users
- Local users
- Endpoints
- Protected
- Not protected
- Shields
- Managers
- Modified policies

Summary Statistics provides a breakdown of endpoints by platform, with a link to a detailed report for the selected platform:

- Windows

- Mac
- All

Endpoint OS Report

To access this page, click a platform link on the dashboard's Summary Statistics. If you click **All** and the Platform Report page opens, click **view** in the OS Report column.

OS/Version - Operating system name and version as reported in the endpoint's inventory

Count - Number of endpoints or devices

Shielded - Number of encrypted endpoints for that OS and version

Unshielded - Number of endpoints for that OS and version that are not encrypted

Platform Report - Click **view** for a report on all the platforms

Endpoint List - Click the icon to navigate to the Endpoints page and the list of endpoints for that OS and version

Platform Report

To access this page, click **All** on the dashboard's Summary Statistics. If you click a specific platform link and access the Endpoint OS Report page, click **view** in the Platform Report column.

Platform - Windows or Mac

Count - Number of endpoints or devices Platform Report for that platform

Shielded - Number of encrypted endpoints for that platform

Unshielded - Number of endpoints for that platform that are not encrypted

OS Report - Click **view** for a report based on each operating system/version for that platform

Endpoint List - Click the icon to navigate to the Endpoints page and the list of endpoints for that platform

Populations

Populations

A population is a grouping for which policies, settings, and actions can be configured.

To access a Populations page, click **Populations** in the left pane and select a Population. For example, **Populations > Enterprise**.

Tabs available on each Populations page provide information, allow you to edit details of the Population, and provide configuration options for that Population. The table lists the tabs available for each Population.

Populations	Security Policies	Details & Actions	Members	Settings	Key Server	Endpoint Groups	Endpoi
Enterprise	•						

Domains	•	•	•	•	•		
User Groups	•	•	•				
Users	•	•					•
Endpoint Groups	•	•	•				
Endpoints	•	•				•	
Administrators		•					

To access the tabs for each Population:

- Enterprise - Click **Populations > Enterprise**.
- Populations other than Enterprise - Click a Population link, then search for or click a Domain, User Group, User, Endpoint Group, Endpoint, or Administrator link.

The tabs available for an administrator may vary, depending on the role.

Enterprise

View or Modify Enterprise Policies

To view or modify Enterprise policies, follow these steps:

1. In the left pane, click **Populations > Enterprise**.
2. Click the **Security Policies** tab.
3. Select the technology group, such as *Windows Encryption*, or policy group, such as *Policy-Based Encryption*, to view or modify.

View Threat Events

Threats are categorized as Malware/Exploit, Web Filter, Firewall, or Uncategorized events. The list of threat events can be sorted by any of the column headers. You can view threat events for the entire enterprise or for a specific endpoint. To view threat events of a specific endpoint, from the Enterprise Threat Events tab, select the endpoint's device in the Device ID column.

To view threat events in the enterprise, follow these steps:

1. In the left pane, click **Populations > Enterprise**.
2. Click the **Threat Events** tab.
3. Select the desired severity level and time period to display events.

To view threat events on a specific endpoint, follow these steps:

1. In the left pane, click **Populations > Endpoints**.
2. Search or select a hostname, then the **Threat Events** tab.

Manage Enterprise Advanced Threats

Advanced Threats tab

If the Advanced Threat Prevention service is provisioned and licenses are available, the Advanced Threats tab provides a dynamic display of detailed events information for the entire enterprise, including a list of the devices on which events occurred and any actions taken on those devices for those events. For information about provisioning the service, see Provision Advanced Threat Prevention Service.

To access the Enterprise Advanced Threats tab, follow these steps:

1. In the left pane, click **Populations > Enterprise**.
2. Select the **Advanced Threats** tab.

Information about events, devices, and actions are organized on the following tabs:

Protection - Lists potentially harmful files and scripts and details about them, including the devices on which the files and scripts are found.

Agents - Provides information about devices running the Advanced Threat Prevention client as well as the option to export the information or remove devices from the list.

Global List - Lists files in the Global Quarantine and Safe list and provides the option to move files to these lists.

Options - Provides a way to integrate with Security Information Event Management (SIEM) software using the Syslog feature as well as export Advanced Threat data.

Certificate - Allows certificate upload. After upload, certificates display on the Global List tab and can be Safe listed.

Tables on the tabs can be organized in these ways:

Add or remove columns from the table - Click the arrow next to any column header, select **Columns**, then select the columns you want to display. Clear the check box of columns to hide.

Sort the data - Click a column header.

Group by a column - Drag the column header up, until it turns green.

Filter based on data of one column - click the down-arrow on any column to display the context menu, and select **Filter**.

Advanced Threat Events tab

The Advanced Threat Events tab displays information about events for the entire enterprise based on information available in the Dell Server.

The tab displays if the Advanced Threat Prevention service is provisioned and licenses are available.

To export data from the Advanced Threat Events tab, click **Export** and select **Excel** or **CSV** file format.

Note: Excel files are limited to 65,000 rows. CSV files have no size limit.

For a list of fields and filters on the tab, see Advanced Threat Events tab fields and filters.

Domains

Domains

On the Domains page, you can add a domain or search and select a domain to View or Modify Domain Information.

Add a Domain

To add a Domain, follow these steps:

1. In the left pane, click **Populations > Domains**.
2. On the Domains page, click **Add**.
3. Complete the fields on the Add Domains page.

   Domain DNS Suffix - Enter the fully qualified host name or the computer name and domain portion of the hostname (for example, <computer_name>.<domainname>.com) for the enterprise directory server.

   Port - Enter a port for the directory server. If you do not specify a port, the default port of 389 is used. The secure port, 636, uses an SSL connection instead of clear text. Global catalog ports are 3268 (clear-text) and 3269 (secure).

   Distinguished Name - Populated when you tab from the completed Host Name field or refresh the URL. If necessary, correct the entry to reflect the domain (for example, DC=domainname, DC=com).

   User Name - Enter a user name with rights for the domain to read and run queries on the enterprise directory server. The format *must* be UPN, such as user@domain.com. The credentials are domain-specific. Dell Server does not fully observe trusted relationships between domains.

   Password - Enter a password with rights for the domain to read and run queries on the enterprise directory server. The credentials are domain-specific. Dell Server does not fully observe trusted relationships between domains.
4. In the Domain Alias area, enter the domain name or other alias and click **Add**. It is recommended that you add a pre-Windows 2000 domain name as an alias. You may enter any UPN suffixes that are allowed for the domain and are configured in the enterprise directory server.

   A Domain Alias is a mapping the Dell Server uses to select which domains to search to locate users that might match the suffix in the UPN.
5. Click **Add Domain**.

Users

Users are added through reconciliation. Reconciliation is the automated process the Dell Serveruses to compare user data in the Dell Server database with user data in the enterprise directory server and update the Dell Server database when necessary.

In the left pane, click **Populations > Users** and then click a user name, to view details about the user. Click the arrow next to a User Name to view the Common Name, sAM Account Name, and User Principal Name.

Add a User by Domain

1. In the left pane, click **Populations > Users**.
2. On the Users page, click **Add Users by Domain**.
3. In the Add Users by Domain dialog, select a domain from the pull-down list.

4. In *Full name*, enter the exact text for the user name or use the wildcard character (*).
5. Select Common Name, Universal Principal Name, or sAMAccountName from the list.

   A Common Name, Universal Principal Name, and sAMAccountName must be defined in the enterprise directory server for every user. If a user is a member of a domain or group but does not display in the domain or group members list in the Management Console, ensure that all three names are properly defined for the user in the enterprise directory server.
6. Click **Search**. Depending on the size, this may take a few minutes to populate.

   If the query is too large, a dialog prompts you to revise the query.
7. Select users from the directory user list to add to the Domain. The user names are added to the field below the list.
8. Click **X** to remove the user name or click **Add**.

User Groups

Add a user group, edit User Group priority, or search and select a user group to View or Modify User Group Policies and Information.

Add a User Group

1. In the left pane, click **Populations > User Groups**.
2. On the User Groups page, click **Add**.
3. Select the type of User Group from the list: **Active Directory User Group** or **ADMIN-DEFINED User Group**
4. Select a domain from the list.
5. For Active Directory User Groups, follow these steps:

   a. Enter the exact text for the group name or use the wildcard character (*).

   b. Click **Search**. Depending on the size, this may take a few minutes to populate.

   c. Select a group from the list to add to the domain. The group name is added to the field below the list.

   Click the **X** in the group name to remove the group name.

   d. Click **Add**.
6. For ADMIN-DEFINED User Groups, follow these steps:

   a. Enter the exact text for the group name or use the wildcard character (*).

   b. Enter a description for the group.

   c. Click **Add Group**.

Notes:

1. Universal security groups are only supported for domains that connect through the Global Catalog port.

   Nested groups are not supported.

Add Non-Domain Users

To add non-domain users, the non-domain activation feature can be enabled by contacting Dell ProSupport and requesting instructions.

View or Modify Domain Policies and Information

1. In the left pane, click **Populations > Domains**.
2. Search or select the appropriate Domain Name to display Domain Detail.

   When you click a Domain, the Domain Detail page displays.
3. Click the tab that corresponds with the action to perform:

   Security Policies - To view or modify policies of the Domain, click **Security Policies**.

   Details & Actions - To view properties of the Domain, click **Details & Actions**

   Members - To view, add, or modify information for groups and users within the domain. For instructions on how to perform these tasks, refer to the appropriate topic:

Add Users to Domain

Add User Groups

View or Modify User Information

View or Modify User Group Information

Settings - To configure LDAP settings for the domain, click **Settings**. Refer to Add Domains for instructions.

Domain Details & Actions

The Domain Details & Actions tab lists the properties of a domain.

To access the Domain Details & Actions tab, follow these steps:

1. In the left pane, click **Populations > Domains**.
2. Search or select a Domain Name, then the **Details & Actions** tab.

Details displayed on the Domain Details & Actions tab:

Domain Name - Name of the domain server. This should match the domain name in the title of the page.

Location - The location (path) of the domain within the enterprise structure. This information is derived from the fully qualified hostname or the computer name and domain portion of the hostname entered when the domain was added. Example: /com/enterpriseserver

LDAP Url - URL to the active directory. This field is populated after adding the domain. The information is derived from the completed hostname.

Example - LDAP://domainname.com:portnumber/DC=domainname,DC=com

To configure LDAP settings for the domain, click the **Settings** tab.

Status - Describes the health of the domain server (Good, Fair, Poor).

Domain Members

This page allows you to view, add, or modify information for groups and users within the domain.

To access the Domain Members tab, follow these steps:

1. In the left pane, click **Populations > Domains**.
2. Search or select a Domain Name, then the **Members** tab.

From this tab, you can perform these actions:

Add Users to Domain - Allows you to add users by domain

Add Group - Allows you to add a user group by domain

Select to view the following information about groups & users, users only, or groups only:

User/Group - Each user or user group in the domain. Click an entry to view details.

Distinguished Name

CN is the common name, either a user or group name.

OU is the organizational unit name, for example, Dallas.

DC are domain components, for example, DC=Organization, DC=com

Common Name - For a user, the user name; for a group, the group name

User - Column displays a green checkmark

Group - Column displays a green checkmark

Domain Settings

This page allows you to configure or modify LDAP settings for the Domain.

To access the Domain Settings tab, follow these steps:

1. In the left pane, click **Populations > Domains**.
2. Search or select a Domain Name, then the **Settings** tab.

On the Domain Settings tab, you can view this information:

Directory URL - Lists the current URL for the enterprise directory server. If you modify the settings, click **Refresh URL**.

Host Name - The fully qualified hostname or the computer name and domain portion of the hostname (for example, <computer_name>.<domainname>.com) for the enterprise directory server.

Port - The port for the directory server. If you do not specify a port, the default port of 389 is used. The secure port, 636, uses an SSL connection instead of clear text. Global catalog ports are 3268 (clear-text) and 3269 (secure).

Distinguished Name - This field is populated when you tab from the completed hostname or refresh the URL. If necessary, correct the entry to reflect the domain (for example, DC=domainname, DC=com).

Secure LDAP - Select this check box for LDAPS.

User Name - The user name with rights to read and run queries on the enterprise directory server. The format *must* be UPN, such as user@domain.com.

Password - Enter a password with rights to read and run queries on the enterprise directory server.

Alias - A mapping that the Dell Server uses to select which domains to search to locate users that might match the suffix in the UPN. The domain name or other alias. It is recommended that you add a pre-Windows 2000 domain name as an alias. You may enter any UPN suffixes that are allowed for the domain and are configured in the enterprise directory server.

Click **Add**, and the entry populates the field below.

Select an alias in the list, and click **Remove Selected**.

Update Domain - Click to update changes.

User Groups

User Groups

Add a user group, edit User Group priority, or search and select a user group to View or Modify User Group Policies and Information.

Add a User Group

1. In the left pane, click **Populations > User Groups**.
2. On the User Groups page, click **Add**.
3. Select the type of User Group from the list: **Active Directory User Group** or **ADMIN-DEFINED User Group**
4. Select a domain from the list.
5. For Active Directory User Groups, follow these steps:
    a. Enter the exact text for the group name or use the wildcard character (*).
    b. Click **Search**. Depending on the size, this may take a few minutes to populate.
    c. Select a group from the list to add to the domain. The group name is added to the field below the list.

    Click the **X** in the group name to remove the group name.

    d. Click **Add**.
6. For ADMIN-DEFINED User Groups, follow these steps:
    a. Enter the exact text for the group name or use the wildcard character (*).
    b. Enter a description for the group.
    c. Click **Add Group**.

Notes:

1. Universal security groups are only supported for domains that connect through the Global Catalog port.

    Nested groups are not supported.

Remove User Groups

1. In the left pane, click **Populations > User Groups**.
2. Click a group name link or enter a filter to search for available groups. The wildcard character (*) is supported.
3. Select a row to highlight it.
4. At the top, click **Delete**.

As another option, click a group name link and select the **Details & Actions** tab. Click **Remove Group**.

If you remove a user group that has administrative privileges and later re-add the group, it remains an Administrator Group.

Find User Groups

1. In the left pane, click **Populations > User Groups**.
2. Enter a filter to search for available Groups. The wildcard character (*) is supported.
3. Click **Search**.

   A Group or list of Groups displays, based on the search filter.

View or Modify User Group Policies and Information

1. In the left pane, click **Populations > User Groups**.
2. Search or select the appropriate group name to display the User Group Detail page. The wildcard character (*) is supported.

   Click a group name to display the User Group Detail page.
3. Click the tab that corresponds with the action to perform:

   Security Policies - To view or modify policies of the Group, click **Security Policies**.

   Details & Actions - To view properties of the Group, click **Details & Actions**. Viewable information includes:

   - Group Name: Group1 (DOMAIN\Group1)
   - Distinguished Name: CN=Group1, OU=Dallas, DC=Organization, DC=com
     Common Name: Group1
   - Last Modified in Directory - date and time stamp
   - Last Reconciled - date and time stamp
   - AG Enabled - is configured for a user group when selected

   Members - To view or modify the information of a user in the group, click **Members**. The list of users in the group displays. Click a user to view the user's Security Policies, Details & Actions, Endpoints, User Groups, and Admin. For instructions on how to view or modify User information, refer to View or Modify User Information.

   Admin - To view, assign, or modify administrator roles assigned to the group, click **Admin**. Select or deselect administrator roles to modify administrator roles assigned to the Group. For

more information about privileges available to each administrator role, refer to Administrator Roles.

4. If modified, click **Save**.

VDI User Policies

To manage policy for users in a VDI environment, create a Windows domain group, associate domain users with that group, and then import the group into Dell Server. This allows Dell Server to manage the users and their policies.

Policy settings differ, based on whether persistent or non-persistent VDI is deployed in the environment. For an explanation of the differences between persistent and non-persistent VDI, see Persistent vs. Non-Persistent VDI.

Policy and Configuration Requirements for VDI Users

The policy requirements below are for VDI users running Advanced Threat Prevention. The list includes only policies that are significant for VDI users. VDI endpoint group policy settings must also meet certain requirements. See Policy and Configuration Requirements for VDI Endpoint Groups.

Note: Ensure that you turn off Advanced Threat Prevention Agent Auto Update. In the left pane of the Management Console, select **Management > Services Management > Advanced Threats - Agent Auto Update**, then select **Off**.

Note: With Persistent VDI groups, ensure that roaming user profiles are configured.

These policy and configuration settings for VDI users must be configured before VDI client activation:

Technology	Category	Policy or Setting	Persistent VDI group setting	Non-Persistent VDI group setting
Windows Encryption	Policy-Based Encryption	Policy-Based Encryption	On	Off
Windows Encryption	Policy-Based Encryption	Encrypt Outlook Personal Folders	Not Selected	Not Selected
Windows Encryption	Policy-Based Encryption	Encrypt Temporary Files	Not Selected	Not Selected
Windows Encryption	Policy-Based Encryption	Encrypt Temporary Internet Files	Not Selected	Not Selected
Windows Encryption	Policy-Based Encryption	Encrypt User Profile Documents	Not Selected	Not Selected
Windows Encryption	Policy-Based Encryption	Secure Post-Encryption Cleanup	Single-pass Overwrite	Single-pass Overwrite
Windows Encryption	Policy-Based Encryption	Force Logoff/Reboot on Policy Updates	Selected	Not Selected
Removable Media Encryption	Windows Media Encryption	Windows Media Encryption	On	On
Removable Media Encryption	Windows Media Encryption	EMS Scan External Media	Not Selected	Not Selected

User Group Details & Actions

The User Group Details & Actions tab lists the properties of a selected user group.

1. In the left pane, click **Populations > User Groups**.
2. Search or select a group name, then the **Details & Actions** tab.

Remove Group

The **Remove Group** command permanently removes this user group from the Dell Server.

Details:

Group Name - Name of the user group <user group>(<domain name>\<user group>). This should match the user group name in the title of the page.

Distinguished Name - CN=Group1, OU=Dallas, DC=Organization, DC=com

CN is the common name

OU is the organizational unit name

DC are domain components

Common Name - non-technical name of the user group

Last Modified - Date/time stamp of the last time this information changed.

Last Reconciled - Date/time stamp of the last time this information was reconciled.

s Enabled - is configured for a user group when selected.

User Group Members

This page displays information about each user within the user group.

1. In the left pane, click **Populations > User Groups**.
2. Search or select a Group Name, then click the numeral in the **Members column**.

User - Each user in that user group

Distinguished Name - CN=Group1, OU=Dallas, DC=Organization, DC=com

CN is the common name

OU is the organizational unit name

DC are domain components

Common Name - non-technical name of the user group

Add Users to the Group

1. On the **Members** tab, click **Add Users to Group**.
2. Search or select a user, then select the check box to the left of the user name.
3. Click **Add Selected Users to Group**.

OR

Select **Upload Multiple User from File**, then click **Browse** to select a CSV file and click **Upload**.

Valid CSV requirements:

- The file must be in valid CSV format and contain a maximum of 999 endpoints.
- The first column must contain valid fully qualified host names. All columns except the first column are ignored.
- Only activated endpoints are added to the group.

Remove Users from the Group

1. In User Group Detail, search or select a user, then select the check box to the left of the user name.
2. Click **Remove Users from Group**.
3. Click **OK**.

Users can also be removed from the ADMIN DEFINED Groups.

User Group Admin

Assign, modify, or view Administrator roles for a group.

1. In the left pane, click **Populations > User Groups**.
2. Search or select a Group Name, then the **Admin** tab.

Administrator Roles - Assign or modify roles for a group membership and click **Save**.

Delegated Roles - Delegate Administrator rights for the Group to a User.

Related topics:

Administrator Roles

Assign or Modify Administrator Roles

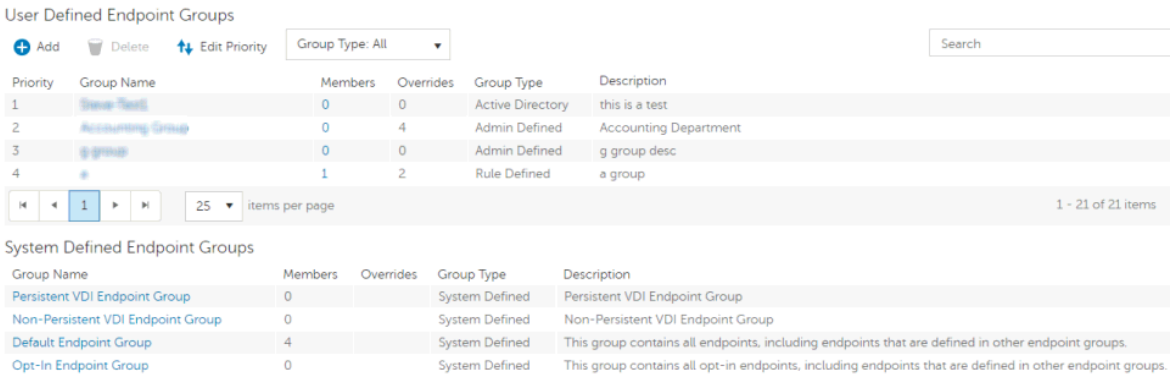
Delegate Administrator Roles

Edit Group Priority

The Group priority feature is used to determine policy precedence for effective policies that affect multiple groups. Group priority creates a weight associated with the specific group it is assigned to, and that weight is used to determine which policy setting is applied to an endpoint that is a member of more than one Endpoint Group when policy settings differ between those groups. Policy overrides are used from the group with higher priority when two (or more) separate groups have different priority levels.

Edit Endpoint Group Priority

Endpoint Group Priority can be changed only for Rule-Defined, Admin-Defined, and Active Directory Groups. System-Defined Group priority cannot be modified. In general, the Endpoint Group at the top of the list of Endpoint Groups has highest priority. The Endpoint Group at the bottom of the list has lowest priority.



Precedence Ranking

The System Defined Non-Persistent VDI Endpoint Group has the highest priority level, followed by the Persistent VDI Endpoint Group.

Order of priority:

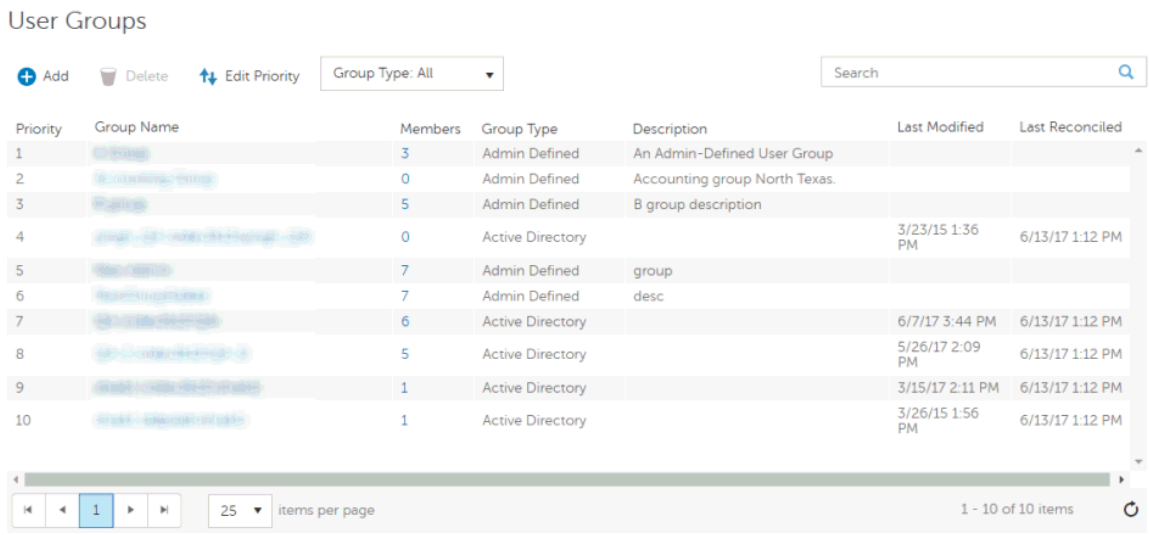
1. Non-Persistent VDI Endpoint Group
2. Persistent VDI Endpoint Group
3. Highest ranked Active Directory/Rule-Defined/Admin-Defined Endpoint Group
4. Second and subsequent highest ranked Active Directory/Rule-Defined/Admin-Defined Endpoint Groups
5. Opt-in Endpoint Group
6. Default Endpoint Group

To change Active Directory/Rule-Defined/Admin-Defined Endpoint Group priority:

1. In the left pane, click **Populations > Endpoint Groups**.
2. Click **Edit Priority**.
3. Select the row of the appropriate group and drag it to the location in the list of Endpoint Groups that reflects its new priority level.
4. Click **Save**.

Edit User Group Priority

The user group at the top of the list has highest priority. The user group at the bottom of the list has lowest priority.



To edit User Group priority:

1. In the left pane, click **Populations > User Groups**.
2. Click **Edit Priority**.
3. Select the row of the appropriate group and drag it to the location in the list of Endpoint Groups that reflects its new priority level.
4. Click **Save**.

Assign or Modify Administrator Roles

View or modify existing administrator privileges.

1. In the left pane, click **Populations > Administrators**.
2. Search or select the row that displays the user name of the appropriate administrator to display User Detail.
3. View or modify administrator roles in the pane at the right.
4. Click **Save**.

Dell recommends assigning administrator roles at the Group level rather than at the User level.

1. In the left pane, click **Populations > User Groups**.
2. Search or select a group name, then the **Admin** tab.
3. Select or deselect administrator roles assigned to the group.
4. Click **Save**.

If you remove a group that has administrative privileges and later re-add the group, it remains an administrator group.

To view, assign, or modify administrator roles at the User level, see User Admin.

Related topics:

Administrator Roles

User Admin

Delegate Administrator Roles

View Reconciliation Date

To view the date and time a user group's or user's information was last reconciled with Active Directory, click the Details & Actions tab for the group or user, and refer to last reconciled. For instructions, refer to View or Modify User Group Policies and Information and View or Modify User Policies and Information.

View Policy Proxy State

The Management Console tracks the Policy Proxy's policy updating state.

1. In the left pane, click **Populations > Endpoints**.
2. Select an endpoint type, for example, **Workstation**.
3. If you know the full endpoint hostname, enter it into *Search* and click .

   For Windows and Mac, enter the full endpoint hostname if you know it. Leave the field blank to display all Windows and Mac endpoints.

   If you do not know the full hostname, scroll through the list of available endpoints to locate the endpoint.
4. Click an endpoint in the list to display the endpoint detail.
5. Click the **Details & Actions** tab of the endpoint to view information.

Users

Users

Users are added through reconciliation. Reconciliation is the automated process the Dell Serveruses to compare user data in the Dell Server database with user data in the enterprise directory server and update the Dell Server database when necessary.

In the left pane, click **Populations > Users** and then click a user name, to view details about the user. Click the arrow next to a User Name to view the Common Name, sAM Account Name, and User Principal Name.

Add a User by Domain

1. In the left pane, click **Populations > Users**.
2. On the Users page, click **Add Users by Domain**.
3. In the Add Users by Domain dialog, select a domain from the pull-down list.
4. In *Full name*, enter the exact text for the user name or use the wildcard character (*).
5. Select Common Name, Universal Principal Name, or sAMAccountName from the list.

   A Common Name, Universal Principal Name, and sAMAccountName must be defined in the enterprise directory server for every user. If a user is a member of a domain or group but does not display in the domain or group members list in the Management

Console, ensure that all three names are properly defined for the user in the enterprise directory server.

6. Click **Search**. Depending on the size, this may take a few minutes to populate.

   If the query is too large, a dialog prompts you to revise the query.

7. Select users from the directory user list to add to the Domain. The user names are added to the field below the list.
8. Click **X** to remove the user name or click **Add**.

Remove Users

In general, a user cannot be removed in the Management Console. Instead, you must remove the user from Active Directory.

Find Users

1. In the left pane, click **Populations > Users**.
2. Do one of these:
   - Enter the user name or a filter in *Search* and click  .
   - Enter Common Name, Universal Principal Name, or sAMAccountName. The wildcard character is supported.
   - Scroll through the user name list.
3. Click a link in the user name column.

   The User Detail page opens, displaying the Security Policies tab.

Deactivate/Suspend Users

If the user to deactivate is no longer associated with your organization, be sure the *Current Shield State* policy is set to a value other than *Activate*, and ensure that the policy commit is complete and successful prior to your enterprise directory server. The user does not need to be in your enterprise directory server, but the policy does need to delivered to be their device for it to take effect.

Best Practice - Deleting users from the enterprise directory server is not recommended. If a user leaves the organization, the account should be moved to a disabled group. With that said, if a deletion occurs, the user is simply marked “removed”, rather than deleted. The user does not display in the Management Console, but their encryption keys and other information are still available in the Dell Server database.

1. In the left pane, click **Populations > Users**.
2. Click a user name link or enter a filter to search for available users.

   Enter Common Name, Universal Principal Name, or sAMAccountName. The wildcard character (*) is supported. On the User Detail > Security Policies tab in the *Windows Encryption* technology group, click the Policy-Based Encryption policy group.
3. Click **Show advanced settings**.
4. Change the *Current Shield State* policy to **Suspend**.

5. Click **Save**.
6. Commit Policies.

To reactivate a deactivated Windows user, follow the instructions in Reinstate Suspended Users.

Reinstate Suspended Users

To reinstate a suspended user, follow these steps:

1. In the left pane, click **Populations > Users**.
2. Click a user name link or enter a filter to search for available users.

   To Search, enter Common Name, Universal Principal Name, or sAMAccountName. The wildcard character (*) is supported.
3. On the **User Detail > Security Policies** tab in the *Windows Encryption* technology group, click the **Policy-Based Encryption** policy group.
4. Click **Show advanced settings**.
5. Change the *Current Shield State* policy to **Activate**.
6. Click **Save**.
7. Commit Policies.

   Repeat these steps for each type of device the user was suspended from.
8. To reinstate a suspended Dell Encryption user, perform the preceding steps and then run WSDeactivate on the computer that was suspended for that particular user. WSDeactivate and its instructions are located in the Dell installation media. When using WSDeactivate, existing local encryption keys, credentials, and policy material are no longer accessible to Dell Encryption, and all managed users are forced to reactivate upon their next log on.

View or Modify User Policies and Information

1. In the left pane, click **Populations > Users**.
2. Click a user name or enter a filter to search for available users. The wildcard character (*) is supported.

   Click a user name to display the User Detail page.
3. Click the tab that corresponds with the action to perform:

   Security Policies - Click to view or modify policies of the user.

   Details & Actions - Click to view properties of the user. Viewable information includes:

   User Name: (username@organization.com)

   Distinguished Name: CN=User Name, OU=Dallas, DC=Organization, DC=com

   Common Name: User Name

   User Principal Name: username@organization.com

   sAM Account Name: username

   User Type - possible values are *AD* or *local*

Last Modified - Date/time stamp

Last Reconciled - Date/time stamp

Endpoints - Click to view or modify information for the User's endpoints. For instructions on how to modify endpoint information, refer to View or Modify Endpoint Information.

User Groups - Click **Groups** to view information for groups for which the user belongs. Click a user group to view the group's Security Policies, Details & Actions, Members, and Admin.

Admin - Click to view, assign, or modify administrator roles assigned to the user. Select or deselect administrator types to modify administrator roles assigned to the user.

4. If modified, click **Save**.

User Details & Actions

The user Details & Actions tab lists the properties of the selected user.

1. In the left pane, click **Populations > Users**.
2. Search or select a user name, then the **Details & Actions** tab.

Details:

User Name - (username@organization.com)

Distinguished Name - CN=User Name, OU=Dallas, DC=Organization, DC=com

Common Name - User Name

Universal Principal Name - username@organization.com

sAMAccountName - username

Email - User email address

User Type - possible values are AD or local

Last Modified - Date/time stamp

Last Reconciled - Date/time stamp

User Endpoints

This page displays information about a user's endpoints, listed by platform type.

1. In the left pane, click **Populations > Users**.
2. Search or select a user name, then the **Endpoints** tab.

Shield

Platform - The platform type

Device ID - Value that uniquely identifies the target device

Last Successful Login - Date/time stamp, per endpoint

Last Unsuccessful Login - Date/time stamp, per endpoint

Last Gatekeeper Sync - Date/time stamp, per endpoint

Effective Policies - Click **view** for a simple layout view of the effective endpoint policies

Actions - Click **Recover** to proceed to the Recover Data page

Last Encryption Sweep Start - Date/time stamp, per user

Sweep End - Date/timestamp, per user

Encryption Failure - Click **view** for a simple list of files that could not be encrypted, per user

States (Date/time stamp, per endpoint):

Policy Updating

User Encryption Profile Updating

EMS Encryption Profile Updating

User Data Encryption On

Deactivation Pending

Suspension Pending

Suspended

User Groups

If the user belongs to a user group, this page displays information about the group and provides a link to the group.

1. In the left pane, click **Populations > Users**.
2. Search or select a user name, then the **Users Groups** tab.

User Group - Group to which the user belongs

Distinguished Name - CN=Group1, OU=Dallas, DC=Organization, DC=com

CN is the common name

OU is the organizational unit name

DC are domain components

Common Name - non-technical name of the user group

User Admin

This page allows you to assign, modify, or view administrator roles for the user.

1. In the left pane, click **Populations > Users**.
2. Search or select a user name, then the **Admin** tab.

Administrator Roles - Assign or modify roles for the user and click **Save**.

Inherited Group Roles - A read-only list of roles that the user inherited from a group. To modify the roles, click the **User Groups** tab for that user and select the group name.

Delegated Roles - Delegate administrator rights to a user.

Related topics:

Administrator Roles

Assign or Modify Administrator Roles

Delegate Administrator Roles

View Reconciliation Date

To view the date and time a user group's or user's information was last reconciled with Active Directory, click the Details & Actions tab for the group or user, and refer to last reconciled. For instructions, refer to View or Modify User Group Policies and Information and View or Modify User Policies and Information.

View Policy Proxy State

The Management Console tracks the Policy Proxy's policy updating state.

1. In the left pane, click **Populations > Endpoints**.
2. Select an endpoint type, for example, **Workstation**.
3. If you know the full endpoint hostname, enter it into *Search* and click .

   For Windows and Mac, enter the full endpoint hostname if you know it. Leave the field blank to display all Windows and Mac endpoints.

   If you do not know the full hostname, scroll through the list of available endpoints to locate the endpoint.
4. Click an endpoint in the list to display the endpoint detail.
5. Click the **Details & Actions** tab of the endpoint to view information.

Issue a User Decryption Policy

1. In the left pane, click **Populations > Users**.
2. Click a user name link or search for a user and then click a link to display the user detail.

   Enter Common Name, Universal Principal Name, or sAMAccountName. The wildcard character (*) is supported.
3. On the **Security Policies** tab, click **Policy-Based Encryption**.
4. Set the value of *Policy-Based Encryption* to **Off**.
5. Click **Save**.
6. Commit Policies.

Once this policy reaches the specified Encryption client, decryption begins.

Endpoint Groups

Endpoint Groups

On the Endpoint Groups page, you can add or remove an Endpoint Group, edit Endpoint Group priority, or search and select an Endpoint Group to view or modify Endpoint Group information.

Types of Endpoint Groups

System - Endpoint Group maintained by Dell Server. System groups include Default Endpoint Group, Opt-In Endpoint Group, Persistent VDI Endpoint Group, and Non-Persistent VDI Endpoint Group. For more information about VDI Endpoint Groups, see VDI Endpoint Groups.

Rule-Defined - Dynamic Endpoint Group based on a specification, or rule set, defined by the administrator.

Admin-Defined - Static endpoint group for which the administrator can select specific endpoints for inclusion. The group remains unchanged unless the administrator adds or removes an endpoint. For more information, see Add Endpoints to an Admin-Defined Endpoint Group or Remove Endpoints from an Admin-Defined Endpoint Group.

Active Directory Group - Endpoint group for which the administrator can select a group from Active Directory for inclusion. The Active Directory group scope must be Global, and type must be Security. At least one endpoint in the Active Directory group must be running a Dell Data Security product and be managed by Dell Server. For more information about adding Active Directory endpoint groups to the Dell Server, see KB article SLN306875.

Add an Endpoint Group

Before you add the first Endpoint Group see Endpoint Groups Specification, which explains fields and expressions used in Group Specifications.

1. In the left pane, click **Populations > Endpoint Groups**.
2. Click **Add**.
3. In *Select the type of Endpoint Group*, select **RULE-DEFINED Group, ADMIN-DEFINED Group**, or **Active Directory Group**.
4. In *Group Name*, enter a name for the new Endpoint Group.
5. In *Description*, enter a description for the new Endpoint Group.
6. (For Rule-Defined Groups only) In *Specification*, enter the rule that describes the Endpoint Group. Specifications can be up to 20,000 characters and are case insensitive.

   (For Active Directory Groups only) In C*hoose AD Group*, enter the beginning characters of an Active Directory group name (Example: Accounting), and select the desired group.
7. (For Rule-Defined and Active Directory Groups only) Click **Preview** to view the endpoints to be included in the group.
8. Click **Add Group** to save the group definition.
9. After the group is added, modify the group priority if necessary.

Remove an Endpoint Group

1. In the left pane, click **Populations > Endpoint Groups**.
2. Select the group to remove.
3. Click **Delete**, then click **OK**.

Modify an Endpoint Group

1. In the left pane, click **Populations > Endpoint Groups**.
2. Select the group to modify.
3. Click the **Details & Actions** tab.
4. Click **Modify**.
5. Make changes as desired.
6. Click **Update Group**.

VDI Endpoint Groups

Upon activation, a VDI endpoint is added to the appropriate VDI Endpoint Group on Dell Server, and policies are sent to the endpoint. Persistent VDI Endpoint Groups and Non-Persistent VDI Endpoint Groups are System Endpoint Groups, which are maintained by Dell Server.

Policy settings differ, based on whether persistent or non-persistent VDI is deployed in the environment. For an explanation of the differences between persistent and non-persistent VDI, see Persistent vs. Non-Persistent VDI.

Policy and Configuration Requirements for VDI Endpoint Groups

The policy requirements below are for VDI endpoints running Advanced Threat Prevention. The list includes only policies that are significant for VDI endpoints. VDI User policy settings must also meet certain requirements. See Policy and Configuration Requirements for VDI Users.

Note: Ensure that you turn off Advanced Threat Prevention Agent Auto Update. In the left pane of the Management Console, select **Management > Services Management > Advanced Threats - Agent Auto Update**, then select **Off**.

Note: With Persistent VDI Groups, ensure that roaming user profiles are configured.

These policy and configuration settings for VDI Endpoint Groups must be configured before VDI client activation:

Technology	Category	Policy or Setting	Persistent VDI Group setting	Non-Persistent VDI Group setting
Windows Encryption	Self-Encrypting Drive (SED)	Self-Encrypting Drive (SED)	Off	Off
Windows Encryption	Hardware Crypto Accelerator (HCA)	Hardware Crypto Accelerator (HCA)	Off	Off
Windows Encryption	Policy-Based Encryption	SDE Encryption Enabled	Not Selected	Not Selected
Windows Encryption	Policy-Based Encryption	Common Encrypted Folders	<retain default settings>	<retain default settings>
Windows Encryption	Policy-Based Encryption	Encrypt Windows Paging File	Not Selected	Not Selected
Windows Encryption	Policy-Based Encryption	Secure Windows Credentials	Not Selected	Not Selected
Windows Encryption	Policy-Based Encryption	Block Unmanaged Access to Domain Credentials	Not Selected	Not Selected

Windows Encryption	Policy-Based Encryption	Secure Windows Hibernation File	Not Selected	Not Selected
Windows Encryption	Policy-Based Encryption	Prevent Unsecured Hibernation	Not Selected	Not Selected
Windows Encryption	Policy-Based Encryption	Enable Software Auto Updates	Not Selected	Not Selected
Windows Encryption	BitLocker Encryption	BitLocker Encryption	Off	Off
Windows Encryption	Server Encryption	Server Encryption	Off	Off
Threat Prevention	Advanced Threat Protection	Advanced Threat Protection	On	On
Removable Media Encryption	Mac Media Encryption	Mac Media Encryption	Off	Off
Port Control	Windows Port Control	Port Control System	Disabled	Disabled

Persistent vs. Non-Persistent VDI

Persistent and Non-Persistent VDI endpoints differ in the following ways:

Persistent VDI	Non-Persistent VDI
Persistent endpoints may exist for many days to years.	Non-persistent endpoints usually exist only for a few days or weeks.
Persistent endpoints retain the configurations that are set for the VM, until the VM clone pool is removed and rebuilt.	Non-persistent endpoints revert to baseline settings after a user logs off.
A persistent endpoint is dedicated to a single user.	After reverting to baseline settings,a non-persistent endpoint is available for another user.

Endpoint Groups Specification

To skip to instructions about how to add an endpoint, see Add Endpoint Groups.

At deployment time, all endpoints belong to a default endpoint group, which is generally sufficient for most deployments. This feature is used to assign policy to a specific group of endpoints. For instance, you may want to create an endpoint group based on the locale that the operating system sends up in

inventory. Once that endpoint group is established, you could then apply a specific policy set to just the endpoints in your specified locale.

Conversely, creating an endpoint group based on a platform type would not be useful because policies are already grouped by platform.

Endpoint groups are created using a group specification. This specification allows you to define the endpoint characteristics used to add endpoints to a group. You cannot manually add endpoints to endpoint groups. The system, based on the characteristics in the endpoint group specification, automatically manages endpoints and endpoint group membership.

Endpoints can be members of many endpoint groups simultaneously, as there is no mutual exclusion requirement for endpoints in groups. All endpoints are included in the default endpoint group in addition to any defined endpoint groups that they may be a member of. This is similar to the way users are a member of the domain they are a part of, in addition to any security groups. Like the user group mapping, the endpoint group mapping creates a potential policy arbitration problem for endpoints. To resolve this problem, the default endpoint group has the lowest possible precedence, and cannot be altered. The endpoint groups that you create have medium precedence by default. For more information on group precedence, see Modify Group Precedence.

Endpoint Group Specification

The endpoint group specification is a domain specific language that allows you to define groups. The endpoint group specification consists of a set of operators and a set of data fields that these operators can be applied to. A group specification is a Boolean expression that is evaluated per endpoint to determine whether or not a endpoint is a member of a group.

The information obtained to assign endpoints to endpoint groups happens when inventory is received, not at activation time. If you set up endpoint groups, all endpoints will stay only in the default endpoint group until inventory is received.

Group specifications are created using the following fields and expressions. Multiple fields and operators can be used in a single group specification.

Field Name	Description
CATEGORY	Endpoint category: WINDOWS, MAC, SED
UID	Windows hostname
DISPLAYNAME	Fully qualified hostname
OSVERSION	Operating system version as reported in inventory. Dell recommends using other available fields, as discrepancies in operating system versions may reduce the usefulness of this field.
OS	Operating system name as reported in the endpoint's inventory
PROCESSOR	System processor information
SERIALNUMBER	Endpoint serial number
LOCALE	The current locale of the endpoint. This is typically only reported by Encryption Enterprise.
WINCOMPUTERNAME	Fully qualified hostname
ASSETTAG	Asset tag of the computer manufacturer
SHIELDVERSION	Version of Encryption client
AGENTVERSION	Agent version for Manager
PLUGINVERSION	Plugin version for Manager
MEMBEROFGROUP	Active Directory group name
MEMBEROFDOMAIN	Active Directory domain name
SEDPRESENT	All SED clients

BITLOCKERPRESENT	TRUE/FALSE value for BitLocker Manager, indicating if BitLocker is enabled.
TOTALMEMORY	Total memory available on the computer
TPMENABLED	TRUE/FALSE value for TPM, indicating if TPM is enabled
TPMPRESENT	All TPM clients

Operators and Expressions

The basic operators are the binary operators that return a Boolean value.

Operator	Meaning
=	Boolean, Integer, and String equality operator
>, >=	Greater than, greater than or equal, integer operator
<, <=	Less than, less than or equal, integer operator
<>	Not equal, integer string operator
AND	Logical AND for Boolean expression
OR	Logical OR for Boolean expression
NOT	Logical NOT for Boolean expression

The logical operators follow the standard Boolean operator precedence (NOT, AND, OR). String fields have the following string operators that return Boolean values:

BEGINSWITH

ENDSWITH

CONTAINS

These operators can be used on the string fields:

```
UID BEGINSWITH "A1850502"
```

```
ASSETTAG CONTAINS "007"
```

String fields also have the following string operators that return substrings of the field:

LEFT(string,int)

RIGHT(string,int)

MID(string,int,int)

The substring operators can be used in the string operators that return Boolean values:

```
LEFT(DISPLAYNAME, 4 ) = "A185"
```

There is one additional string operator that returns an integer value that is the length of the string:

LEN(string)

This can be used in a Boolean expression:

```
LEN(DISPLAYNAME)<=10
```

Rule Specifications in the Management Console allows users to combine rules to filter a unique set of devices. For queries that contain multiple options, isolate sub-rules in parenthesis to ensure they are run separately before they are combined with the larger specification.

This query selects all devices with an operating system named Windows 10 Pro or Windows 10 Ent and DESKTOP in the hostname:

```
OS CONTAINS "Windows 10 Pro" OR OS CONTAINS "Windows 10 Ent" AND UID
CONTAINS "DESKTOP"
```

This query selects any device containing Windows 10 Pro and only devices with the hostname containing DESKTOP that running an operating system with the name containing Windows 10 Ent:

```
OS CONTAINS "Windows 10 Pro" OR (OS CONTAINS "Windows 10 Ent" AND UID
CONTAINS "DESKTOP")
```

- Using the FQDN of the client computer to attach it to a device group can be done by keying on any commonality amongst the desired client computers. In the example below, a child domain of ORGANIZATION, AMERS, represents a domain in America. Additionally, a 2nd child domain, EMEA, represents non-American based clients.

DISPLAYNAME ENDSWITH "AMERS.ORGANIZATION.COM"

This group will contain all clients that are in the AMERS domain according to their FQDN.

DISPLAYNAME ENDSWITH "EMEA.ORGANIZATION.COM"

This group will contain all clients that are in the EMEA domain according to their FQDN

- If the hostname of the client computers contain several notations that indicate desired ways in which to create a group, those specific portions can be captured as long as their location is consistent.

Looking at the hostname: A12345jdoe.AMER.ORGANIZATION.COM

A denotes an asset, while the following 5 digits denotes the asset's assigned value. The user that was assigned the asset has their SAM account appended to the end.

You can capture the assigned number of the asset, and that it is within a certain subsection of assets. This example shows how to look for assets that have a value less than 1000.

MID(DISPLAYNAME , 2, 5) < 1001

This example targets user's computer where their last name begins with 'r'.

MID(DISPLAYNAME , 8, 1) = "r"

For instructions about how to add an endpoint, see Add Endpoint Groups.

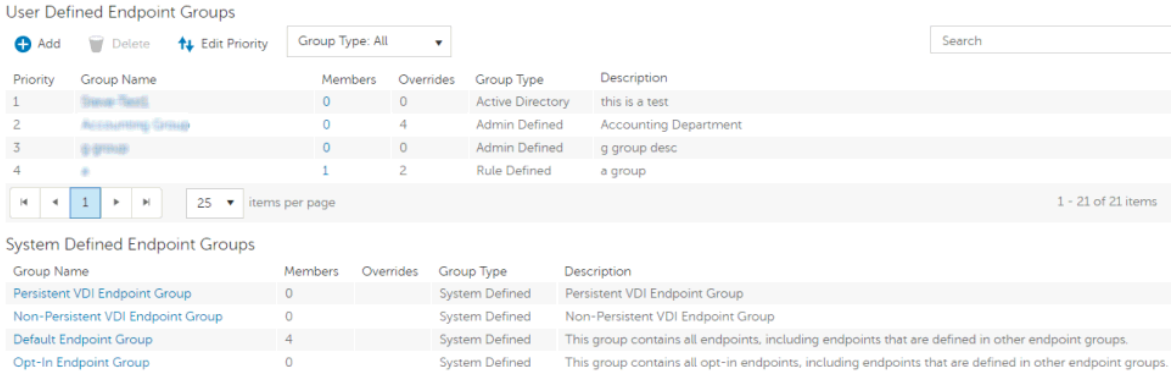
Edit Group Priority

The Group priority feature is used to determine policy precedence for effective policies that affect multiple groups. Group priority creates a weight associated with the specific group it is assigned to, and that weight is used to determine which policy setting is applied to an endpoint that is a member of more

than one Endpoint Group when policy settings differ between those groups. Policy overrides are used from the group with higher priority when two (or more) separate groups have different priority levels.

Edit Endpoint Group Priority

Endpoint Group Priority can be changed only for Rule-Defined, Admin-Defined, and Active Directory Groups. System-Defined Group priority cannot be modified. In general, the Endpoint Group at the top of the list of Endpoint Groups has highest priority. The Endpoint Group at the bottom of the list has lowest priority.



Precedence Ranking

The System Defined Non-Persistent VDI Endpoint Group has the highest priority level, followed by the Persistent VDI Endpoint Group.

Order of priority:

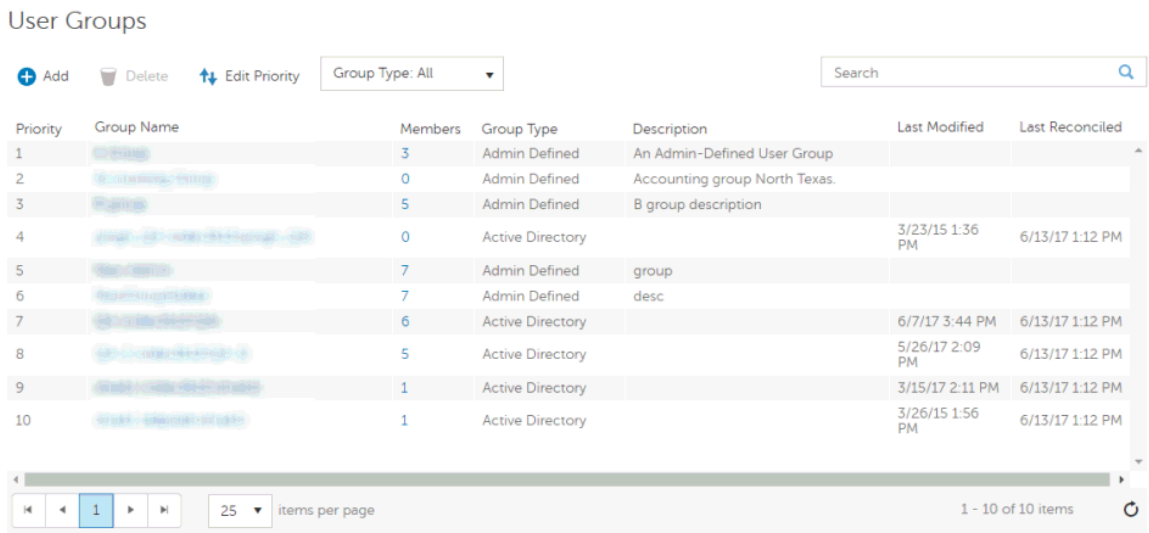
1. Non-Persistent VDI Endpoint Group
2. Persistent VDI Endpoint Group
3. Highest ranked Active Directory/Rule-Defined/Admin-Defined Endpoint Group
4. Second and subsequent highest ranked Active Directory/Rule-Defined/Admin-Defined Endpoint Groups
5. Opt-in Endpoint Group
6. Default Endpoint Group

To change Active Directory/Rule-Defined/Admin-Defined Endpoint Group priority:

1. In the left pane, click **Populations > Endpoint Groups**.
2. Click **Edit Priority**.
3. Select the row of the appropriate group and drag it to the location in the list of Endpoint Groups that reflects its new priority level.
4. Click **Save**.

Edit User Group Priority

The user group at the top of the list has highest priority. The user group at the bottom of the list has lowest priority.



To edit User Group priority:

1. In the left pane, click **Populations > User Groups**.
2. Click **Edit Priority**.
3. Select the row of the appropriate group and drag it to the location in the list of Endpoint Groups that reflects its new priority level.
4. Click **Save**.

View Endpoints in an Endpoint Group

This page displays the endpoints included in information for every user of the specified endpoint.

1. In the left pane, click **Populations > Endpoint Groups**.
2. Click a Group Name link or enter a filter to search for available Groups. The wildcard character (*) is supported.

   When you click a Group Name, the Endpoint Group Detail page displays.
3. If applicable, View or Modify Endpoint Information.

View or Modify Endpoint Group Policies and Information

1. In the left pane, click **Populations > Endpoint Groups**.
2. Click a Group Name or enter a filter to search for available Endpoint Groups. The wildcard character (*) is supported.

   When you click a Group Name, the Endpoint Group Detail page displays.
3. Click the tab that corresponds with the action to perform:

   Security Policies - To view or modify policies of the Group, click **Security Policies**.
   Note: Before modifying VDI Endpoint Group policies, see Policy Requirements for VDI Endpoint Groups.

Details & Actions - To view properties of the Group, click **Details & Actions**. Viewable information includes:

Group Name: Group1 (DOMAIN\Group1)

Description: The description provided when the Group was added.

(For Rule-Defined groups) Specification: The endpoint group specification that defines endpoints as members of the group.

PBA Device Control - The PBA Unlock command for this endpoint group is carried out in the PBA Device Control area. This command unlocks the PBA screen after it has been locked – either by sending a Lock command or by exceeding the maximum number of authentications attempts allowed by policy.

Members - To view or modify the information of an endpoint in the group, click **Members**. The list of endpoints in the group displays. Click an endpoint to view the endpoint's Security Policies, Details & Actions, Users, Endpoint Groups, Threat Events, and Advanced Events.

4. If modified, click **Save**.

Endpoint Group Details & Actions

This page lists the properties of the selected Endpoint Group.

1. In the left pane, click **Populations > Endpoint Groups**.
2. Search or select a Group Name, then the **Details & Actions** tab.

Details:

Group Name of the endpoint group

A description of this endpoint group

The specification that was used to create this endpoint group (applies only to Rule-Defined Groups)

Active Directory Group (applies only to Active Directory Groups)

PBA Device Control

The PBA Unlock command for this endpoint group is carried out in the PBA Device Control area. This command unlocks the PBA screen after it has been locked – either by sending a Lock command or by exceeding the maximum number of authentications attempts allowed by policy.

Endpoint Group Members

This page lists the endpoints within an endpoint group. Information displays based on the group specification used to create the endpoint group.

1. In the left pane, click **Populations > Endpoint Groups**.
2. Search or select a Group Name, then the **Members** tab.

Category - WINDOWS, MAC, SED

Hostname - Endpoint hostname

OS/Version - Endpoint operating system and version

Add Endpoints to an Admin-Defined Endpoint Group

1. In the left pane, click **Populations > Endpoint Groups**.
2. Select the group to which to add endpoints.
3. Click the **Members** tab.
4. Select **Add Endpoints to Group**, then search for specific endpoints or select endpoints in the list, and click **Add Selected Endpoints to Group**.

   OR

   Select **Upload Multiple Endpoints from File**, then click **Browse** to select a CSV file and click **Upload**.

Valid CSV requirements:

- The file must be in valid CSV format and contain a maximum of 999 endpoints.
- The first column must contain valid fully qualified hostnames. All columns except the first column are ignored.
- Only activated endpoints are added to the group.

Remove Endpoints from an Admin-Defined Endpoint Group

1. In the left pane, click **Populations > Endpoint Groups**.
2. Select the group in which to add endpoints.
3. Click the **Members** tab.
4. Search for specific endpoints or select endpoints in the list. To select more than one endpoint, press **Shift** and select the endpoints.
5. Click the red **X** in the right column for each endpoint, or select the endpoints and click **Remove Endpoints from Group**.

Endpoints

Endpoints

On the Endpoints page, you can add an endpoint to a group, remove an endpoint, or search and select an endpoint to View or Modify Endpoint Information. You can also quickly view the following summary information about each endpoint:

*Hostname - Endpoint hostname.

*OS/Version - Operating system and version running on the endpoint (Example: Microsoft Windows 10 Enterprise).

*Category - Catetory of endpoint (Example: Windows or Mac).

*Protected - A green check displays if the endpoint is protected. If the endpoint is not protected, the column is blank.

*Serial Number - Manufacturer assigned serial number.

*Win Computer Name - Computer name Windows uses to identify the computer on the network.

*Enabled Technologies - Security technologies enabled on the endpoint.

*Hardware ID - A unique identifier sent to the server from the client.

* Click the column header to sort by column label.

Click a hostname to view additional details about the endpoint. Click an arrow at the left of a hostname to view the Category, Unique ID, and Processor.

Add Endpoint to Group

To add an endpoint to an Endpoint Group:

1. In the left pane, click **Populations > Endpoints**.
2. Select the check box next to a hostname in the list or enter a filter to search for available endpoints. The wildcard character (*) is supported.

   For Windows and Mac, if you know the endpoint hostname, enter it in *Search*. Leave the field blank to display all Windows and Mac endpoints.
3. At the top left, click **Add Endpoints to Group**.

An endpoint is added to inventory when a user who is in the Dell Server database activates the endpoint.

If the user is not found in the Dell Server database, they is located in Active Directory.

Remove Endpoints

Endpoint removal is permanent. Once an endpoint is removed, the action cannot be undone.

To remove an endpoint:

1. In the left pane, click **Populations > Endpoints**.
2. Select the appropriate endpoint type, for example, **Workstation**.
3. Click the box next to a hostname in the list or enter a filter to search for available endpoints. The wildcard character (*) is supported.

   For Windows and Mac, if you know the hostname of the endpoint, enter it in *Search*. Leave the field blank to display all Windows and Mac endpoints.
4. At the top left, click **Remove**.
5. Click **OK** to confirm removal of the endpoint.

As another option, click an endpoint and select the **Details & Actions** tab. Under *Endpoint Detail*, click **Remove**.

Find Endpoints

1. In the left pane, click **Populations > Endpoints**.
2. Navigate the list of endpoints using the scroll bar or page navigation controls at the bottom of the page or enter a filter into *Search* to search for available endpoints. The wildcard character (*) is supported.

For Windows and Mac, if you know the endpoint hostname, enter it in *Search*. Leave the field blank to display all Windows and Mac endpoints.

View or Modify Endpoint Policies and Information

1. In the left pane, click **Populations > Endpoints**.

2. Select the appropriate endpoint type, for example, **Workstation**.
3. Click a hostname in the list or enter a filter to search for available endpoints. The wildcard character (*) is supported.

   For Windows and Mac, if you know the endpoint hostname, enter it in *Search*. Leave the field blank to display all Windows and Mac endpoints.

   Click a hostname or endpoint serial number to display the Endpoint Detail page.
4. Click the tab that corresponds with the action to perform:

   Security Policies - Click **Security Policies** to view or modify policies of the endpoint.

   Details & Actions - Click **Details & Actions** to view properties of the endpoint, including Inventory Information. Viewable information includes hardware information, effective policies, inventory and protection status, threat protection and Advanced Threat Prevention detail, and SED Device Control commands.

   Users - Click **Users** to view a list of users who store and access data on the endpoint. These statistics of users may be available on the Endpoint Detail page: login, last Gatekeeper sync, effective policies, and states. You can also recover data from this page.

   Endpoint Groups - Click **Endpoint Groups** to view a list of Endpoint Groups to which this endpoint belongs. All endpoint belong to at least one endpoint group, the Default Endpoint Group.

   Threat Events - Click **Threat Events** view information about threat events on the endpoint. The following information is displayed for events: severity, category (malware, web filtering, web protection, and firewall), event ID, event description, user name, and received.

   Advanced Threat Events - Click **Advanced Threat Events** view, export, quarantine, or waive unsafe files. Events are grouped by Status (unsafe, quarantined, or abnormal), and the following information is displayed for events: file name, file paths, score, classification, first found time stamp, running, auto run, and detected by.
5. If modified, click **Save**.

View Effective Policy

When you view Effective Policies, you are viewing the policies and settings that are enforced on an endpoint.

1. In the left pane, click **Populations > Endpoints**.
2. Click a hostname in the list or enter a filter to search for available endpoints. The wildcard character (*) is supported.

   For Windows and Mac, if you know the endpoint hostname, enter it in *Search*. Leave the field blank to display all Windows and Mac endpoints.

   Click a hostname or endpoint serial number to display the Endpoint Detail page.
3. On the Endpoint Detail page, click the **Details & Actions** tab.
4. Under *Manager Detail*, click **View Effective Policies**.

Related topics:

Manage Security Policies

Endpoint Details & Actions

The Details & Actions page lists the details for the selected endpoint as well as commands, such as Remove Endpoint. Available details and commands vary, depending on the endpoint platform.

To access Endpoint Details & Actions, follow these steps:

1. In the left pane, click **Populations > Endpoints**.
2. Search or select a hostname, then the **Details & Actions** tab.

Endpoint Detail

Command:

Remove - Endpoint is removed.

Endpoint removal is permanent. Once an endpoint is removed, the action cannot be undone.

Details:

Windows

Category - Windows

OS/Version - Example: Microsoft Windows 10 Enterprise

Processor

Serial Number - Manufacturer assigned serial number

Host ID - Endpoint identifier

Unique ID - Dell assigned unique identifier

Hardware ID - A unique identifier sent to the server from the client.

Protected - Date and time stamp

Mac

Category - Mac

OS/OS Version - Example: Mac OS X 10.11.0

Processor

Serial Number - Manufacturer assigned serial number

Host ID - Endpoint identifier

Unique ID - Dell assigned unique identifier

Hardware ID - A unique identifier sent to the server from the client.

Protected - Date and time stamp

Shield Detail

Commands:

To view the policies of the endpoint, click **View Effective Policies**.

Obtain the endpoint's recovery keys:

1. Click **Device Recovery Keys**.
2. Enter a Recovery Password and click **Download**.

The recovery bundle containing this endpoint's encryption keys is downloaded. You must remember the this recovery password to access the recovery keys.

Detail:

Windows

Policy Proxy Group (typically CMGREMOTE)

Recovery ID of the specific endpoint

Version (core/edition)

Activation Method (typically Mandatory)

HCA Enabled: True or False

TPM Present: True or False

Edition: Dell or CREDANT

States:

Policy Updating: Date and timestamp

Device Encryption Updating: Date and timestamp

Device Data Encryption On: Date and timestamp

Sweep Started: Date and timestamp

Sweep Completed: Date and timestamp

Inventory Received: Date and timestamp

Inventory Processed: Date and timestamp

Manager Inventory Received: Date and timestamp

Manager Inventory Processed: Date and timestamp

Protected:

- Protection Status Tab:
  - Disk Name
  - Capacity (storage)
  - Protection Status (Protected, Protecting, Unknown)
  - Interface type
  - Model number of the endpoint
- GPE Tab:
  - GPE Available (True or False)
  - GPE Driver Version
  - GPE Functional (True or False)
  - GPE Lifecycle Remaining (number)
  - GPE Lifecycle Owner Remaining (number)
  - GPE Provisioned Status

TPM Tab:

TPM Present (True or False)

TPM Activated (True or False)

TPM Owned (True or False)

TPM Functional Status (True or False)

TPM Spec Version (version number)

HCA Tab:

HCA Functional Status

HCA Provision State

Preboot Present (True or False)

Preboot Set (True or False)

Actions: Effective policies on the specific endpoint and Recovery Keys for the specific endpoint

---

Mac

Policy Proxy Group (typically CMGREMOTE)

Recovery ID of the specific endpoint

Version (core/edition)

Activation Method (typically Mandatory)

Edition (Dell or Credant)

States:

Policy Updating: Date and timestamp

Device Encryption Updating: Date and timestamp

Device Data Encryption On: Date and timestamp

Sweep Started: Date and timestamp

Sweep Completed: Date and timestamp

Inventory Received: Date and timestamp

Inventory Processed: Date and timestamp

Protected:

Protection Status Tab:

Disk Name

Capacity (storage)

Protection Status (Protected, Protecting, Unknown)

Interface type

Model number of the endpoint

Actions: Effective policies on the specific endpoint and Recovery Keys for the specific endpoint

---

Manager Detail (Windows only)

Command:

Click **View Effective Policies** to go to the effective policy page for this endpoint.

States

The client gathers the following information via a Windows Management Instrumentation (WMI) call to the Operating System. It is updated with each inventory update.

Inventory Received - the date and time that the inventory was received by the Dell Server and placed in the queue.

Inventory Processed - the date and time that the inventory was picked up from the queue and processed. (**Note**: If the Dell Server is under load, the Processed and Received times may be different, but usually they is the same.)

Agent Version - the version of Manager the endpoint is running.

Protected - the date and time that the device was protected.

Protection Status

Disk - number of the disk

Partitions - number of partitions the disk has

Capacity - capacity of the disk

Encryption Technology - encryption technology in use

Protection Status - Protected or unprotected

Interface - Disk interface (Examples: IDE, SATA)

Model - Manufacturer name and model of the disk

Click the small black arrow on the left to expand the disk details to view information for each partition of the disk.

Logical Disk - The name of the logical disk.

ID - The identifying number of the logical disk.

Encryption % - The percentage of the partition that has been encrypted.

Capacity - The capacity of the partition.

Protection Status - Protection status for the partition: Protected, Unprotected, Locked

Providers

Agent - SED, FDE, Authentication Proxy, Preboot Authentication, Windows Authentication, BitLocker, TPM, Threat Protection, Advanced Threat Prevention

Plugin Functional Status (green check mark or red "x") - This indicates whether the Agent has been enabled via policy. To get more detail on whether each plugin is working as expected, look at Plugin State column.

Plugin State:

- BitLocker Plugin:

Starting - Manager is starting up. Because this is a fairly quick process, it is unlikely an inventory update would capture this so you would probably never see this state in the Management Console.

Disabled - Manager is disabled by policy and not enforcing any previously received policy.

Active - Manager is running normally and enforcing policies.

No Policy - Initial policy has not been received so the plugin is not actively enforcing any policy. This is only relevant the very first time you install the Manager client. Manager does not start a plugin until an initial policy is received from the Dell Server, versus starting the plugin with some default policy placed on the client during install. After an initial policy has been received from the Dell Server, via the activation process, plugins are always started with the last policy the client is aware of.

OpSys Not Supported - Manager does not support this operating system. Manager is not actively enforcing policy related to this plugin, due to this plugin-specific exception.

- TPM Plugin:

Starting - Manager is starting up. Because this is a fairly quick process, it is unlikely an inventory update would capture this so you would probably never see this state in the Management Console.

Disabled - Manager is disabled by policy and not enforcing any previously received policy.

Active - Manager is running normally and enforcing policies.

TPM Services Not Started – In the Enterprise Server Console this is listed as *TPM Base Services Failed*. It means something is preventing the TPM service from starting as expected. The Manager is not actively enforcing policy related to this plugin, due to this plugin-specific exception.

No TPM Device – The TPM device is not present or is not detectable in the indicated computer. The Manager is not actively enforcing policy related to this plugin, due to this plugin-specific exception.

No Policy - Initial policy has not been received so the plugin is not actively enforcing any policy. This is only relevant the very first time you install the Manager client. Manager does not start a plugin until an initial policy is received from the Dell Server, versus starting the plugin with some default policy placed on the client during install. After an initial policy has been received from the Dell Server, via the activation process, plugins are always started with the last policy the client is aware of.

- SED Plugin:

Initialized - Manager is initialized waiting for delayed startup

Starting - Manager is starting up. Because this is a fairly quick process, it is unlikely an inventory update would capture this so you would probably never see this state in the Management Console.

Disabled - Manager is disabled by policy and not enforcing any previously received policy.

Active - Manager is running normally and enforcing policies.

No Policy - Initial policy has not been received so the plugin is not actively enforcing any policy. This is only relevant the very first time you install the Manager client. Manager does not start a plugin until an initial policy is received from the Dell Server, versus starting the plugin with some default policy placed on the client during install. After an initial policy has been received from the

Dell Server, via the activation process, plugins are always started with the last policy the client is aware of.

Waiting For Escrow - Manager is waiting for keys to escrow

Waiting For Server Public Key - Manager is waiting for public key to proceed with activation

No Opal Drive Present - Manager did not detect an OPAL drive

Plugin Version - The version of the plugin, which is taken from the plugin's version information

Vendor version - The version of the underlying framework. For example, BitLocker is Microsoft's technology, therefore Vendor Version is Microsoft's version for BitLocker.

Threat Protection Detail (Windows only)

Scan Engine Version - Lists the version of the engine that performed the last scan.

DAT File Version - Lists the version of the DAT file.

Last Scan Started - Date/time stamp that the last scan was started.

Last Scan Completed - Date/time stamp that the last scan was completed.

Advanced Threat Prevention Detail

Device ID - Lists the identifier of the device as it pertains to Advanced Threat Prevention.

Agent Version - Lists the version of the agent.

Update Date - Date/time stamp that the agent was updated.

Provisioned Date - Date/time stamp that the client was provisioned.

FDE Device Control (Windows only)

Current State of the Endpoint - Unlocked or Locked

Commands:

PBA commands for a specific endpoint are carried out in the PBA Device Control area. Each command has a priority ranking. A command with a higher priority rank cancels commands of lower priorities in the enforcement queue. For a list of command priority rankings, see Priority of Commands for Self-Encrypting Drives.

Lock - Locks the PBA screen and prevents any user from logging into the computer.

Unlock - Unlocks the PBA screen after it has been locked on this endpoint, either by sending a Lock command or by exceeding the maximum number of authentications attempts allowed by policy.

Remove Users - Removes all users from the PBA.

Bypass Login - Bypasses the PBA screen one time to allow a user into the computer without authenticating. The user will still need to login to Windows after PBA has been bypassed.

Wipe - The Wipe command functions as a “restore to factory state” for the FDE drive. The Wipe command can be used to re-purpose a computer or, in an emergency situation, wipe the computer, making the data permanently unrecoverable. When the wipe command is consumed by the client, all history and details about this endpoint are removed from the Dell Server. Ensure that this is the desired behavior before invoking this command.

The FDE Device Control Table

The table lists the commands most recently sent to the PBA Device.

To sort the table, click a column header.

PBA Device Control (Windows only)

Current State of the Endpoint - Unlocked or Locked

Commands:

PBA commands for a specific endpoint are carried out in the PBA Device Control area. Each command has a priority ranking. A command with a higher priority rank cancels commands of lower priorities in the enforcement queue. For a list of command priority rankings, see Priority of Commands for Self-Encrypting Drives.

Lock - Locks the PBA screen and prevents any user from logging into the computer.

Unlock - Unlocks the PBA screen after it has been locked on this endpoint, either by sending a Lock command or by exceeding the maximum number of authentications attempts allowed by policy.

Remove Users - Removes all users from the PBA.

Bypass Login - Bypasses the PBA screen one time to allow a user into the computer without authenticating. The user will still need to login to Windows after PBA has been bypassed.

Wipe - The Wipe command functions as a “restore to factory state” for the SED drive. The Wipe command can be used to re-purpose a computer or, in an emergency situation, wipe the computer, making the data permanently unrecoverable. When the wipe command is consumed by the client, all history and details about this endpoint are removed from the Dell Server. Ensure that this is the desired behavior before invoking this command.

The PBA Device Control

Lists the commands most recently sent to the PBA device.

To sort, click a column header.

Protected Status

Protected status is indicated if any of the following criteria are met:

- Advanced Threat Prevention is installed and enabled.
- Self-Encrypting Drive Management is installed, enabled, and the PBA is enabled.
- BitLocker Manager is installed, enabled, and encryption has completed.
- Dell Encryption (Mac) is installed and enabled, and policy-based encryption has been enforced.
- Dell Encryption (Windows) is installed, enabled, Policy-Based Encryption has been set for the endpoint, and the most recent policy has been applied for the last logged on user.

To check Protected Status of an endpoint:

1. In the left pane, click **Populations > Endpoints**.
2. Click a hostname in the list or enter a filter to search for available endpoints. The wildcard character (*) is supported.

   For Windows and Mac, if you know the endpoint hostname, enter it in the *Search* field. Leave the field blank to display all Windows and Mac endpoints.

   Click a hostname or endpoint serial number to display the Endpoint Detail page.
3. A green check mark displays in the Protected column if any of the criteria for Protected status are met.

Endpoint Users

This page displays information for every user of the specified endpoint. The user information differs for each technology group or policy category.

1. In the left pane, click **Populations > Endpoints**.
2. Search or select a hostname, then the **Users** tab.

Shield

User - Each user on the specific endpoint

Last Successful Login - Date/time stamp, per user

Last Unsuccessful Login - Date/time stamp, per user

Last Gatekeeper Sync - Date/time stamp, per user

Effective Policies - Click **view** for a simple layout view of the effective user policies

Actions - Click **Recover** to proceed to the Recover Data page

Last Encryption Sweep Start - Date/time stamp, per user

Sweep End - Date/time stamp, per user

Encryption Failure - Click **view** for a simple list of files that could not be encrypted, per user

States (Date/time stamp, per user):

Policy Updating

User Encryption Profile Updating

EMS Encryption Profile Updating

User Data Encryption On

EMS Data Encryption On

Deactivation Pending

Suspension Pending

Suspended

Endpoint Threat Events

This page lists information on threat events for the selected endpoint.

1. In the left pane, click **Populations > Endpoints > Workstation**.
2. Search or select a Hostname, then the **Threat Events** tab.

Threat Event Data

Severity - Severity of the threat, where Critical is the most dangerous threat to the endpoint, and Information is just a notification of an event that is unlikely to harm the endpoint. (Critical, Major, Minor, Caution, Information)

Category - Category of the threat. Upon identification, threats are sorted into these categories: Malware, Web Filtering, Web Protection, and Firewall.

Event ID - Unique number assigned to each threat event.

Description - Description of the last preventative action taken to handle the threat.

User Name - The DOMAIN\Username associated with the endpoint where the threat was identified.

Received - Date/time stamp when the last action was taken to handle a threat.

Navigate the Threat Event Data

To sort the data, click a column header.

Use the controls at the bottom of the page to:

- Advance to the top of the data.
- Go back one page.
- Go forward one page.
- Advance to the end of the data.
- Increase or reduce the items per page.
- View the range of items currently displayed.
- Refresh the data.

Endpoint Advanced Threats

This page allows you to view, export, quarantine, or waive unsafe files that trigger events on the selected endpoint.

An event is not necessarily a threat. An event is generated when a recognized file or program is quarantined, safe listed, or waived. Threats are a category of events that are newly detected as potentially unsafe files or programs and require guided remediation.

1. In the left pane, click **Populations > Endpoints**.
2. Search or select a hostname, then the **Advanced Events** tab.

List of Events

The list presents all files that have triggered events found on this device.

Columns

- Icon - An icon displays in this column, when available.
- Name - File triggering the event.
- File Paths - The location of the file on the device.
- Cylance Score - A score is assigned to each file that is deemed Abnormal or Unsafe. The score represents the confidence level that the file is malware. The higher the number, the greater the confidence.
- Status - Indicates whether the file has been quarantined or waived.
- Classification - Classification of the threat: High, Medium, or Low. For details, see Advanced Threat Protection Classifications.
- First Found - Date/timestamp that the file was first found.
- Running - Indicates whether the file that triggered the event is running or not.

- Auto Run - Indicates whether the file was set to automatically run upon startup.
- Detected By - Indicates whether the file was detected by Execution Control or by Memory Protection.

Configure the Threat List

Add or Remove Columns

Click an arrow next to any column header and select **Columns** to add columns to, or remove columns from, the table.

Filter on Column Data

To filter the list based on column data, click the down-arrow on any column to display the context menu, and select **Filter**.

The filter options vary, depending on the type of data in the column. For example, you may want to filter the list so that it shows only high priority threats.

Group by a Column

Drag a column header, such as Status, to the area directly above the column headers to group the data by Status. When you drag a column header, it turns green, indicating that the table can be grouped by that data. You can drag additional headers over the table to group the data even further.

For each group, a number displays in parentheses to indicate the total number of threats that share that group's attribute.

Commands:

Select the check box next to a file name to perform an action on the file. To select all files, select the check box in the column heading row.

Export lets you export selected data to a .CSV file so that you can view the data in Excel or a similar application which has powerful sorting/organizing features.

After selecting the data to export, click **Export** to save the data in a .CSV file.

Click **Quarantine** to add the file to the Quarantine list.

Quarantining a file will prevent the file from being executed on this device.

Note: Quarantining a file will move the file from its original location to the Quarantine directory (C:\ProgramData\Cylance\Desktop\q).

Click **Waive** to allow the file to run on this device.

Note: Occasionally, a “good” file could be quarantined or reported. This could happen if the features of that file strongly resemble those of malicious files. Waiving or globally safe listing the file can be useful in these instances.

Exploit Attempts

This section lists the detection of attempts to exploit running processes, or malware that executes from within memory space.

A number displays the total number of events, followed by the number in each subcategory.

Check box - Select all events by selecting the check box in the column heading row, or select individual events. When you select a check box, Quarantine and Waive are activated.

Added - Date and time when the exploit attempt was added.

Process Name - Name of the process identified as an exploit attempt.

Process ID - Unique number associated with the exploit attempt.

Type - Type of memory exploit: Exploitation, Process Injection, Escalation.

Action - Action taken to protect the system from the exploit attempt:

- Ignore - The agent does not take any action against identified memory violations.
- Alert - The agent will record the violation and list the incident on this page.
- Block - If an application attempts to call a memory violation process, the agent will block the process call. The application that made the call is allowed to continue to run.
- Terminate - If an application attempts to call a memory violation process, the agent will block the process call and will also terminate the application that made the call.

User Name - Name of the user who was logged in when the exploit attempt was identified.

Endpoint Advanced Threat Events

The Advanced Threat Events tab displays if the Advanced Threat Prevention service is provisioned and Advanced Threat Prevention is enabled on the endpoint.

The tab displays information about events for the endpoint based on information available in the Dell Server.

To access the Enterprise Advanced Threats tab, follow these steps:

1. In the left pane, click **Populations > Endpoints**.
2. Search or select a hostname, then the **Advanced Threat Events** tab.

Use the following filters to select content to display on the Advanced Threat Events tab:

Type - Threat Found, Threat Blocked, Threat Terminated, Memory Violation Blocked, Memory Violation Terminated, Memory Violation (Detected), Threat Removed, Threat Quarantined, Threat Waived, Threat Changed, Protection Status Changed.

Severity - Severity level of the event: Critical, Major, Minor, Caution, or Informational.

Timeframe (in days) - 1, 7, 14, 30, 60, 90

Columns - Allows you to select the following additional columns to display:

Hostname - The fully qualified name of the computer

Data - Details about the event

Created - Date and time that the event was captured

Machine Name - Name of the computer on which the threat event was detected

Path - Path to the file in which the threat was detected

Sha256 - The file's 256-character Secure Hash Algorithm can be compared with an expected result to indicate whether the file has been tampered with.

Score - The threat file's score, indicating the confidence level that the file is malware. The higher the number, the greater the confidence.

Server Encryption Clients

Suspend an Encrypted Server

When you suspend an encrypted server, you suspend the user associated with the encryption client rather than an individual user who logs on to the endpoint.

To suspend a Server Encryption client:

1. In the left pane, click **Populations > Users**.
2. In *Search*, enter **SERVER-USER** and click the  .
3. Click the user name of the appropriate user.
4. On the User Detail page, click the **Endpoints** tab.
5. Click the Device ID of the appropriate endpoint.
6. On the Endpoint Detail page, click the **Details & Action** tab.
7. In Server Device Control, click **Suspend**.

Suspension takes effect the next time the endpoint is rebooted.

To reinstate an encrypted server, follow the instructions in Reinstate a Suspended Server Encryption Client.

Reinstate an Encrypted Server

To reinstate an encrypted server, follow these steps:

1. In the left pane, click **Populations > Users**.
2. In *Search*, enter **SERVER-USER** and click  .
3. Click the user name of the appropriate user.
4. On the User Detail page, click the **Endpoints** tab.
5. Click the Device ID of the appropriate endpoint.
6. On the Endpoint Detail page, click the **Details & Action** tab.
7. In Server Device Control, click **Reinstate**.

Reinstatement takes effect the next time the endpoint is rebooted.

Commands for Self-Encrypting Drives

Priority of Commands for Self-Encrypting Drives

Each command for self-encrypting drives has a priority ranking. A command with a higher priority rank cancels commands of lower priorities in the enforcement queue.

Priority rankings (1 is highest):

1. Wipe
2. Lock
3. Remove Users
4. Unlock
5. Bypass

For example, a Wipe command cancels a Lock command that was previously queued to send to the endpoint.

Related topics:

Send Wipe Command to Self-Encrypting Drive

Lock a Self-Encrypting Drive

Remove Users from Endpoint with Self-Encrypting Drive

Unlock a Self-Encrypting Drive

Allow PBA Login Bypass

Allow PBA Login Bypass

You can allow users to bypass the Preboot Authentication (PBA) screen one time to allow a user into the computer without authenticating on an endpoint equipped with a self-encrypting drive.

To send the Bypass Login command, follow these steps:

1. In the left pane, click **Populations > Endpoints**.
2. Select the Workstation Endpoint Type.
3. If you know the full endpoint hostname, enter it in *Search*. Leave the field blank to display all Workstation endpoints.
4. Click . An endpoint or list of endpoints displays, based on your search filter.
5. Click the endpoint hostname on which to allow PBA login bypass.
6. Click the **Details & Actions** tab.
7. Under *SED Device Control*, click **Bypass Login**.
8. Click **Yes** to confirm that you want to send the Bypass Login command to the endpoint.

Unlock a Self-Encrypting Drive

You can unlock the PBA screen after it has been locked on this endpoint, either by sending a Lock command or by exceeding the maximum number of authentications attempts allowed by policy.

To send the Unlock command, follow these steps:

1. In the left pane, click **Populations > Endpoints**.
2. Select the **Workstation** endpoint type.

3. If you know the full endpoint hostname, enter it in *Search*. Leave the field blank to display all Workstation endpoints.
4. Click . An endpoint or list of endpoints displays, based on your search filter.
5. Click the endpoint hostname with the self-encrypting drive to unlock.
6. Click the **Details & Actions** tab.
7. Under *SED Device Control*, click **Unlock**.
8. Click **Yes** to confirm that you want to send the Unlock command to the endpoint.

Remove Users from Endpoint with Self-Encrypting Drive

To remove users from the PBA, follow these steps:

1. In the left pane, click **Populations > Endpoints**.
2. Select the **Workstation** endpoint type.
3. If you know the full Hostname of the endpoint, enter it in the *Search* field. However, you may leave the field blank to display all Workstation endpoints.
4. Click the search icon.

   An endpoint or list of endpoints displays, based on your search filter.
5. Click the Hostname of the endpoint from which to remove users.
6. Click the **Details & Actions** tab.
7. Under SED Device Control, click **Remove Users**.
8. Click **Yes** to confirm that you want to send the Remove Users command to the endpoint.

Lock a Self-Encrypting Drive

To lock the PBA screen and prevent any user from logging onto the computer, follow these steps:

1. In the left pane, click **Populations > Endpoints**.
2. Select the Workstation Endpoint Type.
3. If you know the full endpoint hostname, enter it in *Search*. Leave the field blank to display all Workstation endpoints.
4. Click . An endpoint or list of endpoints displays, based on your search filter.
5. Click the endpoint hostname with the self-encrypting drive to lock.
6. Click the **Details & Actions** tab.
7. Under *SED Device Control*, click **Lock**.
8. Click **Yes** to confirm that you want to send the Lock command to the endpoint.

Send Wipe Command to Self-Encrypting Drive

CAUTION: The Wipe command clears all data from the disk and cannot be undone.

The Wipe command functions as a “restore to factory state” for the self-encrypting drive. In an emergency situation, wipe the computer, making the data permanently unrecoverable. When the wipe command is consumed, all history and details about this endpoint are removed. Ensure that this is the desired behavior before invoking this command.

To send the Wipe command, follow these steps:

1. In the left pane, click **Populations > Endpoints**.
2. Select the Workstation Endpoint Type.
3. If you know the full endpoint hostname, enter it in *Search*. Leave the field blank to display all Workstation endpoints.
4. Click . An endpoint or list of endpoints displays, based on your search filter.
5. Click the endpoint hostname on which to wipe the self-encrypting drive.
6. Click the **Details & Actions** tab.
7. Under *SED Device Control*, click **Wipe**.
8. Click **Yes** to confirm that you want to send the Wipe command to the endpoint.

Set the Dell Server Connection Retry Interval

To set the interval that the Manager client attempts to contact the Dell Server when it is unavailable to communicate with the Manager client, set the following value on the client computer:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\DellMgmtAgent\Parameters

CommErrorSleepSecs (DWORD Value)=300

This value is the number of seconds the Manager client waits to attempt to contact the Dell Server if it is unavailable to communicate with the Manager client. The default is 300 seconds (5 minutes).

Administrators

Assign or Modify Administrator Roles

View or modify existing administrator privileges.

1. In the left pane, click **Populations > Administrators**.
2. Search or select the row that displays the user name of the appropriate administrator to display User Detail.
3. View or modify administrator roles in the pane at the right.
4. Click **Save**.

Dell recommends assigning administrator roles at the Group level rather than at the User level.

1. In the left pane, click **Populations > User Groups**.
2. Search or select a group name, then the **Admin** tab.
3. Select or deselect administrator roles assigned to the group.
4. Click **Save**.

If you remove a group that has administrative privileges and later re-add the group, it remains an administrator group.

To view, assign, or modify administrator roles at the User level, see User Admin.

Related topics:

Administrator Roles

User Admin

Delegate Administrator Roles

Administrator Roles

Administrator login is integrated with Active Directory to simplify the process of managing administrators and to allow you to leverage your existing user authentication infrastructure. Administrators are assigned roles that define what level of access each administrator is allowed. For example, some administrators may only be allowed to implement help desk assisted recovery while others have full access to edit security policies. You can assign administrator roles to Active Directory groups so you can easily change the level of administrator access users have with a simple change to AD group membership. Non-domain users can be granted reporting-only access via Compliance Reporter.

There are 11 types of administrators. Distributed administration is key to the secure administration of your environment. It allows you to divide roles appropriately among your administrators and ensures the proper level of privileges are assigned to each administrator. A single administrator can have privileges of more than one administrator type. However, it is recommended to have a maximum of one super administrator (an administrator who has privileges of all administrator types).

The following table shows the tasks each administrator can perform in the Management Console or Compliance Reporter.

Task	Performed by Type of Administrator							
	Help Desk	System	Security	Log	Account	Forensic[1]	Policy[2]	Repo
Log in	•	•	•	•	•			•
Log out	•	•	•	•	•			•
View current system state	•	•	•		•			
Search for Users, Groups, and Endpoints	•	•	•		•			
Add Users and Groups		•	•		•			
Browse Domains	•	•	•		•			
Add and edit Domains		•	•					
Upload licenses		•						
Recover an endpoint - Authentication Failure	•		•					

Remove an endpoint		•	•					
Change Dell Server Options		•	•					
Suspend a User			•					
Reinstate suspended user			•					
Deactivate a User			•					
View policies		•	•				•	
Modify policies		•	•				•	
Commit policies		•	•				•	
Issue commands			•					
Analyze logs		•	•	•				
View Administrators					•			
Create, change, and delete Administrator accounts					•			
Delegate Administrator privileges					•			
Download Endpoint software	•	•	•				•	
Download recovery key bundle	•		•					
Provision or recover the Advanced Threat Prevention service		•						
Enroll for Advanced Threat Prevention auto updates		•						
Set email notifications of Client Access Licenses, Threat Protection, and Advanced Threat		•	•					

Prevention alerts								
Log in to Compliance Reporter		•	•					•
Manage report folders and modify/save Compliance Reporter report layouts		•	•					•
Access the Compliance Reporter reports window		•	•					•
Work with Compliance Reporter report views and generate reports		•	•					•
Access the Compliance Reporter report administrator window		•	•					•
Create, manage, schedule, and make Compliance Reporter report layouts available to report users		•	•					•
Specify the data source for Compliance Reporter and Manage Reports		•	•					•
Manage Compliance Reporter and Manage Reports user privileges		•	•					•
Edit or delete a report that is set to run at a specified interval in the Compliance Reporter Scheduler and Manage Reports		•	•					•

Schedule and rename a report that is set to run at a specified interval in the Compliance Reporter Scheduler and Manage Reports		•	•					•
Enter or modify settings in Compliance Reporter and Manage Reports Settings		•	•					•
Set up Compliance Reporter plug-ins		•	•					•
Open a Report, modify an online Report display, and rename a Report view in Compliance Reporter Manage Reports		•	•					•
Generate, export, store, print, and email a Report result in Compliance Reporter and Manage Reports		•	•					•
Add, edit, and delete a Compliance Reporter Report folder		•	•					•
Access the Manage Reports Tab		•	•					•

1 The forensic administrator role provides the rights to use the forensic administrator tools via XAPI.

[2] The policy administrator role is reserved for future use.

Delegate Administrator Rights

Administrator rights for a user group can be delegated to a user. The delegated administrator and users must be members of the user group not only in Active Directory but in the Dell Server database. Administrator rights are available to the delegated administrator only if the delegated administrator is a

member of the user group in the Dell Server database. Delegated administrator rights are effective only with regard to Users who are members of the user group in the Dell Server database.

Only the superadmin and account administrator can delegate administrator rights.

To delegate Administrator rights, follow these steps:

1. In the left pane, click **Populations > User Groups**.
2. Search for the appropriate group.
3. Click the **Admin** tab.
4. Under *Delegated Roles*, click **Add**.
5. Search for and select the user to receive administrator rights, then click **Add**.

To remove delegated administrator rights, under *Delegated Roles* in User Group Detail, locate the user to remove as delegated administrator and click the red **X** next to the user name.

Reporting

Manage Reports

Manage Reports

In the left pane, click **Reports > Manage Reports**. For compliance and monitoring purposes, you can:

- Manage reports
- View or modify an existing report
- Create a new report

The Manage Reports page has:

- **New Report** - See Create a new report.
- **Report Type** - Select **All** (default) or specific report types to display in the Name column. **Clear selected items** to undo selections. See Report Type.

Note: Policy-based reports are not an option.

- **Grouping** - Group by **Report Type**, **Author**, **Private**, or **None** (default).
- **Columns** - Select which columns to display on the Manage Reports page, such as Name, Description, Report Type, Author. Also:
    - **Private - True** indicates only the owner of the report can access it.
        - Report Administrator - can view all public and private reports.
        - Other Administrators - can view private reports they created and all public reports.
    - **Created** - Date the report was created.
    - **Modified** - Date the report was modified.
- **Search** - Hover to view columns for performing a search, then enter specific text for those columns. Use * for a wildcard. For additional filtering to provide a detailed search on a specific report, see Use_Search_and_More_to_filter.

View or Modify an Existing Report

On the Manage Reports page, select a report from the Name column to view an instance of that report. The owner can make the report private or public. See View Report.

Create a New Report

On the Manage Reports page, click **Create New Report** and select an option. An instance of that report opens to customize the information to display. See View Report.

View Report

On the Manage Reports page, select an option in **Create New Report** or click an existing report in the **Name** column.

- New report - An administrator can select **Save As**. Save, Rename, and Delete options are activated, and the report is saved to the Manage Reports page. The owner can make the report private or public. You can create:
    - Single reports
    - Report templates - Determine frequent report content that you will generate. Select Column and Grouping options that are common to all those reports and save it as a template. See View_or_modify_an_existing_report.
- Existing report:
    - To filter a report, perform a query using ***Search*** and ***More.***
    - Owner of a report - Can view their private reports and all public ones. Only the Owner or a Report administrator can modify or rename the report.
    - Report administrator - Can view all private and public reports. Can modify or rename public and private reports.
    - Public reports - Any administrator can select **Save As** to modify a copy of the report.

Grouping, Columns, and More differ for each report type. Some Column and Grouping options are selected by default.

- **Columns** allows customized options to display. After you select options, you can drag and resequence to avoid scrolling. The resequenced columns return to the default when you close the report.
- **Grouping** allows you to sort the column options you selected.
- Hover over *Search* to view suggested columns for performing a search, then enter specific text. Suggested column options differ for each report type. Use (*) as a wildcard.

For a description of each report's Column and Grouping options, click a link below.

Report Type	Description and link
Device Detail	Provides reports based on Windows or, Mac details. See Endpoint Details & Actions.
Shield Detail	Customize a report of an endpoint's policies, recovery keys, or details. See Shield Detail.
Notifications	Customize a report of news, alerts, and events or email notifications. See Notifications.
Log Analyzer	Customize a report of policy modifications or logs based on message

	priority level, date and time periods, and occurrences of usernames and hosts. See Log Analyzer.
ATP Event	Provides reports of events for the entire enterprise based on information available in the Dell Server. See Advanced Threat Events tab filters.
EMS Event	Provides data about events that occur when removable media is used.
BitLocker Manager	Customize a report to see if BitLocker is enabled and to view details. See Manager Detail (Windows only).
Windows Encryption Failures	Provides a report on files that were not encrypted on a Windows Encryption client. See Endpoints and Endpoint Details & Actions.
Windows Shield User Encryption Status	For Windows, provides a report more focused on the user and a device, for example if one device has multiple users. See Protected Status.

Query using Search and More... to filter

Search performs a text-only quick search across multiple fields and may return numerous results.

- Hover to view columns that apply to this search, then enter specific text for those columns.
- Use * for a wildcard.

To filter and narrow the search with *More...* :

- Select **More...** and select a check box. Check boxes differ for each report type. Select one or multiple check boxes to narrow the search.
- An additional field displays for that check box option where you can either enter text to search on that column or select from a list of enumerators or a data type for that column.

Query example for Log Analyzer report

1. In Columns, select options. From menu options such as, **Priority** and **Category** select enumerators. **Created** allows you to filter by date.
2. Enter text in *Search* to perform a quick search on *Username* and *Message*.
3. For additional filtering, select **More....** and then select **Username**, **Message**, or both. Additional text fields allow you to limit the text search specifically to that column.

Query example for BitLocker Manager report

1. In Columns, select options.
2. Enter text in *Search* to perform a quick search on *Registered User*.
3. For additional filtering, select **More....** and then select one or more options. Additional text fields allow you to limit the text search to that column:
    - Registered User - Enter text to search specifically on that column.
    - BitLocker Enabled or TPM Enabled - Boolean search specifically on those columns.
    - Disk Status and Logical Disk Status - Enumerator searches specifically on those columns.

Export File

Export to Excel or a .csv file.

Add Schedule

To add an email schedule for a report:

1. In the left pane of the Management Console, click **Reporting > Manage Reports**.
2. In Columns, click a report name then click **Schedule**.
3. In *Schedules*, click **Add Schedule**.
4. In *Add Schedule*, set the following parameters:
    - Email - add a single or multiple addresses separated by commas
    - Schedule - select one of the following:
        - Every Day
        - Days of Week **-** select a specific weekday or multiple weekdays
        - Day of Month - select a day of the month
    - Time - select a time of day
    - Locale - select a language
5. Click **Save**.

Compliance Reporter

Compliance Reporter has its own help system. When Compliance Reporter launches, click the Help link on the top menu.

To launch Compliance Reporter:

1. In the left pane of the Management Console, click **Compliance Reporter**.
2. When Compliance Reporter launches, log in with superadmin credentials or reporting credentials.

Export Events to a SIEM/Syslog Server

Integrating with a SIEM/syslog server allows administrators to run customized analytics on threat and audit data within their environments. The Dell Server supports the export of Advanced Threat Prevention events.

To export audit events to a syslog server or to a local file:

1. In the left pane, click **Management > Services Management**.
2. Select the **Events Management** tab.
3. Select the appropriate option(s):

Export to Local File allows export of audit events to a file. Enter the location in which to store the file. This option also provides a backup of the audit events database.

Export to Syslog allows specification of the syslog server to which to export the file. If TCP protocol is not selected, select it.

4. Click **Save Preferences**.

Export Audit Events with TLS/SSL over TCP

To use TLS/SSL,the syslog server must be configured to listen for TLS/SSL messages. The root certificate used for the syslog server configuration must be added to the Dell Server Java keystore.

The following example shows necessary configurations for a Splunk server with default certificates. Configurations are specific to individual environments. Property values vary when using non-default certificates.

1. Configure the Splunk server to use the Splunk server certificate and root certificate to listen on TCP for TLS/SSL messages:

   $SPLUNK_HOME\etc\system\local\inputs.conf

   [tcp-ssl:<port number>]

   disabled = 0

   [SSL]

   serverCert = $SPLUNK_HOME\etc\auth\server.pem

   sslPassword = <password>

   requireClientCert = false

   $SPLUNK_HOME\etc\system\local\server.conf

   [sslConfig]

   sslRootCAPath = $SPLUNK_HOME\etc\auth\cacert.pem

   sslPassword = <password>

2. Restart the Splunk server.

   After the restart, **splunkd.log** will have entries similar to the following:

   07-10-2017 16:27:02.646 -0500 INFO TcpInputConfig - IPv4 port 5540 is reserved for raw input (SSL)

   07-10-2017 16:27:02.646 -0500 INFO TcpInputConfig - IPv4 port 5540 will negotiate new-s2s protocol

   07-10-2017 16:27:02.653 -0500 INFO TcpInputConfig - IPv4 port 5540 is reserved for raw input (SSL)

   07-10-2017 16:27:02.653 -0500 INFO TcpInputConfig - IPv4 port 5540 will negotiate new-s2s protocol

   07-10-2017 16:27:02.653 -0500 INFO TcpInputConfig - IPv4 port 9997 is reserved for splunk 2 splunk

   07-10-2017 16:27:02.653 -0500 INFO TcpInputConfig - IPv4 port 9997 will negotiate new-s2s protocol

   07-10-2017 16:27:02.653 -0500 INFO TcpInputProc - Creating raw Acceptor for IPv4 port 5540 with SSL

   07-10-2017 16:27:02.653 -0500 INFO TcpInputProc - Creating raw Acceptor for IPv4 port 5541 with Non-SSL

   07-10-2017 16:27:02.654 -0500 INFO TcpInputProc - Creating fwd data Acceptor for IPv4 port 9997 with Non-SSL

3. Configure the Dell Server to communicate with the Splunk server and export audit events.

Use the keytool command to add the Splunk server's root certificate (cacert.pem) to the Dell Server operating system Java keystore. The certificate is added to the operating system Java keystore and not to the Dell Server application Java keystore.

keytool -keystore <keystore_location> -alias <alias-name> -importcert -file <certificate_file>

Add the Splunk server's root certificate (cacert.pem) to **/etc/ssl/certs/java/cacerts** and restart the Security Management Server Virtual.

4. Modify the Dell Server database to change the SSL value from **false** to **true**:

   In the database, navigate to the information table, SIEM-specific support configuration.

   Change the "SSL":"false" value to "SSL":"true" – for example:

   {"eventsExport":{"exportToLocalFile":{"enabled":"false","fileLocation":"./logs/siem/audit-export.log"},"exportToSyslog":{"enabled":"true","protocol":"TCP","SSL":"true","host":"yourDellServer.yourdomain.com","port":"5540"}}}

Advanced Threat Prevention Syslog Event Types

Following are event types that are supported with the Syslog/SIEM Advanced Threats option.

Application Control

This option is visible when the Application Control feature is enabled. Application Control events represent actions occurring when the device is in Application Control mode. Selecting this option sends a message to the Syslog server whenever an attempt is made to modify or copy an executable file, or when an attempt is made to execute a file from an external device or network location.

Example Message for Deny PE File Change:

```
CylancePROTECT: Event Type: AppControl, Event Name: pechange, Device Name: WIN-
7entSh64, IP Address: (192.168.119.128), Action: PEFileChange, Action Type: Deny,
File Path: C:\Users\admin\AppData\Local\Temp\MyInstaller.exe, SHA256:
04D4DC02D96673ECA9050FE7201044FDB380E3CFE0D727E93DB35A709B45EDAA
```

Example Message for Deny Execution from External Drive:

```
CylancePROTECT: Event Type: AppControl, Event Name: executionfromexternaldrives,
Device Name: WIN-7entSh64, IP Address: (192.168.119.128), Action: PEFileChange,
Action Type: Allow, File Path: \\shared1\psexec.exe, SHA256:
F8DBABDFA03068130C277CE49C60E35C029FF29D9E3C74C362521F3FB02670D5
```

Devices

Select this option to send device events to the Syslog server.

- When a new device is registered, two messages for this event are received: Registration and SystemSecurity.

  Example Message for Device Registered Event:

```
Event Type: Device, Event Name: Registration, Device Name: WIN-55NATVQHBUU

Event Type: Device, Event Name: SystemSecurity, Device Name: WIN-
55NATVQHBUU, Agent Version: 1.1.1270.58, IP Address: (10.3.0.154), MAC Address:
(005056881877), Logged On Users: (WIN-55NATVQHBUU\Administrator), OS: Microsoft
Windows Server 2008 R2 Standard Service Pack 1 x64 6.1.7601
```

- When a device is removed.

  Example Message for Device Removed Event:

```
Event Type: Device, Event Name: Device Removed, Device Names: (
), User: (
)
```

- When a device's policy or logging level has changed.

  Example Message for Device Updated Event:

```
Event Type: Device, Event Name: Device Updated, Device Message:
Renamed: 'WIN-55NATVQHBUU' to 'WIN-2008R2-IRV1'; Policy Changed: 'Default' to
'IRVPolicy1';
```

Memory Protection

Selecting this option logs any Memory Exploit Attempts that might be considered an attack from any of the Tenant's devices to the Syslog server.

There are four types of Memory Exploit actions:

- **None:** Allowed because no policy has been defined for this violation.
- **Allowed:** Allowed by policy.
- **Blocked:** Blocked from running by policy.
- **Terminated:** Process has been terminated.

Example Message of Memory Protection Event:

```
Cyl CylancePROTECT: Event Type: ExploitAttempt, Event Name: blocked, Device Name:
WIN-7entSh64, IP Address: (192.168.119.128), Action: Blocked, Process ID: 3804,
Process Name: C:\AttackTest64.exe, User Name: admin, Violation Type: LSASS Read
```

Script Control

Selecting this option logs any newly found scripts that have been blocked or have triggered an alert to the Syslog server.

Syslog Script Control events contain the following properties:

- **Alert:** The script is allowed to run. A script control event is sent to the Dell Server.
- **Block:** The script is not allowed to run. A script control event is sent to the Dell Server.

Example Message of Script Control

```
CylancePROTECT - - - Event Type: ScriptControl, Event Name: Blocked, Device Name:
Fake_Device, File Path: d:\windows\system32\windowspowershell\v2.1\newlyMade.vbs,
Interpreter: active, Interpreter Version: 6.1.7600.16385 (win7_rtm.090713-1255)
```

Threats

Select this option to log any newly found threats or changes observed for any existing threat, to the Syslog server. Changes include a threat being Removed, Quarantined, Waived, or Executed.

There are five types of Threat Events:

- **threat_found**: A new threat has been found in an Unsafe status.
- **threat_removed**: An existing threat has been Removed.
- **threat_quarantined**: A new threat has been found in the Quarantine status.
- **threat_waived**: A new threat has been found in the Waived status.
- **threat_changed**: The behavior of an existing threat has changed (examples: Score, Quarantine Status, Running Status).

  Example Message of Threat Event:

```
Event Type: Threat, Event Name: threat_found, Device Name:
1, IP Address: (), File Name: virusshare_00fbc4cc4b42774b50a9f71074b79bd9,
Path: c:\ruby\host_automation\test\data\test_files\, SHA256:
1EBF3B8A61A7E0023AAB3B0CB24938536A1D87BCE1FCC6442E137FB2A7DD510B, Status: Unsafe,
Cylance Score: 100, Found Date: 6/1/2015 10:57:42 PM, File Type: Executable, Is
Running: False, Auto Run: False, Detected By: FileWatcher
```

Threat Classifications

Hundreds of threats are classified each day as either Malware or Potentially Unwanted Programs (PUPs). If this option is selected, you subscribe to be notified when these events occur.

Example Message of Threat Classification:

```
Event Type: ThreatClassification, Event Name: ResearchSaved, Threat
Class: Malware, Threat Subclass: Worm, SHA256:
1218493137321C1D1F897B0C25BEF17CDD0BE9C99B84B4DD8B51EAC8F9794F65
```

Security Information and Event Management (SIEM)

Specifies the type of Syslog server or SIEM that events are to be sent to.

Protocol

This must match what is configured on your Syslog server. The choices are UDP or TCP. UDP is generally not recommended as it does not guarantee message delivery. Dell recommends TCP (default).

TLS/SSL

Only available if the Protocol specified is TCP. TLS/SSL ensures the Syslog message is encrypted in transit from Advanced Threat Prevention to the Syslog server. Dell encourages customers to select this option. Ensure that the Syslog server is configured to listen for TLS/SSL messages. To use TLS/SSL, it is necessary to configure the Syslog server and import certificates. For more information, see Export Audit Events with TLS/SSL over TCP.

IP/Domain

Specifies the IP address or fully-qualified domain name of the Syslog server that the customer has setup. Consult with your internal network experts to ensure firewall and domain settings are properly configured.

Port

Specifies the port number on the devices that the Syslog server listens for messages. It must be a number between 1 and 65535. Typical values are: 512 for UDP, 1235 or 1468 for TCP, and 6514 for Secured TCP (example: TCP with TLS/SSL enabled).

Severity

Specifies the severity of the messages that should display in the Syslog server. This is subjective, and it may be set to whatever level preferred. The value of severity does not change the messages that are forwarded to Syslog.

Facility

Specifies what type of application is logging the message. The default is Internal (or Syslog). This is used to categorize the messages when they are received by the Syslog server.

Testing the Connection

Click **Test Connection** to test the IP/Domain, Port and Protocol settings. If valid values are entered, after a couple of moments, a success confirmation displays.

Advanced Threat Prevention Syslog IP Addresses

Syslog server IP addresses to allow, by region:

US (includes my.cylance.com and my-vs2.cylance.com):

52.2.154.63

52.20.244.157

52.71.59.248

52.72.144.44

54.88.241.49

AU (my-au.cylance.com):

52.63.15.218

52.65.4.232

EU (my-vs0-euc1.cylance.com and my-vs1-euc1.cylance.com):

52.28.219.170

52.29.102.181

52.29.213.11

Note: This IP Address should remain static.

For the latest IP addresses for Syslog messages, contact Dell ProSupport.

Management

Commit Policies

Uncommitted policies display in a badge icon in the top left of the Management Console. Click the badge icon to navigate to **Management > Commit**.

To commit polices that have been modified and saved:

1. In the left pane, click **Management > Commit**.
2. In Comment, enter a description of the change.

   Best practice: add a comment about the changes that are committed.
3. Click **Commit Policies**.

A policy publication/commit occurs when an administrator clicks **Commit Policies**. The following information displays:

Pending Policy Changes - The number of policy changes ready to commit.

Date Committed - Date and time the policies were committed.

Changed by - User name of the administrator who performed the policy commit.

Comment - Any comments that were added when the polices were committed.

Version - The number of policy saves since the last policy commit plus the previous Version.

Policy Logs - Select **View Logs** to see logs associated with this row's policy commit.

View Pending Commit(s)

Uncommitted policies display in a badge icon in the top left of the Management Console. Click the badge icon to go to **Management > Commit**.

To see pending policy changes in **Log Analyzer**:

1. In the left pane, click **Management > Commit**.
2. Select **View Pending Commit(s)**.

Log Analyzer

Log Analyzer gives you the power to search logs by message priority level, date and time periods, and occurrences of usernames and hosts.

To view or export logs:

1. In the left pane, click **Management > Log Analyzer**.
2. Select a Category.

   The Categories are Admin Actions, Shield for Server Events, Policy, Advanced Threat Events, System Logs, Whitelist, and Full Access List.
3. To narrow the results, select from these optional filters:

- Priority - Choose DEBUG, INFO, WARN, ERROR, or FATAL. FATAL returns fewest entries; DEBUG returns the greatest number of entries.
- And more severe - Select this option to include all areas of greater severity than the priority level you selected.

- Date Range - Enter a Start Date and End Date to limit results to entries that occur between these dates. To insert dates into these fields, click the calendar icons to the right of the fields.
- Time Range - If you entered a Date Range, further narrow the entries by entering a Start Time and End Time. To insert times into these fields, click the calendar icons to the right of the fields.
- Username and Host - Enter a either a username or host or both.

4. Click **Search**.
5. To sort the results in ascending order by column, click the heading of the column to sort.
6. To export the results to an Excel or CSV file, pull down the **Export File** list and select **Excel** or **CSV**.

   Exported files can hold up to 100,000 records.

Recovery

Recover Data - Encryption External Media Authentication Failure

Encryption External Media encrypts data on removable media, as defined by policy. There may be several conditions where access to encrypted data needs to be regained. In general, these scenarios fall into two categories:

- The Encryption External Media password is lost or forgotten
- The Encryption External Media software or encryption key material has been lost or corrupted on the device

If more than one Dell Server is part of a federation, to perform Encryption External Media Recovery across Dell Servers in the federation, see Enable Federated Key Recovery.

Manual Authentication when Encryption External Media Password is Lost or Forgotten

If a user has lost or forgotten a password, manual authentication is necessary.

1. The user is prompted for their password. Since the password is not available, the user clicks **I forgot**.
2. The user is given another opportunity to try again. If the user clicks **Yes - I forgot**, manual authentication begins (or the manual authentication begins upon the set number of retries allowed).
3. The user is instructed to contact their administrator and inform them that they need to manually recover Encryption External Media for Windows.
4. As a Dell administrator, log in to the Management Console.
5. In the left pane, click **Populations > Users**.
6. Enter a filter to search for the user. The wild card character is *. You can enter Common Name, Universal Principal Name, or sAMAccountName.
7. Click . A user or list of users displays, based on your search filter.
8. Locate the appropriate user and click the **Endpoints** tab.
9. Locate the appropriate *Shielded* Endpoint.
10. Under *Actions*, click the **Recover** link.

Tip: Numbers are red and letters are blue.

11. Ask the user for the **Shield ID** and verify that it is correct or enter it into *Shield ID*. Shield IDs do not contain the letters B, O, Q, and S.
12. Ask the user for the 8, 16, or 32-character **Endpoint Code** (not case sensitive) and enter it into the appropriate field. Endpoint Codes contain only the letters A-F.
13. Ask the user for the **Key ID** and enter it into the appropriate field (if your organization allows non-domain user activation, the Key ID is required.
14. Click **Generate Access Code**. The Restore User Access page displays the directory user alias associated with the Encryption client, along with an access code.
15. Confirm to your satisfaction that the request is coming from the directory user alias shown.

    This is especially important if recovering media that may have been given to another user. Dell recommends that you set a help desk policy for how to handle requests from users other than those who originally copied the data.
16. Do **one** of the following:
    - To allow the user to access the endpoint, click **Activate**.
    - To **not** allow the user to access the endpoint, click **Cancel**.
17. If the requester is the device authorized user, ask the user to enter the Access Code (not case sensitive) on the endpoint and click **OK**. The Access Code policies of the user affect this process (for example, how many attempts the user has to enter the code correctly).
18. When the user successfully enters the Access Code, the Encryption client changes the *Current Shield State* policy to *Activate*, and the successfully entered Access Code is no longer valid. Instruct the user to click **OK** to close the dialog.
19. In the left pane, click **Management > Commit**.
20. Click **Commit Policies**.

Once manual authentication is successful, the user is directed to reset their password. Depending on how policies are set, one of the following three options are displayed. The user enters a new password and confirms it, then clicks **OK** or **Cancel**.

Depending on policies set, the user may be prompted to type this password when using this removable media in other computers.

If the policy is set to **block** all access to removable media until authenticated/encrypted and the user clicks Cancel, they cannot access any files on this removable storage. If a user re-uses a password that has been used too recently, a dialog displays asking them to use a different password. If a password does not	If the policy gives **read-access** to removable storage until authenticated/encrypted and the user clicks Cancel, they can read/delete existing files on this removable media , but cannot edit/add files to this removable storage. If a user re-uses a password that has been used too recently, a dialog displays asking them to use a different	If the policy gives **full access** to removable media until authenticated/encrypted and the user clicks Cancel, they have full access to unencrypted files on this removable media, but cannot access encrypted files. If a user re-uses a password that has been used too recently, a dialog displays asking them to use a different

meet the criteria set by policy, a dialog displays, outlining the password criteria.	password. If a password does not meet the criteria set by policy, a dialog displays, outlining the password criteria.	password. If a password does not meet the criteria set by policy, a dialog displays, outlining the password criteria.

The user may now use the removable media as usual.

If manual authentication is **not** successful, the device is disabled according to policy, as follows:

- The policy could be set to wait (cooldown) between unsuccessful manual authentication attempts.

  or

- The policy may be set to delete the encryption key material and prevent any access to encrypted files on this removable media . In this case, the user need to contact an administrator again for instructions to re-enable access.

  Restore Lost Encryption Key Material

  If encryption keys have been deleted on the removable media (because of failed manual authentication, accidentally deleting a necessary file, a change in policy), the encrypted data is inaccessible until an authorized user reinitializes the encryption key material.

  A dialog displays, notifying the user that key material is missing. Click **Yes** to use the self-healing feature of Encryption External Media or click No.

If the policy **blocks** all access to removable media until encrypted and the user clicks No, they cannot access this removable media .	If the policy gives **read-access** to removable media until encrypted and the user clicks No, they have read-access to unencrypted data on this media, but no access to encrypted data.	If the policy gives **full access** to removable media , whether or not encrypted and the user clicks No, they have full access to unencrypted data on this media. They cannot access encrypted data.

  Occasionally, based on policies set, encryption keys cannot be reinitialized on the computer that the removable media is inserted in. If policy permits, the user can insert the media into any Dell-encrypted computer where the original user is logged in, to reinitialize the encryption keys. If policy does not permit this, it must be inserted into the originally encrypting computer, with the originally specified user name.

  On rare occasions, when encryption key material is lost, the Encryption client cannot automatically locate the necessary information. Use the following process to recover encrypted data.

  1. Attach the device to a Windows computer that is not running the Encryption client.
  2. Copy all folders from the device onto the Windows computer.
  3. Use WSScan to determine the DCID of the encrypted data.
  4. Follow the process for recovering access to encrypted data on Windows computers. Use the DCID obtained from WSScan for the RecoveryID.

Enable Federated Key Recovery

If more than one Dell Server is part of a federation, to perform Encryption External Media Recovery across Dell Servers in the federation, enable federated key recovery:

1. Navigate to <Security Server install dir>\conf\ and open the federatedservers.properties file.
2. Update the **server.code** property with a new a code, password or passphrase to be shared across Dell Servers in the federation. Enclose the code, password, or passphrase within a new CLR() tag, to replace the ENC() tag.

   Example: **server.code=CLR(mypassword)**
3. List all Dell Servers to be federated in the server uris property, delimited by a comma.

   Example:
   server.uris=https://server1.company.com:8443,https://server2.company.com:8443
4. Save and copy the federatedservers.properties file to all Dell Servers that are part of the federation.
5. Restart all Security Servers in the federation.

   The restart converts the CLR() tag to the encrypted tag, ENC(), in the federatedservers.properties file.

Recover Data - BitLocker Manager

See the *Recovery Guide* for the most up-to-date recovery instructions.

Recover Endpoint

To download encryption keys of a managed or removed endpoint:

NOTE: Select **Include Removed Endpoints** to display endpoints that were previously removed.

1. In the left pane, click **Management > Recover Endpoint**.
2. Enter the hostname and click **Search**.
3. Click **Recover** next to the endpoint.
4. Enter a password then click **Downloadx86** or **Downloadx64**.
5. Copy the recovery file to the endpoint and run the file.

Windows Recovery

For Windows Recovery, follow the instructions in the *Recovery Guide.* The latest *Recovery Guide* is available at these locations:

Encryption

Endpoint Security Suite Enterprise

SED Recovery

For information about SED authentication failure or SED endpoint recovery, see SED Recovery.

Encryption External Media Recovery

For information about recovering after Encryption External Media authentication failure, see Encryption External Media Authentication Failure.

Mac Recovery

See the *Encryption Enterprise for Mac Administrator Guide,* available at dell.com/support for the most up-to-date recovery instructions.

License Management

License Management

To view usage of Client Access Licenses (CALs) that you own and upload new licenses, click **Management > License Management**.

Upload Client Access Licenses

You received CALs separately from the installation files, either at the initial purchase or later if you added additional CALs.

1. In the left pane, click **Management > License Management**.
2. Under Upload Volume Licenses, click **Choose File** to browse to and select the saved CAL.

View or Add License Notifications

Through Notification Management, you can set up notifications of license usage or expiration.

In the left pane, click **Management > Notification Management**.

Related topics:

CAL Information

Notification Management

Client Access License (CAL) Information

Upon log in to the Management Console, if there is a problem with your CAL, an error message displays (typically, the error states that the Dell Server has exceeded the maximum number of authorized client licenses). The next step is to review your CALs to ensure that your enterprise has the appropriate number of CALs to client ratio (1-to-1 ratio).

If authorized CALs exceed 5% of that specific CAL total, new client activations for that specific product is blocked until the license key is brought into compliance. No other client or Dell Server functions is impacted when a license key is in the over 105% state. Two separate warning messages are displayed, the first warning message is when the CAL reaches 99% of the authorized licenses, the second when the CAL count reaches or exceeds the 105% total.

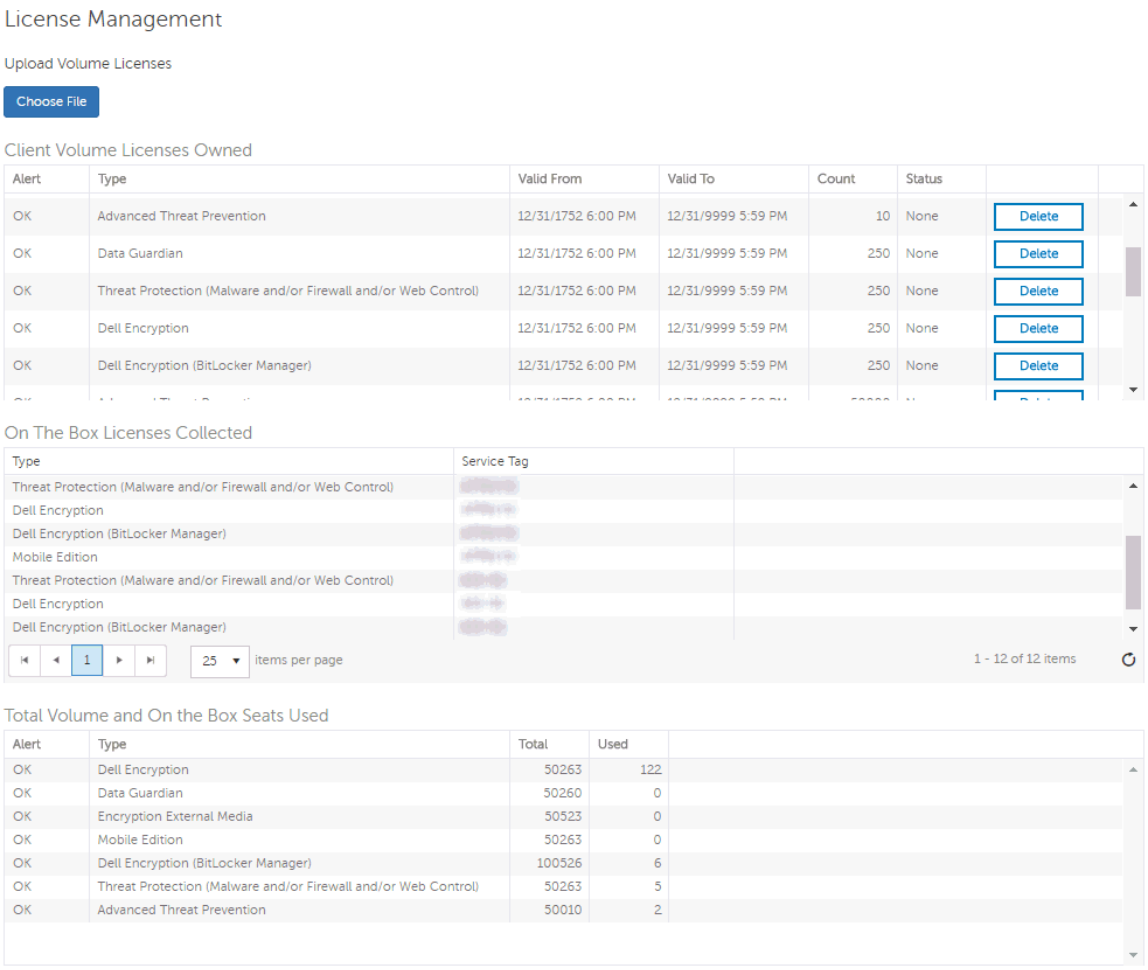
For example:

- Authorized CAL for Dell Encryption (Windows): 5000 user licenses
- First warning message from Dell Server and an email message is sent to the administrator: CAL count reaches 5000
- Second warning message from Dell Server and an email message is sent to the administrator: CAL count reaches 5250

If a user has previously been activated and inventory records exist, then it is not blocked from any re-activation. However, if the CAL authorized count is exceeded during this process, new activations are blocked for the specific CAL that is in the over 105% state.

Licensing

1. License structure:
    a. Disk Encryption (DE) – Dell Encryption (Windows and Mac), Encryption External Media , SED Manager, Full Disk Encryption, BitLocker Manager.
    b. Encryption External Media (EME)
    c. Threat Protection (TP) - includes Malware Protection and/or Client Firewall and/or Web Protection features
    d. Advanced Threat Prevention (ATP) - includes optional Client Firewall and/or Web Protection features
2. Dell Digital Delivery of entitlements



Upload Client Access Licenses

You received CALs separately from the installation files, either at the initial purchase or later if you added additional CALs.

1. In the left pane, click **Management > License Management**.
2. *Under Upload Licenses*, click **Choose File** to browse to the location of the saved CAL.

Related topics:

CAL Information

License Management

On The Box Licenses

See On The Box Licenses for information about the type of licenses in use and the associated Service Tags.

1. In the left pane, click **Management > License Management**.
2. Select the **On The Box Licenses** pane.

Services Management

Services Management

From the left pane of the Management Console, select **Management > Services Management**. The following options are available:

Provision or Recover the Advanced Threat Prevention service - After the service is provisioned, clients are automatically provisioned with Advanced Threat Prevention. For more information, see Provision or Recover Advanced Threat Prevention Service.

Enroll to receive Advanced Threat Prevention agent auto updates - After enrollment, clients can automatically download and apply updates from the Advanced Threat Prevention server. For more information, see Enroll for Agent Auto Update.

Export audit events - Audit events can be exported to a syslog server or to a local file. For more information, see Export Events to SIEM Server.

Provision or Recover Advanced Threat Prevention Service

The Advanced Threat Prevention service is provisioned and recovered through the Services Management Advanced Threats tab. Only system administrator can provision and recover the service.

After provisioning is complete, the contact information of the administrator who provisioned the service is displayed.

The guided setup prompts the system administrator to back up the Advanced Threat Prevention certificate at this time.

Provision service

To provision the Advanced Threat Prevention service:

1. In the left pane of the Management Console, click **Management > Services Management**.
2. Select the **Advanced Threats** tab.
3. Click **Setup Advanced Threat Prevention Service**.
4. Follow the guided setup and complete the necessary fields.

Regional provisioning to support geographical data centers is available for NA (North America), EU (EMEA), and AU (APAC).

Download and back up the Advanced Threat Prevention certificate in a safe location, separate from the server running the Dell Server. The backed up certificate is required if a service recovery is necessary.

Clients are automatically provisioned with Advanced Threat Prevention.

After provisioning is complete, the **Setup** link no longer displays.

Recover service

You will need your backed up certificate to recover the Advanced Threat Prevention service.

1. In the left pane of the Management Console, click **Management > Services Management**.
2. Click **Recover Advanced Threat Prevention Service**.
3. Follow the guided service recovery dialogs and upload the Advanced Threat Prevention certificate when prompted.

Enroll for Advanced Threat Prevention Agent Auto Updates

You can enroll to receive Advanced Threat Prevention agent auto updates. Enrolling to receive agent auto updates allows clients to automatically download and apply updates from the Advanced Threat Prevention server. Updates are released monthly.

Receive agent auto updates

To enroll to receive agent auto updates:

1. In the left pane of the Management Console, click **Management > Services Management**.
2. On the **Advanced Threats** tab, under *Agent Auto Update*, click **On** then click **Save Preferences**.

Stop receiving agent auto updates

To stop receiving agent auto updates:

1. In the left pane of the Management Console, click **Management > Services Management**.
2. On the **Advanced Threats** tab, under *Agent Auto Update*, click **Off** then click the **Save Preferences**.

Events Management - Export Audit Events to a SIEM Server

To export audit events to a syslog server or to a local file:

1. In the left pane, click **Management > Services Management**.
2. Select the **Events Management** tab.
3. Select the appropriate option(s):

   Export to Local File allows you to export audit events to a file. Enter the location in which to store the file. This option also provides a backup of the audit events database.

   Export to Syslog lets you specify the syslog server to which to export the file. If TCP protocol is not selected, select it.

4. Click the **Save Preferences** button.

Product Notifications

You can enroll to receive notifications of product updates, recommended configuration changes, and relevant knowledge base articles.

Receive product notifications

To enroll to receive product notifications:

1. In the left pane, click **Management > Services Management**.
2. Select the **Product Notifications** tab.
3. Click **On** then click **Save Preferences**.

Note: The product notification switch does not display when servers are configured in disconnected mode.

Stop receiving product notifications

To stop receiving product notifications:

1. In the left pane of the Management Console, click **Management > Services Management**.
2. Select the **Product Notifications** tab.
3. Click **Off** then click **Save Preferences**.

Notification Management

Notification Management

The Notification Management page lets you manage email notifications.

To add an email notification:

1. In the left pane, click **Management > Notification Management**.
2. Click **Add** and enter the following information:

   Email: Enter or select your email address.

   Notification Type: Select the type of alert to add.

   Priority Level: Select the priority levels of notifications.

   Email Frequency: Select how often alerts of this type. The default frequency is 24 hours.
3. Click **Add** when complete.

To edit an alert:

- Select the alert to change, click **Edit**, make the changes, and press **Enter**.

To delete an alert:

- Select the alert to delete, and click **Delete**.

Send Test Email

Send test emails from the Management Console to validate email workflows.

To test email workflows:

1. Navigate to **Management > Notification Management**.
2. Select **Send Test Email**.
3. Enter an email address and select **Send Email**.

If the test email passes through the Dell Server successfully, a notification with the following results displays:

- Sent From - email used for testing workflow.
- Server Name - SMTP server used.
- SMTP Port - SMTP port in use for email notifications.
- Authentication - true or false value for authentication protected notifications.

Related topics:

License Management

Enable SMTP Server for Email Notifications

Use this procedure to enable the SMTP server for email notifications.

When configuration changes are complete, restart the Security Server service. The Security Server service must be restarted for the settings to be updated.

Configure SMTP Settings

To receive email notifications, follow the steps in this section to configure SMTP settings. Dell Server email notifications inform recipients of status error states, password updates, availability of Dell Server updates, and client license issues.

It is a best practice to restart the services any time a settings change is made.

To configure SMTP settings, follow these steps:

1. From the Advanced Configuration menu, select **Email Notifications**.
2. In the Set up Email Notifications screen, to enable email alerts, press the space bar to enter an **X** in the Enable Email Alerts field.
3. Enter the *SMTP server* fully qualified domain name.
4. Enter the *SMTP port*.
5. In *From User*, enter the email account ID that will send email notifications.
6. In *Enter User*, enter an email account ID for access to change configured email notifications.
7. In *Password*, enter a password for access to change configured email notifications.
8. In *Mail IDs* for Dell Server Status, Password Updates, and Updates Availability, enter lists of recipients for each notification type.
9. Follow these conventions when listing recipients:

   Email address format is recipient@dell.com.

   Recipients are separated with commas or semicolons.
10. In *Service alert reminder*, to enable reminders, press the space bar to enter an X in the field then set the reminder interval in minutes.
11. A Service alert reminder is triggered when the reminder interval has passed after a notification is sent about a system health issue and the host or service remains in the same state.

12. In the *Summary Report*, to enable reports of notifications, select the desired interval (daily, weekly, or monthly) and then press the space bar to enter an **X** in the field.
13. Select **OK**.

Product Notifications

You can enroll to receive notifications of product updates, recommended configuration changes, and relevant knowledge base articles.

Receive product notifications

To enroll to receive product notifications:

1. In the left pane, click **Management > Services Management**.
2. Select the **Product Notifications** tab.
3. Click **On** then click **Save Preferences**.

Note: The product notification switch does not display when servers are configured in disconnected mode.

Stop receiving product notifications

To stop receiving product notifications:

1. In the left pane of the Management Console, click **Management > Services Management**.
2. Select the **Product Notifications** tab.
3. Click **Off** then click **Save Preferences**.

Change Superadmin Password

1. In the masthead at the top of the screen, click the gear icon and select **Change superadmin password**.
2. Enter the current password.
3. Enter the new password.

   The new password must be at least 6 characters, contain at least one capital letter and one of these characters: **~@#$%^*()|?!{}[]**.
4. Confirm the new password.
5. Click **Update**.

After three failed login attempts, the superadmin account is locked for five minutes. To change these settings, see Set or Change Account Lockout Settings.

Change Account Lockout Settings

After three failed login attempts, the superadmin account is locked for five minutes. To change these settings:

1. Open <Security Server installation folder>\conf\application.properties.
2. Edit the following property to change the maximum allowed number of failed login attempts.

login.cooldown.max.failed.attempts=3

3. Edit the following property to change the length of lockout time after the maximum allowed number of failed login attempts is reached.

   login.cooldown.minutes=5

4. Save the file, and restart the Security Server.

Downloads

Endpoint Software

To download the latest version of Dell Encryption:

1. In the left pane, click **Management > Downloads.**
2. Select the **Endpoint Software** tab.
3. Click **Navigate to Download.**

   The **Download** tab is only available if the user has been assigned a security and a system administrator role.

To download the latest version of Endpoint Security Suite Enterprise (ESSE):

1. In the left pane, click **Management > Downloads.**
2. Select the **Endpoint Software** tab.
3. Click **Dell Support** to contact Dell for access to Dell Endpoint Security Suite Enterprise.

Manage Policies

Manage Security Policies

You can apply security policies at the Enterprise, Domain, User Group, User, Endpoint Group, and Endpoint levels. Default policy settings allow your enterprise to get started with Dell security, but you should customize the security and configuration settings. If you've migrated from an earlier version of Dell Server, your policy settings have been migrated for you.

Security policies are grouped by technology. Click a technology group to view its policies and policy descriptions.

Windows Encryption	**Threat Prevention**	**Mac Encryption**
Full Disk Encryption (FDE)	Advanced Threat Prevention	Dell Volume Encryption
Self-Encrypting Drive (SED)	Threat Protection	Mac Global Settings
Policy-Based Encryption	Web Protection	
BitLocker Encryption	Client Firewall	
Server Encryption	Protection Settings	

Authentication	**Removable Media Encryption**	**Port Control**
Pre-Boot Authentication	Windows Media Encryption	Windows Port Control
Windows Authentication	Mac Media Encryption	Windows Device Control
	Media Encryption Settings	

Global Settings
Settings

The following override information displays at the top of the Security Policies page:

Override count - the number of policy settings that are changed from their default settings.

Uncommitted overrides - the number of changes from default settings that are not yet committed.

NOTE: The Security Policies page for a population displays overrides to localizable policies in the browser language only.

Icons and their meanings:

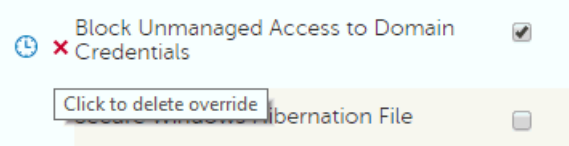
	The master switch for policies in the subgroup is On, which means the policy group is enabled. Policies in the group are sent to clients when policies are committed.
	Policies in the subgroup are not enabled.
	At least one default setting in the policy group has been overridden.
	Group of policy settings that has no master switch.
	The policy change is not yet committed.
	The policy value can be localized, so that policies on the endpoint computer display in a

selected language. For more information, see Localize Policies Displayed on the Endpoint Computer and Localizable policies.

The default setting of a localizable policy is overridden.

A localizable policy change is not yet committed.

To remove a policy override, hover over the red flag next to the policy name. The red flag becomes a red X. Click the red **X** to revert to the default value.



Group precedence

You can Modify Group Precedence. Group precedence creates a weight associated with the specific group it is assigned to, and that weight is used in policy arbitration for all policy overrides.

Related topics:

View or Modify Enterprise-Level Policies

View or Modify Domain Policies and Information

View or Modify User Group Policies and Information

View or Modify User Policies and Information

View or Modify Endpoint Group Policies and Information

View or Modify Endpoint Policies and Information

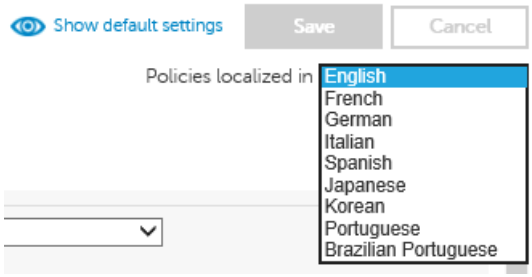
Localize Policies Displayed on the Endpoint Computer

Localizable policies are indicated by:

To localize policies that are displayed on the endpoint computer, follow these steps:

1. In the left pane, expand **Populations** and select a population.
2. Click the **Security Policies** tab.
3. Select the technology group, such as *Windows Encryption*, or policy group, such as *Policy-Based Encryption*, to modify.

4. Select a language for localizable policies from the list at the top right of the screen.



5. Enter text that is in the language you selected for localizable policies. Navigate the populations and technology groups as necessary to localize all desired policies for that language.
6. Click **Save**.
7. To update policies in a different language, select the language from the list, enter localized text for all desired policies, and click **Save**.

   Save policy changes before selecting another language in the list. A different language cannot be selected until policy changes are saved.
8. When finished, select the desired language. Any changes made to localizable policies are made in the language that displays.

NOTE: The Security Policies page for a population displays overrides to localizable policies in the browser language only.

Localizable Policies

Localizable policies are indicated with by

Available languages:

English	Korean
French	Brazilian Portuguese
German	Portuguese
Italian	Spanish
Japanese	

For instructions about localizing policies, see Localize_policies.

The following policies can be displayed in a selected language on the endpoint computer:

Enterprise Level

Technology Group	**Policy**

Windows Encryption > Full Disk Encryption	Support Information Text
	Full Disk Encryption Title Text
	Legal Notice Text
	Self Help Questions
Windows Encryption > Self-Encrypting Drive (SED)	Support Information Text
	PBA Title Text
	Legal Notice Text
	Self Help Questions (Pre-8.0 clients)
Windows Encryption > Policy-Based Encryption	Common Encrypted Folders
	User Encrypted Folders
	OS Update Encryption Rules
	Application Data Encryption List
	Managed Services
Windows Encryption > BitLocker Encryption	Default Folder Location to Save Recovery Password
Authentication > Windows Authentication	Recovery Questions for Windows Authentication (check box selections)
Removable Media Encryption > Windows Media Encryption	EMS Device Whitelist
	EMS Access Code Required Message
	EMS Access Code Failed Message

Users Level

Technology Group	**Policy**
Windows Encryption > Policy-Based Encryption	User Encrypted Folders

	Application Data Encryption List
	Managed Services
Removable Media Encryption > Windows Media Encryption	EMS Device Whitelist
	EMS Access Code Required Message
	EMS Access Code Failed Message
Endpoints Level	
Technology Group	**Policy**
Windows Encryption > Self-Encrypting Drive (SED)	Support Information Text
	PBA Title Text
	Legal Notice Text
	Self Help Questions (Pre-8.0 clients)
Windows Encryption > Policy-Based Encryption	Common Encrypted Folders
	OS Update Encryption Rules
Windows Encryption > BitLocker Encryption	Default Folder Location to Save Recovery Password

Windows Encryption

Windows Encryption

A word about types of encryption: SDE is designed to encrypt the operating system and program files. To accomplish this purpose, SDE must be able to open its encryption key while the operating system is booting without intervention of a password by the user. Its intent is to prevent alteration or offline attacks on the operating system by an attacker. SDE is not intended for user data. Common and User key encryption are intended for sensitive user data because they require a user password to unlock encryption keys.

Policy descriptions also display in tooltips in the Management Console. In this table, master policies are in bold font.

Policy	Default Setting	Description
Full Disk Encryption (FDE)		

This technology manages drives using software-based Full Disk Encryption. Authentication by users through a Pre-Boot Authentication environment (before the operating system has booted) is required to unlock the drive.		
Full Disk Encryption (FDE)	Off	*On* *Off* Toggle to ON to enable all full disk encryption policies. If this policy is toggled to OFF, no full disk encryption takes place, regardless of other policy values. On means that all Full Disk Encryption policies are enabled. Changing the value of this policy triggers a new sweep to encrypt/decrypt files.
Encryption Algorithm	AES 256	AES 256, AES 128, FIPS AES 256, FIPS AES 128 Encryption algorithm used for Full Disk Encryption.
Encryption Mode	CBC	CBC, XTS Encryption mode used for Full Disk Encryption.
Enable FDE Plugin	Selected	The plugin must remain selected. To deactivate the PBA and disable full disk encryption, toggle the *Full Disk Encryption* policy to OFF.
Self-Encrypting Drive (SED) This technology manages self-encrypting drives (SEDs). Authentication by users through a Pre-Boot Authentication environment (before the operating system has booted) is required to unlock the drive.		
Self-Encrypting Drive (SED)	On	*On* *Off* Enable this policy to provision the PBA. If disabled after the PBA is provisioned, the PBA is de-provisioned and the PBA database is deleted. Re-enabling this policy re-provisions the PBA and re-creates the PBA database.
See advanced settings		
Policy	Default Setting	Description
Policy-Based Encryption This technology uses Dell's proprietary data centric encryption to allow user data and computer		

encryption. This allows greater protection over individual data than traditional full disk encryption, by limiting access on a computer to only what a user is authorized to view.		
Policy-Based Encryption	On	*On* *Off* Toggle to ON to enable all policy-based encryption policies. If this policy is toggled to OFF, no policy-based encryption takes place, regardless of other policy values. On means that all Policy-Based Encryption policies are enabled. Changing the value of this policy triggers a new sweep to encrypt/decrypt files.
Application Data Encryption Key	Common	Common, User, User Roaming Choose a key to indicate who can access files encrypted by Application Data Encryption List, and where. More... Common for these files to be accessible to all managed users on the computer where they were created (the same level of access as Common Encrypted Folders), and encrypted with the Common encryption algorithm. User for these files to be accessible only to the user who created them, only on the computer where they were created (the same level of access as User Encrypted Folders), and encrypted with the user encryption algorithm. User Roaming for these files to be accessible only to the user who created them, on any encrypted Windows computer, and encrypted with the User encryption algorithm. Changes to this policy do not affect files already encrypted because of this policy.
SDE Encryption Enabled	Not Selected	If this policy is not selected, SDE

		encryption is disabled, regardless of other policy values. Selected means that all data not encrypted by other Intelligent Encryption policies are encrypted per the SDE Encryption Rules policy. Changing the value of this policy requires a reboot.
SDE Encryption Rules	String F#:\ -^%ENV:SYSTEMDRIVE%\System Volume Information -^%ENV:SYSTEMROOT%\;dll.exe.sys.ocx.man.cat.manifest.policy -^%ENV:SYSTEMROOT%\System32 -^%ENV:SYSTEMROOT%\SysWow64 -^%ENV:SYSTEMROOT%\WinSxS -^%ENV:SYSTEMROOT%\Fonts ^3@%ENV:SYSTEMROOT%\SYSTEM32\;exe -^3@%ENV:SYSTEMROOT%\SYSTEM32\cmd.exe;exe -^3@%ENV:SYSTEMROOT%\SYSTEM32\autochk.exe;exe -^3@%ENV:SYSTEMROOT%\SYSTEM32\winresume.exe;exe -^F#:\bootmgr -^F#:\boot -^@%ENV:SYSTEMDRIVE%\;vol -^%ENV:SYSTEMDRIVE%\Program Files\PGP Corporation -^3%ENV:SYSTEMDRIVE%\PGPWDE00 -^3%ENV:SYSTEMDRIVE%\PGPWDE01 -^3%ENV:SYSTEMDRIVE%\PGPWDE02 -^3%ENV:SYSTEMDRIVE%\PGPWDE03 -^%ENV:SYSTEMDRIVE%\Program Files\Symantec -^%ENV:SYSTEMDRIVE%\Program Files (x86)\Symantec -^%ENV:SYSTEMDRIVE%\Program Files\Common Files\Symantec Shared -^%ENV:SYSTEMDRIVE%\Program Files (x86)\Common Files\Symantec Shared -^%ENV:SYSTEMDRIVE%\ProgramData\Symantec -^3%ENV:SYSTEMDRIVE%\SafeBoot.fs -^3%ENV:SYSTEMDRIVE%\SafeBoot.rsv -^3%ENV:SYSTEMDRIVE%\SafeBoot.csv -^3%ENV:SYSTEMDRIVE%\Program Files\McAfee -^3%ENV:SYSTEMDRIVE%\Program Files\Common Files\McAfee	Encryption rules to be used to encrypt/not encrypt certain drives, directories, and folders. See Encryption Rules for information. SDE Encryption Rules may be changed as appropriate for your environment. However, these defaults have been tested extensively. Removing these exclusions may result in Windows issues, particularly after applying patch updates. Contact ProSupport for guidance if you are unsure about changing the values.

	-^3%ENV:SYSTEMDRIVE%\Program Files\McAfee -^3%ENV:SYSTEMDRIVE%\Program Files (x86)\Common Files\McAfee -^3%ENV:SYSTEMDRIVE%\\Program Files (x86)\Mcafee -^%ENV:SYSTEMDRIVE%\Program Files\Trend Micro\ -^3%ENV:SYSTEMDRIVE%\ProgramData\Dell\Kace -^3%ENV:SYSTEMDRIVE%\Program Files\Dell\Kace -^3%ENV:SYSTEMDRIVE%\Program Files (x86)\Dell\Kace	
Common Encrypted Folders	String %ENV:SYSTEMDRIVE%\;accdb.doc.docm.docx.mdb.pdf.ppam.pps.ppsm.ppsx.ppt.pptm.pptx.pub.puz.sldm.sldx.tif.tiff.vdx.vsd.vss.vst.vsx.vtx.xlam.xlm.xls.xlsb.xlsm.xlsx.xsf.zip.rar %ENV:USERPROFILE%\Desktop %ENV:USERPROFILE%\Download -^%ENV:SYSTEMDRIVE%\;dat.ini.xml.txt.log.db.lnk	String - maximum of 100 entries of 500 characters each (up to a maximum of 2048 characters) A list of folders on computer drives to be encrypted or excluded from encryption, which can then be accessed by all managed users who have access to the computer. See Encryption Rules for information. The text in this policy is translatable. **Important:** *Overriding directory protection can result in an unbootable computer and/or require reformatting drives.* More... The available drive letters are: #: Refers to all drives f#: Refers to all fixed (non-removable) drives r#: Refers to all removable drives If the same folder is specified in both this policy and the User Encrypted Folders policy, this policy prevails.
See advanced settings		

Policy	Default Setting	Description
Bitlocker Encryption This technology manages Microsoft BitLocker policies for full disk and removable media encryption.		

BitLocker Encryption	Not Managed	*Managed* *Not Managed* Toggle to Managed to enable BitLocker Manager policy settings. Toggling to Not Managed disables all BitLocker Manager policies, regardless of other policy values.
TPM Manager Enabled	Not Selected	*Selected* *Not Selected* Selected enables TPM management with BitLocker management. Not Selected disables **all** TPM management policies, *including* policies in the Operating System Volume Settings category.
Disable Sleep Mode	Not Selected	*Selected* *Not Selected* Selected disables sleep mode on the local computer. Changing this policy requires a reboot for the new value to take effect.
Encrypt System Drive	Do Not Manage	*Do Not Manage* *Turn On Encryption* *Turn Off Encryption* Do Not Manage ignores the System Drive (typically the drive that the operating system is installed on). Turn On Encryption allows BitLocker to encrypt the System Drive only. Turn Off Encryption disables BitLocker from encrypting the system drive or decrypts any BitLocker-encrypted system drives.
Encrypt Fixed Drives	Do Not Manage	*Do Not Manage* *Turn On Encryption* *Turn Off Encryption* This policy does not encrypt the system drive. To also encrypt the system drive, make sure that Encrypt System Drive Only is also Turn On Encryption. Do Not Manage ignores Fixed Drives. Turn On Encryption allows BitLocker to encrypt

		Fixed Drives. Turn Off Encryption causes Manager to decrypt any BitLocker encrypted fixed drives.
Encrypt Removable Drives	Do Not Manage	*Do Not Manage* *Turn On Encryption* *Turn Off Encryption* Do Not Manage ignores Removable Drives. Turn On Encryption allows BitLocker to encrypt Removable Drives. Turn Off Encryption causes Manager to decrypt any BitLocker encrypted removable drives.
Require Additional Authentication at System Startup	Not Selected	*Selected* *Not Selected* This policy allows for the configuration of BitLocker to require additional authentication each time the computer starts up [with or without a Trusted Platform module (TPM)]. More... This policy is the parent policy to: Allow BitLocker Encryption Without a Compatible TPM Configure TPM Startup Configure TPM Startup PIN Configure TPM Startup Key Configure TPM Startup Key and PIN
Allow BitLocker Encryption Without a Compatible TPM	Selected	*Selected* *Not Selected* Selected allows a computer without a compatible TPM to use BitLocker encryption. In this mode, a USB drive is required for startup. When the key is inserted, access to the drive is authenticated and the drive is accessible. If the USB key is lost or unavailable, the computer will require

		BitLocker recovery for access. To use this policy, Require Additional Authentication at System Startup must be set to Selected.
Configure TPM Startup	Allow	*Do Not Allow* *Require* *Allow* On computers with a compatible TPM, three types of authentication are supported. Only one of the following can be required or allowed: Configure TPM Startup PIN Configure TPM Startup Key Configure TPM Startup Key and PIN To use this policy, Require Additional Authentication at System Startup must be set to Selected.
Configure TPM Startup PIN	Allow	*Do Not Allow* *Require* *Allow* To use this policy, Require Additional Authentication at System Startup must be set to Selected. This type of authentication involves the entry of a 4-digit to 20-digit personal identification number (PIN).
Configure TPM Startup Key	Do Not Allow	*Do Not Allow* *Require* *Allow* To use this policy, Require Additional Authentication at System Startup must be set to Selected. This type of authentication involves insertion of a USB drive containing the startup key.

Configure TPM Startup Key and PIN	Do Not Allow	*Do Not Allow* *Require* *Allow* To use this policy, Require Additional Authentication at System Startup must be set to Selected. This type of authentication involves a 4-digit to 20-digit personal identification number (PIN) and a USB drive containing the startup key.
Encryption Method and Cipher Strength (OS Volumes)	XTS-AES-128	*AES-128* *AES-256* *XTS-AES-128 (for use with Windows 10 Anniversary Edition and later)* *XTS-AES-256 (for use with Windows 10 Anniversary Edition and later)* Algorithm and cipher strength used by BitLocker Drive Encryption for OS Volumes.
Encryption Method and Cipher Strength (Removable Volumes)	AES-128	*AES-128* *AES-256* *XTS-AES-128 (for use with Windows 10 Anniversary Edition and later)* *XTS-AES-256 (for use with Windows 10 Anniversary Edition and later)* Algorithm and cipher strength used by BitLocker Drive Encryption for Removable Volumes. To encrypt removable drives to use with older versions of Windows as well as with Windows 10 Anniversary Edition and later, use AES-128 or AES-256.
Encryption Method and Cipher Strength (Fixed Volumes)	XTS-AES-128	*AES-128* *AES-256* *XTS-AES-128 (for use with Windows 10 Anniversary Edition and later)* *XTS-AES-256 (for use with Windows 10 Anniversary Edition and later)* Algorithm and cipher

		strength used by BitLocker Drive Encryption for Fixed Volumes.
See advanced settings		
Policy	**Default Setting**	**Description**
Server Encryption This technology manages Dell's data centric encryption using certificate-based authentication instead of the typical user-based authentication instead of the typical user-based authentication. This technology allows for protection of devices such as Windows Servers that do not commonly have users logged in.		
Server Encryption	Off	*On* *Off* This policy enables or disables System Data Encryption (SDE) and Common Encryption on the client server. Changing the value of this policy triggers a new sweep to encrypt/decrypt files.
Allow Software Server Encryption	Selected	*Selected* *Not Selected* If this policy is Selected, client servers are activated at the Enterprise level. This policy may be set to Not Selected to block activations during initial Dell Server setup and maintenance interruptions.
Server Maintenance Schedule	Not Selected	This policy must be selected to use all other Server Maintenance policies. If this policy is Not Selected, no Server Maintenance policies are enforced, regardless of other policy values. Selected allows a maintenance schedule to control application of policy that requires a reboot.
Server Maintenance Schedule Repeats	Weekly	*Daily, Weekly, Monthly, Quarterly, Annually* The schedule configuration defines when the task should run.

		Daily: Runs the task every day at the specified Server Maintenance Schedule Start Time. Weekly: Runs the task weekly on the days specified in Server Maintenance Day of the Week. Monthly: Runs the task monthly on the specified Server Maintenance Day of the Month. Quarterly: Runs the task quarterly on the specified Server Maintenance Day of the Month. Annually: Runs the task annually on the specified Server Maintenance Day of the Month.
Port Control System	Disabled	Enable or Disable all Port Control System policies. If this policy is set to Disable, no Port Control System policies are applied, regardless of other Port Control System policies. **All** PCS policies require a reboot before the policy takes effect.
SDE Encryption Enabled	Selected	If this policy is Not Selected, SDE encryption is disabled, regardless of other policy values. Selected means that all data not encrypted by other Intelligent Encryption policies are encrypted per the SDE Encryption Rules policy. Changing the value of this policy requires a reboot
SDE Encryption Rules	String F#:\ -^%ENV:SYSTEMDRIVE%\System Volume Information -^%ENV:SYSTEMROOT%\;dll.exe.sys.ocx.man.cat.manifest.policy -^%ENV:SYSTEMROOT%\System32 -^%ENV:SYSTEMROOT%\SysWow64 -^%ENV:SYSTEMROOT%\WinSxS -^%ENV:SYSTEMROOT%\Fonts ^3@%ENV:SYSTEMROOT%\SYSTEM32\;exe -^3@%ENV:SYSTEMROOT%\SYSTEM32\cmd.exe;exe -^3@%ENV:SYSTEMROOT%\SYSTEM32\autochk.exe;exe	Encryption rules to be used to encrypt/not encrypt certain drives, directories, and folders. See Encryption Rules for information. SDE Encryption Rules may be changed as appropriate for your environment. However, these defaults have

	-^3%ENV:SYSTEMDRIVE%\ProgramData\Dell\Kace -^3%ENV:SYSTEMDRIVE%\Program Files\Dell\Kace -^3%ENV:SYSTEMDRIVE%\Program Files (x86)\Dell\Kace	been tested extensively. Removing these exclusions may result in Windows issues, particularly after applying patch updates. Contact ProSupport for guidance if you are unsure about changing the values.
Encryption Enabled	Selected	This policy must be selected to use all Common Encryption policies. Not Selected means that no Common Encryption takes place, regardless of other policy values. Changing the value of this policy triggers a new sweep to encrypt/decrypt files.
See advanced settings		

Variables

Some Windows policies support the following variables. A pathname can consist entirely of one or more of these variables, or can include one or more of these variables at any point.

To get directory locations that these CSIDL values resolve to, go to http://msdn.microsoft.com/en-us/library/bb762494.aspx. All names listed on the MSDN page are CSIDL_<name>.

- Includes any of the following Windows CSIDL constants:

DESKTOP

INTERNET

PROGRAMS

CONTROLS

PRINTERS

PERSONAL

FAVORITES

STARTUP

RECENT

SENDTO

STARTMENU

STARTMENU

MYDOCUMENTS

MYMUSIC

MYVIDEO

DESKTOPDIRECTORY

DRIVES

NETWORK

NETHOOD

FONTS

TEMPLATES

COMMON_STARTMENU

COMMON_PROGRAMS

COMMON_STARTUP

COMMON_DESKTOPDIRECTORY

APPDATA

PRINTHOOD

LOCAL_APPDATA

ALTSTARTUP

COMMON_ALTSTARTUP

COMMON_FAVORITES

INTERNET_CACHE

COOKIES

HISTORY

COMMON_APPDATA

WINDOWS

SYSTEM

PROGRAM_FILES

PROGRAMFILES

MYPICTURES

PROFILE

SYSTEMX86

PROGRAM_FILESX86

PROGRAMFILESX86

PROGRAM_FILES_COMMON

PROGRAM_FILES_COMMONX86

COMMON_TEMPLATES

COMMON_DOCUMENTS

COMMON_ADMINTOOLS

ADMINTOOLS

CONNECTIONS

COMMON_MUSIC

COMMON_PICTURES

COMMON_VIDEO

RESOURCES

PROFILES

- Includes a numeric or text value stored in the registry for the current user. If you specify a path but not an item, the client uses the default value

- Includes a numeric or text value stored in the registry for the local computer. If you specify a path but not an item, the client uses the default value

- Includes the value of a Windows local environment variable

- Includes the % character

Windows Policies that Require Reboot

- SDE Encryption Enabled
- Encrypt Windows Paging File
- Secure Windows Credentials
- All PCS policies

Windows Policies that Require Logoff

- SDE Encryption Enabled
- User state change to Suspended
- EMS Encrypt External Media
- EMS Scan External Media
- EMS Encryption Algorithm
- EMS Exclude CD/DVD Encryption
- EMS Data Encryption Key

Advanced Windows Encryption

A word about types of encryption: SDE is designed to encrypt the operating system and program files. To accomplish this purpose, SDE must be able to open its encryption key while the operating system is booting without intervention of a password by the user. Its intent is to prevent alteration or offline attacks on the operating system by an attacker. SDE is not intended for user data. Common and User key encryption are intended for sensitive user data because they require a user password to unlock encryption keys.

Policy descriptions also display in tooltips in the Management Console. In this table, master policies are in bold font.

Policy	Default Setting	Description
Self-Encrypting Drive (SED) This technology manages self-encrypting drives (SEDs). Authentication by users through a Pre-Boot Authentication environment (before the operating system has booted) is required to unlock the drive.		
Enable SED Plugin	Selected	The plugin must remain selected. To deactivate the PBA and disable SED Manager, toggle the *Self-encrypting Drive* policy to OFF.
See basic settings		
Policy	**Default Setting**	**Description**
Policy-Based Encryption This technology uses Dell's proprietary data centric encryption to allow user data and computer encryption. This allows greater protection over individual data than traditional full disk encryption, by limiting access on a computer to only what a user is authorized to view.		
Encrypt with SDE when SED is detected	Not Selected	When Selected, this policy applies SDE encryption to self-encrypting drives. Use this policy when SDE encryption is preferred instead of native SED encryption.
User Encrypted Folders	String	String - maximum of 100 entries of 500 characters each (up to a maximum of 2048 characters) A list of folders on the computer hard drive to be encrypted with the user data encryption key or excluded from encryption. If the same folder is specified in this policy for multiple users of the same Windows computer, each file in that folder is encrypted for the **first owner** of the file after the policy takes effect, and can be decrypted only by that owner. The text in this policy is translatable. More... Specify as for Common Encrypted Folders. This policy applies to all drives classified by Windows as Hard Disk Drives (see My Computer). You cannot use this policy to encrypt drives or external media whose type displays as Removable Disk, use EMS Encrypt External Media instead.
Application Data Encryption List	Exe List winword.exe excel.exe powerpnt.exe msaccess.exe winproj.exe outlook.exe acrobat.exe visio.exe mspub.exe winzip.exe winrar.exe onenote.exe	String - maximum of 100 entries of 500 characters each Do not add explorer.exe or iexplorer.exe to the ADE list, as unexpected or unintended results may occur. Explorer.exe is the process used to create a new notepad file on the desktop using the right-click menu. Setting encryption by file extension, instead of the ADE list, provides more comprehensive coverage. Changes to this policy do not affect files already encrypted because of this policy. List process names of applications (without paths) whose new files you want encrypted, separated by carriage returns. Do not use wildcards.

	onenotem.exe	The text in this policy is translatable. More... You can also specify these process names (separated by commas) via the registry value HKLM\Software\Dell\CMGShield\ApplicationDataEncryptionList. The Encryption client encrypts all new files (not already being encrypted by Common Encrypted Folders and User Encrypted Folders) on the current computer hard drives created by these application processes whenever they are owned by a currently-logged-on managed user. This may include files excluded from encryption by Common Encrypted Folders and/or User Encrypted Folders. The following folders and their subfolders are always excluded from encryption by this policy: C:\Windows\system32 C:\Windows\Software Distribution C:\Windows\Security C:\System Volume Information\Program Files\Dell\(.dll.exe.sys.mac.ddp.wip.rty.nmd.inv) Dell strongly recommends not listing applications or installers that write system-critical files. Doing so could result in encryption of important system files, which could make a Windows computer unbootable. Common process names: outlook.exe winword.exe powerpnt.exe msaccess.exe wordpad.exe mspaint.exe excel.exe The following hard-coded system and installer process names are ignored if specified in this policy (you can also add to this list via the registry value HKLM\Software\Dell\CMGShield\EUWPrivilegedList): hotfix.exe, a Windows update process update.exe, a Windows update process setup.exe, a third-party installer process msiexec.exe, a third-party installer process wuauclt.exe, a Windows update process wmiprvse.exe, a Windows system process migrate.exe, a Windows update process unregmp2.exe, a Windows update process ikernel.exe, a third-party installer process wssetup.exe, the Windows Encryption client installer svchost.exe, a Windows system process
User Encryption Algorithm	AES256	AES256, Rijndael 256, AES128, Rijndael 128, 3DES Encryption algorithm used to encrypt data at the individual user level. You can specify different values for different users of the same computer. Encryption algorithms in order of speed, fastest first, are Rijndael 128, AES 128, Rijndael 256, AES 256, 3DES.
SDE Encryption Algorithm	AES256	AES 256, AES 128, 3DES Encryption algorithm used to for System Data Encryption. Encryption algorithms in order of speed, fastest first, are AES 128, AES 256, 3DES.
Common Encryption Algorithm	AES256	AES256, Rijndael 256, AES128, Rijndael 128, 3DES Encryption algorithm used to encrypt data at the endpoint (all users) level. System paging files are encrypted using AES 128. Encryption algorithms in order of speed, fastest first, are Rijndael 128, AES 128, Rijndael 256, AES 256, 3DES.
Encrypt	Not Selected	Encrypts Outlook Personal Folders (%csidl:local_appdata

Outlook Personal Folders		%\Microsoft\Outlook) with the User data encryption key.
Encrypt Temporary Files	Selected	When this policy is selected, the paths listed in the environment variables TEMP and TMP are encrypted. TEMP and TMP for the operating system are encrypted with the Common encryption key. To reduce encryption sweep time, the contents of the TEMP and TMP folders are cleared for initial encryption, as well as updates to this policy. However, if your organization uses a third-party application that requires the file structure within the \temp directory to be preserved, you should prevent this deletion. To disable temporary file deletion, create DeleteTempFiles (REG_DWORD) and set its value to 0 in the registry at HKLM\SOFTWARE\Credant\CMGShield.
Encrypt Temporary Internet Files	Selected	When this policy is selected, the path listed in the environment variable CSIDL_INTERNET_CACHE is encrypted with the User data encryption key. To reduce encryption sweep time, the contents of CSIDL_INTERNET_CACHE are cleared for initial encryption, as well as updates to this policy. This policy is applicable when using Microsoft Internet Explorer only. For other web browsers, an administrator must create an encryption policy that is specific to the storage location of the temporary internet files used by each browser.
Encrypt User Profile Documents	Not Selected	When this policy is selected, the following are encrypted: • The users profile (C:\Users\jsmith) with the User data encryption key • \Users\Public with the Common encryption key
Encrypt Windows Paging File	Selected	When this policy is selected, the Windows paging file is encrypted. A change to this policy requires a reboot.
Managed Services	String	String - maximum of 100 entries of 500 characters each (up to a maximum of 2048 characters) When a service is managed by this policy, the service is started only after the user is logged in and the Encryption client is unlocked. This policy also ensures that the service managed by this policy is stopped before the Encryption client is locked during logoff. This policy can also prevent a user logoff if a service is unresponsive. More... Syntax is one Service name per line. Spaces in the service name are supported. Wildcards are not supported. Entries are not case-sensitive. For example, GoogleDesktop Manager is the same as googledesktopmanager. The service "log on as" setting has no bearing on whether or not the Encryption client can control it. It does not matter if a user logs on with user credentials verses the local system. The startup type (Automatic or Manual) does not affect the ability of the Encryption client to control it. Automatic or Manual startup is acceptable. Managed services are not started if an unmanaged user logs on.
Secure Post-Encryption Cleanup	No Overwrite	No Overwrite, Single-pass Overwrite, Three-pass Overwrite, Seven-pass Overwrite Once encryption is complete, this policy determines what happens to the unencrypted residue of the original files: • No Overwrite deletes it. This value yields the fastest encryption processing. • Single-pass Overwrite overwrites it with random data. • Three-pass Overwrite overwrites it with a standard pattern

		of 1s and 0s, then with its complement, and then with random data. • Seven-pass Overwrite overwrites it with a standard pattern of 1s and 0s, then with its complement, and then with random data five times. This value makes it most difficult to recover the original files from memory, and yields the most secure encryption processing.
Secure Windows Credentials	Not Selected	When this policy is selected, the Windows Credentials are secured by encrypting the entire registry with the exception of registry information required for computer boot. The information required for computer boot includes HKLM/SYSTEM and all sub-keys.. More... A reboot is required when a change to this policy is delivered. To control this reboot, configure the following policies: Force Reboot on Update, Length of Each Reboot Delay, and Number of Reboot Delays Allowed.
Block Unmanaged Access to Domain Credentials	Not Selected	This policy prevents unmanaged users and applications from accessing the Windows domain credentials when a user is logged in.
Secure Windows Hibernation File	Not Selected	When this policy is selected, the hibernation file is encrypted only when the computer enters hibernation. The Encryption client disengages protection when the computer comes out of hibernation, providing protection without impacting users or applications while the computer is in use.
Prevent Unsecured Hibernation	Not Selected	When this policy is selected, the Encryption client does not allow computer hibernation if the client is unable to encrypt the hibernation data.
Scan Workstation on Logon	Not selected	When this policy is selected, all current and previously encrypted folders on the encrypted computer's local hard drives are scanned each time a managed user logs on, ensuring that all Common Encrypted Folders and User Encrypted Folders policy values are properly implemented. Abides by the Workstation Scan Priority policy.
Workstation Scan Priority		Highest, High, Normal, Low, Lowest Specifies the relative Windows priority of encrypted folder scanning. High and Highest prioritize scanning speed over computer responsiveness, Low and Lowest prioritize computer responsiveness over scanning speed and favor other resource-intensive activities, and Normal balances the two. The client checks for a changed Workstation Scan Priority before processing the next file. The scan priority levels are used in two ways. 1. These values correspond with the values used by the Microsoft SDK to set thread execution priority. 2. The client uses these values to introduce a delay in the encryption sweep after every single file is processed. The values translate to the following millisecond delay ranges, where the encryption thread will sit idle and then return full control to the operating system: Highest=0 ms / Lowest=100 ms
User Data Encryption Key	User	Common, User, User Roaming Choose a key to indicate who can access files encrypted by the following policies, and where: • User Encrypted Folders • Encrypt Outlook Personal folders • Encrypt Temporary Files (\Users\<Username>\AppData\Local\Temp only)

		• Encrypt Temporary Internet Files • Encrypt User Profile Documents (except \All Users\Shared Documents) Select: • Common for User Encrypted Folders to be accessible by all managed users on the computer where they were created (the same level of access as Common Encrypted Folders), and encrypted with the Common encryption algorithm. More... The Common encryption algorithm controls the encryption algorithm for all User Encrypted Folders and overrides any encryption algorithm selected, including the default User encryption algorithm. For example, if the Common encryption algorithm is set to AES 256, all Common and User Encrypted Files/Folders is encrypted with the AES 256 algorithm. All other encryption parameters can be selected to override default settings. For example, if the Encrypt Temporary Files policy is set to Not Selected, you can override this setting for any managed user by setting this value to Selected. Designated User Encrypted Folders use the Common Key, resulting in all managed users having the key to access any encrypted files stored in these folders as permitted by security settings on the operating system. • User for these files to be accessible only to the user who created them, only on the computer where they were created (the same level of access as User Encrypted Folders), and encrypted with the User Encryption Algorithm. • User Roaming for these files to be accessible only to the user who created them, on any encrypted Windows computer, and encrypted with the User encryption algorithm. When incorporating an encryption policy to encrypt entire disk partitions, Dell recommends using the default SDE policy, rather than Common or User. This ensures that any operating system files that are encrypted are accessible during times when the managed user is not logged in.
Policy Proxy Connections	String	String - maximum of 1500 characters List fully qualified Policy Proxy hostnames, or IP addresses, separated by carriage returns. Ports cannot be specified in this policy. More... Once a valid entry is found, the remainder of the Policy Proxies listed are ignored. Entries are processed in the following order: 1. GKConnections Override (this registry entry overrides all other entries) 2. GKConnections (this registry entry is set automatically by the client, based on the this policy) 3. GK To override this policy and specify ports via the registry key, set HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\CMGShield\GKConnectionsOverride. The client communicates with Policy Proxies using the GKPORT (the default is 8000). If necessary, change that port via the registry key HKLM\SOFTWARE\Microsoft\WindowsNT\Current Version\Winlogon\CMGShield\GKPort. Inherited values for this policy accumulate. For the client to connect to a Policy Proxy specified in this policy, it must be in the same group as the Policy Proxy specified during client installation. Because the client supports up to 255 users per computer, this policy is available only at the Enterprise policy level.
Policy Proxy	360	1-1440 minutes

Polling Interval		The interval that the Encryption client attempts to poll Policy Proxy for policy updates, and send inventory information to Policy Proxy. The Encryption client also attempts to poll Policy Proxy each time a user logs on.
Allow Activations	Selected	This policy is available at the Enterprise, Domain, User Group, and User levels. This policy is used only by the Encryption client. Other applications do not have an activation policy setting. When this policy is selected, Encryption client activations are allowed. When this policy is not selected, activations are blocked. Blocking activations is useful for staggering activations, preventing activations during the initial Dell Server setup, or preventing activations during a maintenance interruption.
Current Shield State	Activate	Activate, Suspend Activate is the normal state for an encrypted user. A user must be in this state to activate a computer. Select Suspend to require recovery before the user can access the computer. When a user is suspended, encrypted data cannot be accessed. The user can be recovered by changing this policy to Activate, and committing the policy.
See basic settings		
Enable Software Auto Updates	Not Selected	*Selected* *Not Selected* Selected enables the client update agent to automatically check for updates to Encryption client software. If this policy is not selected, Encryption client auto updates do not take place, regardless of other policy values. If this policy is selected, the On Premise Update Staging Location policy must have a network location in its value.
On Premise Update Staging Location	String	*String* This policy defines the network location (UNC) where the Dell Server stages Encryption client update packages. If a network location is not specified in this policy, the Enable Software Auto Updates policy should not be published.
Update Check Period	10080	*1-43200 minutes (1 minute to 30 days)* The period in minutes between checks for software auto updates.
Number of Policy Update Delays Allowed	3	0-5000 If Force Logoff/Reboot on Policy Updates is Selected, a non-zero value allows the user to delay the required logoff or reboot the specified number of times. Set to zero to disable delays.
Force Logoff / Reboot on Policy Updates	Selected	Selected requires either a logoff or a reboot in order for key policy updates to take effect. Otherwise, these policy updates take effect whenever the next logoff or reboot occurs.
Policy Viewer Enabled	Not Selected	When Selected, the user can view their encryption policies from the Encryption icon in the notification area.
Display Local Encryption Processing Control	Not Selected	When Selected, the user sees a menu option in the notification area icon that allows them to pause/resume encryption/decryption (depending on what the client is currently doing). **Important:** *Allowing a user to pause encryption could allow the user to prevent the Encryption client from fully encrypting or decrypting data per policy.*
Suppress File Contention Notification	Selected	This policy controls whether users see notification pop-ups if an application attempts to access a file while the client is processing it. More...

		If the client is processing a large file that an application needs, and this policy is Selected, it may appear that the application is unresponsive or slow to open (with no message indicating what the issue is). Care should be taken when using this policy.
Number of Encryption Processing Delays Allowed	0	0-5000 A non-zero value allows the user to delay any encryption processing required by the encryption policies you set, the specified number of times. Set to zero to disable delays.
Length of Each Encryption Processing Delay	5	5-40320 minutes If Number of Encryption Processing Delays Allowed has a non-zero value, use this policy to specify how often the user is prompted to continue with encryption processing or delay again. More... This prompt displays for five minutes each time. If the user does not respond to the prompt, encryption processing begins. The final delay prompt includes a countdown and progress bar, and it displays until the user responds, or the final delay expires and encryption processing begins. Calculate the maximum possible delay as follows (a maximum delay would involve the user responding to each delay prompt immediately prior to the 5-minute mark): (Number of Encryption Processing Delays Allowed x Length of Each Encryption Processing Delay) + (5 minutes x [Number of Encryption Processing Delays Allowed - 1])
Length of Each Policy Update Delay	15	5-40320 minutes If Number of Policy Update Delays Allowed has a non-zero value, use this policy to specify how often the user is prompted to logoff/reboot or delay again. More... This prompt displays for five minutes each time. If the user does not respond to the prompt, the next delay begins. The final delay prompt includes a countdown and progress bar, and it displays until the user responds, or the final delay expires and the required logoff/reboot occurs. You can change the behavior of the user prompt to begin or delay encryption, to prevent encryption processing following no user response to the prompt. To do this, set the registry key SnoozeBeforeSweep |(DWORD), stored in HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield, to a non-zero value. Any non-zero value will change the default behavior to snooze. With no user interaction, encryption processing is delayed up to the number of configurable allowed delays. When the final delay expires, encryption processing begins. Calculate the maximum possible delay as follows (a maximum delay would involve the user never responding to a delay prompt, each of which displays for 5 minutes): (Number of Policy Update Delays Allowed x Length of Each Policy Update Delay) + (5 minutes x [Number of Policy Update Delays Allowed - 1])
Force Reboot on Update	Selected	When selected, the computer immediately reboots to allow processing of encryption or updates related to device-based policy, such as System Data Encryption (SDE).
Length of Each Reboot Delay	15	5-40320 minutes The number of minutes to delay when the user chooses to delay reboot for device-based policy.
Number of Reboot Delays Allowed	3	0-5000 The number of times the user is allowed to delay reboot for device-based policy.
Allow	False	True, False, User-Optional

Encryption Processing Only When Screen is Locked		When True, there is no encryption or decryption of data while the user is actively working. The client will only process data when the workstation screen is locked. When False, encryption processing occurs any time, even while the user is working. User-Optional adds an option to the notification area icon allowing the user to turn this feature on or off. Enabling this option will significantly extend the amount of time it takes to complete encryption or decryption.
Hide Overlay Icons	Selected	When Selected, Encryption overlay icons is not present on encrypted files in File Explorer for all managed users on the computer.
Encrypt temporary files	Off	When Off SDE Common
See basic settings		
Policy	Default Setting	Description
BitLocker Encryption This technology manages Microsoft BitLocker policies for full disk and removable media encryption.		
Disable BitLocker on Self-Encrypting Drives	Selected	*Selected* *Not Selected* If Selected, BitLocker Manager does not start encryption on a volume that is already protected by a provisioned SED. For example, if this policy is Selected and both C: and D: are on one physical self-encrypting drive, and the PBA has been provisioned, then C: and D: does not encrypt for BitLocker even if System and Fixed drive encryption are turned on in the BitLocker Manager policies.
See basic settings		
BitLocker Encryption - Fixed Data Volume Settings		
Configure the Use of Smart Cards on Fixed Data Drives	Allow	*Allow* *Disallow* *Require* This policy specifies whether smart cards can be used to authenticate access to BitLocker fixed data drives. These settings are enforced when turning on BitLocker, not when unlocking a drive. BitLocker will allow unlocking a drive with any of the protectors available on the drive.
Deny Write Access to Fixed Data Drives Not Protected by BitLocker	Disabled	*Enabled* *Disabled* *Enabled for Organizations* If the drive is protected by BitLocker, it is mounted with read and write access. If you disable or do not configure this policy setting, all fixed data drives on the computer is mounted with read and write access. When Disabled, this policy element will force the option to be blocked from being used, and will not proceed until it is met. When Enabled, this policy element will force the option to be used, and will not proceed unless it is met.
Allow Access	Selected	*Selected*

to BitLocker Protected Fixed Data Drives from Earlier Versions of Windows		*Not Selected* When Selected, fixed data drives with the FAT file system can be unlocked and viewed on computers running Windows Server 2008. This policy does not apply to drives that are formatted with the NTFS file system. Set this policy to Selected and the Do Not Install BitLocker to Go Reader on FAT formatted Fixed Drives policy to Not Selected to allow BitLocker to Go Reader to be installed on the fixed drive.
Do Not Install BitLocker to Go Reader on FAT Formatted Fixed Drives	Not Selected	*Selected* *Not Selected* If this policy is Not Selected, BitLocker to Go Reader is installed on the fixed drive to enable users to unlock the drive on computers running Windows Server 2008. Set this policy to Not Selected and the Allow Access to BitLocker Protected Fixed Data Drives from Earlier Versions of Windows policy to Not Selected to allow BitLocker to Go Reader to be installed on the fixed drive.
Configure Use of Passwords for Fixed Data Drives	Allow	*Allow* *Require* *Disallow* When set to Require, a connection to a domain controller is necessary to validate the complexity of the password. When set to Allow, a connection to a domain controller is attempted to validate complexity, but if no domain controller is found, the password will still be accepted. When set to Do Not Allow, no password complexity validation is done. To use this policy, Configure Use of Passwords for Fixed Data Drives must be set to Allow or Require.
Configure Password Complexity for Fixed Data Drives	Allow	*Do Not Allow* *Require* *Allow* When set to Require, a connection to a domain controller is necessary to validate the complexity of the password. When set to Allow, a connection to a domain controller is attempted to validate complexity, but if no domain controller is found, the password will still be accepted. When set to Do Not Allow, no password complexity validation is done. To use this policy, Configure Use of Passwords for Fixed Data Drives must be set to Allow or Require.
Minimum Password Length for Fixed Data Drives	8	*8 min* *20 max* Passwords must be at least 8 characters. To configure a greater minimum length for the password enter the desired number of characters. To use this policy, Configure Use of Passwords for Fixed Data Drives must be set to Allow or Require.
Encryption Type for Fixed Data Drives	Full Encryption	*Full Encryption* *Used Space Only Encryption* Select the type of encryption to use for Fixed Data Drives.
Choose How BitLocker-protected Fixed Drives Can be Recovered	Not Selected	*Selected* *Not Selected* BitLocker drives can always be recovered with BitLocker Manager, even if this value is Not Selected. This policy allows for the control of how BitLocker protected fixed data drives are recovered in the absence of the required credentials. More... This policy is the parent policy to:

		Allow Data Recovery Agent for Protected Fixed Data Drives Config User Storage of BitLocker 48-digit Recovery Password Config User Storage of BitLocker 256-bit Recovery Key Omit Recovery Options from the BitLocker Setup Wizard Save BitLocker Recovery Info to AD DS for Fixed Data Drives BitLocker Recovery Info to Store in AD DS Do Not Enable BitLocker Until Recovery Info is Stored in AD DS for Fixed Data Drives
Allow Data Recovery Agent for Protected Fixed Data Drives	Selected	*Selected* *Not Selected* When Selected, a data recovery agent is allowed for use with BitLocker protected fixed data drives. Before the agent can be used, it must be added from the Public Key Policies in either the Group Policy Management Console or the Local Group Policy Editor. When setting this policy to Selected, the Choose How BitLocker-protected Fixed Drives Can be Recovered policy must also be set to Selected.
Configure User Storage of BitLocker 48-digit Recovery Password	Allow	*Allow* *Require* *Do Not Allow* This policy determines if a user is allowed, required, or not allowed to generate a 48-digit password. When setting this policy to Allow or Require, the Choose How BitLocker-protected Fixed Drives Can be Recovered policy must also be set to Selected.
Configure User Storage of BitLocker 256-bit Recovery Key	Allow	*Allow* *Require* *Do Not Allow* This policy determines if a user is allowed, required, or not allowed to generate a 256-bit recovery key. When setting this policy to Allow or Require, the Choose How BitLocker-protected Fixed Drives Can be Recovered policy must also be set to Selected.
Omit Recovery Options from the BitLocker Setup Wizard	Not Selected	*Selected* *Not Selected* When Selected, users are prevented from specifying recovery options when BitLocker is enabled. Recovery options for the drive are determined by policy settings. When setting this policy to Not Selected, the Choose How BitLocker-protected Fixed Drives Can be Recovered policy must also be set to Selected.
Save BitLocker Recovery Information to AD DS for Fixed Data Drives	Selected	*Selected* *Not Selected* Selected allows BitLocker recovery information to be stored in AD DS for fixed data drives. BitLocker recovery information is always saved to the Dell Serve. Enabling this policy additionally saves the information to AD. More... The appropriate schema extensions and access control settings on the domain must be first configured before AD DS backup can succeed. When setting this policy to Selected, the Choose How BitLocker-protected Fixed Drives Can be Recovered policy must also be set to Selected. Set this policy to Selected to use the policy BitLocker Recovery Information to Store in AD DS.
BitLocker Recovery Information to Store in AD DS	Recovery Passwords and Key Packages	*Recovery Passwords and Key Packages* *Recovery Passwords Only* This policy provides the option of storing recovery passwords and key packages, or storing the recovery password only in AD DS. The appropriate schema extensions and access control

		settings on the domain must be first configured before applying this policy. The Choose How BitLocker-protected Fixed Drives Can be Recovered policy must be set to Selected to use this policy. To use this policy, Save BitLocker Recovery Information to AD DS for Fixed Data Drives must be set to Selected.
Do Not Enable BitLocker Until Recovery Information is Stored in AD DS for Fixed Data Drives	Not Selected	*Selected* *Not Selected* Although BitLocker recovery information is automatically stored in the Dell Server this policy additionally requires BitLocker drive encryption recovery information to be stored in AD DS. The appropriate schema extensions and access control settings on the domain must be configured before using this policy. More... This policy is used to prevent users from enabling BitLocker unless the computer is connected to the domain and the backup of the BitLocker recovery information to AD DS has succeeded. The Choose How BitLocker-protected Fixed Drives Can be Recovered policy must be set to Selected to use this policy.
Configure Use of Hardware-Based Encryption for Fixed Data Drives	Selected	*Selected* *Not Selected* PARENT to the next 4 policies. Selected enables the configuration of hardware-based encryption on fixed data drives.
Use Hardware-Based Encryption for Fixed Data Drives	Selected	*Selected* *Not Selected* Selected enables hardware-based encryption for fixed data drives. To use this policy, Configure Use of Hardware-Based Encryption for Fixed Data Drives must be set to Selected.
Use BitLocker Software-Based Encryption on Fixed Data Drives When Hardware Encryption is Not Available	Selected	*Selected* *Not Selected* Selected enables BitLocker software-based encryption on fixed data drives if hardware-based encryption is not available. To use this policy, Configure Use of Hardware-Based Encryption for Fixed Data Drives must be set to Selected.
Restrict Crypto Algorithms and Cipher Suites Allowed for Hardware-Based Encryption on Fixed Data Drives	Not Selected	*Selected* *Not Selected* Selected allows only specific crypto algorithm and cipher suites for BitLocker hardware encryption on fixed data drives. To use this policy, Configure Use of Hardware-Based Encryption for Fixed Data Drives must be set to Selected.
Configure Specific Crypto Algorithms and Cipher Suites Settings on Fixed Data Drives	String	String - 2.16.840.1.101.3.4.1.2; 2.16.840.1.101.3.4.1.42 Set specific Crypto Algorithms and Cipher Suites on fixed data drives. To use this policy, Configure Use of Hardware-Based Encryption for Fixed Data Drives must be set to Selected.
See basic settings		
Bitlocker Encryption - Global Settings		
Default Folder Location to		Qualified path Important: This policy is not used by BitLocker Manager,

Save Recovery Password		because it does not prompt the user when saving recovery passwords. Microsoft defines this policy as: This setting provides the default path that is displayed when the BitLocker drive encryption setup wizard prompts the user to enter the location of a folder to save the recovery password. The text in this policy is translatable.
Encryption Method and Cipher Strength	AES 128 with Diffuser	*AES 128 with Diffuser* *AES 256 with Diffuser* *AES 128* *AES 256* This policy specifies the encryption method and cipher strength used for BitLocker drive encryption. Changing this policy has no effect if the drive is already encrypted or encryption is in progress.
Enable Organizational Unique Identifiers	Not Selected	*Selected* *Not Selected* This policy allows for the association of unique organizational identifiers to a new drive that is enabled with BitLocker. These identifiers are stored as the identification field and allowed identification field. The allowed identification field is used in combination with the Deny Write Access to Removable Drives Not Protected by BitLocker policy to help control the use of removable drives in the organization. This policy must be set to Selected to use the policies Set Organizational Unique Identifiers and Set Allowed Organizational Unique Identifiers.
Set Organizational Unique Identifiers		*Up to 260 characters* The identification field allows you to associate a unique organizational identifier to BitLocker-protected drives. This identifier is automatically added to new BitLocker-protected drives and can be updated on existing BitLocker-protected drives using the Manage-BDE command-line tool. An identification field is required for management of certificate-based data recovery agents on BitLocker-protected drives and for potential updates to the BitLocker To Go Reader. BitLocker will only manage and update data recovery agents when the identification field on the drive matches the value configured in the identification field. In a similar manner, BitLocker will only update BitLocker To Go Reader when the identification field on the drive matches the value configured for the identification field. To use this policy, Enable Organizational Unique Identifiers must be set to Selected.
Set Allowed Organizational Unique Identifiers		*Up to 260 characters* The allowed identification field is used in combination with the Deny Write Access to Removable Drives Not Protected by BitLocker policy to help control the use of removable drives in the organization. It is a comma separated list of identification fields from your organization or other external organizations. To use this policy, Enable Organizational Unique Identifiers must be set to Selected.
Prevent Memory Overwrite on Restart	Not Selected	*Selected* *Not Selected* Selected prevents memory from being overwritten on restart. Preventing memory overwrite may improve restart performance, but will increase the risk of exposing BitLocker secrets. When Not Selected, BitLocker secrets are removed from memory when the computer restarts.
Enable Smart	Not Selected	*Selected*

Card Certificate Identifier		*Not Selected* This policy allows or denies an object identifier to be specified for enhanced key usage with a certificate. This policy must be set to Selected to use the policy Smart Card Certificate Identifier.
Smart Card Certificate Identifier	1.3.6.1.4.1.311.67.1.1	*1.3.6.1.4.1.311.67.1.1* This policy provides for an object identifier to be specified for enhanced key usage with a certificate. BitLocker can identify which certificates may be used to authenticate a user certificate to a BitLocker drive by matching the object identifier in the certificate with the object identifier that is defined by this policy. Use caution if changing the default value. To use this policy, Enable Smart Card Certificate Identifier must be set to Selected.
See basic settings		
Bitlocker Encryption - Operating System Volume Settings		
Allow Enhanced PINs for Startup	Not Selected	*Selected* *Not Selected* Selected allows enhanced startup PINs to be used with BitLocker. Enhanced startup PINs permit the use of characters including uppercase and lowercase letters, symbols, numbers, and spaces. This policy setting is applied when you turn on BitLocker.
Number of Characters Required in PIN	4	*4-20 digits* This policy configures the minimum length for a TPM startup PIN. The startup PIN must have a minimum length of 4 digits and can have a maximum of 20 digits.
Allow Network Unlock at Startup on Operating System Drives	Not Selected	*Selected* *Not Selected* This policy specifies if a user is allowed to use the Network Unlock at Startup feature on operating system drives.
Allow SecureBoot on Operating System Drives	Selected	*Selected* *Not Selected* This policy specifies if a user is allowed to use SecureBoot on operating system drives.
Disallow Standard Users from Changing the PIN on Operating System Drives	Not Selected	*Selected* *Not Selected* This policy specifies if a standard user is allowed to change their PIN on operating system drives.
Enable Use of Preboot Keyboard Input on Slates	Not Selected	*Selected* *Not Selected* This policy specifies if a preboot keyboard input is enabled on Slates.
Reset Platform Validation Data After Recovery	Not Selected	*Selected* *Not Selected* This policy specifies if a preboot keyboard input is enabled on Slates.
Choose How BitLocker-protected Operating System Drives Can be Recovered	Not Selected	*Selected* *Not Selected* BitLocker drives can always be recovered with BitLocker Manager, even if this value is Not Selected. For the GPO, a Selected value allows you to specify how BitLocker drives are recovered. More... This policy is the parent policy to: Allow Data Recovery Agent for Protected Operating System Drives

		Configure User Storage of BitLocker 48-digit Recovery Password Configure User Storage of BitLocker 256-bit Recovery Key Omit Recovery Options from the BitLocker Setup Wizard Save BitLocker Recovery Info to AD DS for Operating System Drives BitLocker Recovery Information to Store in AD DS (Windows Server 2008 Only) Do Not Enable BitLocker Until Recovery Information is Stored in AD DS for Operating System Drives
Allow Data Recovery Agent for Protected Operating System Drives	Selected	*Selected* *Not Selected* The "Allow Certificate Based Data Recovery Agent" is used to specify whether a data recovery agent can be used with BitLocker operating system drives. Before a data recovery agent can be used, it must be added from the Public Key policies in either the Group Policy Management Console or the Local Group Policy Editor. To use this policy, Choose How BitLocker-protected Operating System Drives Can be Recovered must be set to Selected.
Configure User Storage of BitLocker 48-digit Recovery Password	Allow	*Do Not Allow* *Require* *Allow* This policy configures if a user is allowed, required, or not allowed to generate a 48-digit password. To use this policy, Choose How BitLocker-protected Operating System Drives Can be Recovered must be set to Selected.
Configure User Storage of BitLocker 256-bit Recovery Key	Allow	*Do Not Allow* *Require* *Allow* This policy configures if a user is allowed, required or not allowed to generate a 256-bit recovery key. To use this policy, Choose How BitLocker-protected Operating System Drives Can be Recovered must be set to Selected.
Omit Recovery Options from the BitLocker Setup Wizard	Not Selected	*Selected* *Not Selected* When Selected, users are prevented from specifying recovery options when BitLocker is enabled. Recovery options for the drive are determined by policy settings. To use this policy, Choose How BitLocker-protected Operating System Drives Can be Recovered must be set to Selected.
Save BitLocker Recovery Information to AD DS for Operating System Drives	Selected	*Selected* *Not Selected* Selected allows BitLocker recovery information to be stored in AD DS for operating system drives. The appropriate schema extensions and access control settings on the domain must be first configured before AD DS backup can succeed. To use this policy, Choose How BitLocker-protected Operating System Drives Can be Recovered must be set to Selected.
BitLocker Recovery Information to Store in AD DS (Windows Server 2008 Only)	Recovery Passwords and Key Packages	*Recovery Passwords and Key Packages* *Recovery Passwords Only* This policy provides the option of storing recovery passwords and key packages, or storing the recovery password only in AD DS. The appropriate schema extensions and access control settings on the domain must be first configured before applying this policy. This policy is applicable only to computers running Windows Server 2008. To use this policy, Choose How BitLocker-protected Operating System Drives Can be Recovered must be set to Selected.
Do Not Enable BitLocker Until Recovery	Not Selected	*Selected* *Not Selected* Although BitLocker recovery information is automatically

Information is Stored in AD DS for Operating System Drives		stored in the Dell Server, this policy additionally requires BitLocker drive encryption recovery information to be stored in AD DS. The appropriate schema extensions and access control settings on the domain must be configured before using this policy. This policy is used to prevent users from enabling BitLocker unless the computer is connected to the domain and the backup of the BitLocker recovery information to AD DS has succeeded. To use this policy, Choose How BitLocker-protected Operating System Drives Can be Recovered must be set to Selected.
Configure Use of Hardware-Based Encryption for Operating System Drives	Selected	*Selected* *Not Selected* PARENT to the next 4 policies. Selected enables the configuration of hardware-based encryption on operating system drives.
Use Hardware-Based Encryption for Operating System Drives	Selected	*Selected* *Not Selected* Selected enables hardware-based encryption on operating system drives. To use this policy, Configure Use of Hardware-Based Encryption for Operating System Drives must be set to Selected.
Use BitLocker Software-Based Encryption on Operating System Drives When Hardware Encryption is Not Available	Selected	*Selected* *Not Selected* Selected enables BitLocker software-based encryption on operating system drives if hardware-based encryption is not available. To use this policy, Configure Use of Hardware-Based Encryption for Operating System Drives must be set to Selected.
Restrict Crypto Algorithms and Cipher Suites Allowed for Hardware-Based Encryption on Operating System Drives	Not Selected	*Selected* *Not Selected* Selected allows only specific crypto algorithm and cipher suites for BitLocker hardware encryption on operating system drives. To use this policy, Configure Use of Hardware-Based Encryption for Operating System Drives must be set to Selected.
Configure Specific Crypto Algorithms and Cipher Suites Settings on Operating System Drives	2.16.840.1.101.3.4.1.2;2.16.840.1.101.3.4.1.42	*String -* *2.16.840.1.101.3.4.1.2;* *2.16.840.1.101.3.4.1.42* Specific Crypto Algorithms and Cipher Suites allowed on operating system drives. To use this policy, Configure Use of Hardware-Based Encryption for Operating System Drives must be set to Selected.
Encryption Type for Operating System Drives	Full Encryption	*Full Encryption* *Used Space Only Encryption* Select the type of encryption to use for operating system drives.
Configure Use of Passwords for Operating System Drives	Not Configured	*Enabled* *Disabled* *Not Configured* Configure password requirements for Operating System Drives. When Disabled, this policy element will force the option to be blocked from being used, and will not proceed until it is met. When Enabled, this policy element will force the option to be used, and will not proceed unless it is met. When Not Configured, this policy element will consume the default action to do nothing.

Configure Password Complexity for Operating System Drives	Allow	*Allow* *Require* *Do Not Allow* When set to Require, a connection to a domain controller is necessary to validate the complexity of the password. When set to Allow, a connection to a domain controller is attempted to validate complexity, but if no domain controller is found, the password will still be accepted. When set to Do Not Allow, no password complexity validation is done. To use this policy, Configure Use of Passwords for Operating System Drives must be set to Enabled.
Minimum Password Length for Operating System Drives	8	*8-256* The default value is a password length of 8 characters. 8-256 characters are allowed. To use this policy, Configure Use of Passwords for Operating System Drives must be set to Enabled.
Require ASCII-Only Passwords for Operating System Drives	Not Selected	*Selected* *Not Selected* Require ASCII-only passwords for operating system drives to create stronger passwords. To use this policy, Configure Use of Passwords for Operating System Drives must be set to Enabled.
Use Enhanced Boot Configuration Data Profile	Disabled	*Enabled* *Disabled* *Not Configured* Set this policy to Enable to allow the verification and exclusion of BCD settings. When Disabled, this policy element will force the option to be blocked from being used, and will not proceed until it is met. When Enabled, this policy element will force the option to be used, and will not proceed unless it is met. When Not Configured, this policy element will consume the default action to do nothing.
Verify Additional BCD Settings	String	*String* Specify the additional Boot Configuration settings. To use this policy, Use Enhanced Boot Configuration Data Profile must be set to Enabled.
Exclude Additional BCD Settings	String	*String* Exclude specific Boot Configuration settings. To use this policy, Use Enhanced Boot Configuration Data Profile must be set to Enabled.
Configure TPM Platform Validation Profile	Not Selected	*Selected* *Not Selected* Set to Selected to enable boot up TPM drive unlocking for Windows 7 and Windows Server 2008 R2. Selected allows the configuration of how the TPM security hardware secures the BitLocker encryption key. This policy does not apply if the computer does not have a compatible TPM or if BitLocker has already been turned on with TPM protection. This policy must be set to Selected to use the policy Configure Specific TPM Platform Settings. See http://technet.microsoft.com/en-us/library/jj679890.aspx#BKMK_depopt3 for more information.
Configure Specific TPM Platform Settings	PCR0,on PCR1,off PCR2,on PCR3,off PCR4,on PCR5,on PCR6,off PCR7,off	This policy allows you to configure how the computer's TPM security hardware secures the BitLocker encryption key. This policy setting does not apply if the computer does not have a compatible TPM or if BitLocker has already been turned on with TPM protection. This setting determines what values the TPM measures when it validates early boot components before unlocking a drive on a computer running Windows 7 or Windows Server 2008 R2.

	PCR8,on PCR9,on PCR10,on PCR11,on PCR12,off PCR13,off PCR14,off PCR15,off PCR16,off PCR17,off PCR18,off PCR19,off PCR20,off PCR21,off PCR22,off PCR23,off	More... If you enable this policy before turning on BitLocker, you can configure the boot components that the TPM will validate before unlocking access to the BitLocker-encrypted operating system drive. If any of these components change while BitLocker protection is in effect, the TPM does not release the encryption key to unlock the drive and the computer will instead display the BitLocker recovery console and require that either the recovery password or recovery key be provided to unlock the drive. If you disable or do not configure this policy, the TPM uses the default platform validation profile or the platform validation profile specified by the setup script. A platform validation profile consists of a set of Platform Configuration Register (PCR) indices ranging from 0 to 23. The default platform validation profile secures the encryption key against changes to the Core Root of Trust of Measurement (CRTM), BIOS, and Platform Extensions (PCR 0), the Option ROM Code (PCR 2), the Master Boot Record (MBR) Code (PCR 4), the NTFS Boot Sector (PCR 8), the NTFS Boot Block (PCR 9), the Boot Manager (PCR 10), and the BitLocker Access Control (PCR 11). The descriptions of PCR settings for computers that use an Extensible Firmware Interface (EFI) are different than the PCR settings described for computers that use a standard BIOS. The BitLocker Drive Encryption Deployment Guide on Microsoft TechNet contains a complete list of PCR settings for both EFI and standard BIOS. **Caution:** Changing from the default platform validation profile affects the security and manageability of your computer. BitLocker's sensitivity to platform modifications (malicious or authorized) is increased or decreased depending upon inclusion or exclusion (respectively) of the PCRs. To use this policy, Configure TPM Platform Validation Profile must be set to True.
Configure BIOS TPM Platform Validation Profile	Not Selected	Selected Not Selected Set to Selected to enable boot up BIOS TPM drive unlocking. Selected allows the configuration of how the BIOS TPM security hardware secures the BitLocker encryption key. This policy does not apply if the computer does not have a compatible TPM or if BitLocker has already been turned on with TPM protection. This policy must be set to Selected to use the policy Configure Specific BIOS TPM Platform Settings. See http://technet.microsoft.com/en-us/library/jj679890.aspx#BKMK_tpmbios for more information.
Configure Specific BIOS TPM Platform Settings	PCR0,on PCR1,off PCR2,on PCR3,off PCR4,on PCR5,off PCR6,off PCR7,off PCR8,on PCR9,on PCR10,on PCR11,on PCR12,off PCR13,off PCR14,off PCR15,off PCR16,off	This policy setting allows you to configure how the computer's TPM security hardware secures the BitLocker encryption key. This setting determines what values the TPM measures when it validates early boot components before unlocking an operating system drive on a computer with BIOS configuration or with UEFI firmware that has the Compatibility Support Module (CSM) enabled. If you enable this policy before turning on BitLocker, you can configure the boot components that the TPM will validate before unlocking access to the BitLocker-encrypted operating system drive. If any of these components change while BitLocker protection is in effect, the TPM does not release the encryption key to unlock the drive and the computer will instead display the BitLocker recovery console and require that either the recovery password or recovery key be provided to unlock the drive. To use this policy, Configure BIOS TPM Platform Validation

	PCR17,off PCR18,off PCR19,off PCR20,off PCR21,off PCR22,off PCR23,off	Profile must be set to Selected.
Configure UEFI TPM Platform Validation Profile	Not Selected	*Selected* *Not Selected* Set to Selected to enable boot up UEFI TPM drive unlocking. Selected allows the configuration of how the UEFI TPM security hardware secures the BitLocker encryption key. This policy does not apply if the computer does not have a compatible TPM or if BitLocker has already been turned on with TPM protection. This policy must be set to Selected to use the policy Configure Specific UEFI TPM Platform Settings. See http://technet.microsoft.com/en-us/library/jj679890.aspx#BKMK_tpmvaluefi for more information.
Configure Specific UEFI TPM Platform Settings	PCR0,on PCR1,off PCR2,on PCR3,off PCR4,on PCR5,off PCR6,off PCR7,off PCR8,off PCR9,off PCR10,off PCR11,on PCR12,off PCR13,off PCR14,off PCR15,off PCR16,off PCR17,off PCR18,off PCR19,off PCR20,off PCR21,off PCR22,off PCR23,off	This policy setting allows you to configure how the computer's TPM security hardware secures the BitLocker encryption key. This setting determines what values the TPM measures when it validates early boot components before unlocking an operating system drive on a computer with native UEFI firmware configurations. If you enable this policy before turning on BitLocker, you can configure the boot components that the TPM will validate before unlocking access to the BitLocker-encrypted operating system drive. If any of these components change while BitLocker protection is in effect, the TPM does not release the encryption key to unlock the drive and the computer will instead display the BitLocker recovery console and require that either the recovery password or recovery key be provided to unlock the drive. To use this policy, Configure UEFI TPM Platform Validation Profile must be set to Selected.
See basic settings		
Bitlocker Encryption - Removable Storage Settings		
Allow User to Apply BitLocker Protection on Removable Drives	Selected	*Selected* *Not Selected* When Selected, users are permitted to run the BitLocker setup wizard on a removable data drive.
Allow User to Suspend and Decrypt BitLocker Protection on Removable Data Drives	Selected	*Selected* *Not Selected* When Selected, users are authorized to suspend and decrypt BitLocker protection on removable data drives.
Configure Use of Smart Cards on Removable	Allow	*Allow* *Disallow* *Require*

Data Drives		This policy specifies whether smart cards can be used to authenticate access to BitLocker removable data drives. These settings are enforced when turning on BitLocker, not when unlocking a drive. BitLocker will allow unlocking a drive with any of the protectors available on the drive.
Deny Write Access to Removable Drives Not Protected by BitLocker	Disabled	*Enabled* *Disabled* *Enabled for Organization* If this policy is enabled, all removable drives that are not BitLocker protected are mounted as read only. If this policy is disabled, all removable drives on the computer are mounted with read and write access.
Allow Access to BitLocker Protected Removable Data Drives from Earlier Versions of Windows	Selected	*Selected* *Not Selected* When Selected, removable data drives with the FAT file system can be unlocked on computers running Windows Server 2008. This policy does not apply to drives that are formatted with the NTFS file system.
Do Not Install BitLocker to Go Reader on FAT formatted Removable Drives	Not Selected	*Selected* *Not Selected* If this policy is Not Selected, removable data drives formatted with the FAT file system that are BitLocker protected cannot be unlocked on computers running Windows Server 2008. Bitlockertogo.exe is not installed.
Configure Use of Passwords for Removable Data Drives	Allow	*Allow* *Require* *Do No Allow* This policy specifies whether a password is required to unlock BitLocker removable data drives. These settings allow the use of a password, require the use of a password, or disallow the use of a password. This policy must be set to Allow or Require to use the Configure Password Complexity for Removable Data Drives and Minimum Password Length for Removable Data Drives polices.
Configure Password Complexity for Removable Data Drives	Allow	*Allow* *Require* *Do Not Allow* When set to Require, a connection to a domain controller is necessary to validate the complexity of the password. When set to Allow, a connection to a domain controller is attempted to validate complexity, but if no domain controller is found, the password will still be accepted. When set to Do Not Allow, no password complexity validation is done. To use this policy, Configure Use of Passwords for Removable Data Drives must be set to Allow or Require.
Minimum Password Length for Removable Data Drives	8	*8-20 characters* Passwords must be at least 8 characters in length, with a maximum of 20 characters. To use this policy, Configure Use of Passwords for Removable Data Drives must be set to Allow or Require.
Encryption Type for Removable Data Drives	Full Encryption	*Allow User to Choose* *Full Encryption* *Used Space Only Encryption* Select the type of encryption to use for Removable Data Drives.
Choose How BitLocker-protected Removable Drives Can be	Not Selected	*Selected* *Not Selected* BitLocker drives can always be recovered with BitLocker Manager, even if this value is Not Selected. This policy allows for the control of how BitLocker protected removable

Recovered		data drives are recovered in the absence of the required credentials. More... This policy is the parent policy to: Allow Data Recovery Agent for Protected Removable Data Drives Configure User Storage of BitLocker 48-digit Recovery Password Configure User Storage of BitLocker 256-bit Recovery Key Omit Recovery Options from the BitLocker Setup Wizard for Removable Media Save BitLocker Recovery Information to AD DS for Removable Data Drives BitLocker Recovery Info to Store in AD DS for Removable Data Drives Do Not Enable BitLocker Until Recovery Info is Stored in AD DS for Rem Data Drives
Allow Data Recovery Agent for Protected Removable Data Drives	Selected	*Selected* *Not Selected* When Selected, a data recovery agent is allowed for use with BitLocker protected removable data drives. Before the agent can be used, it must be added from the Public Key Policies in either the Group Policy Management Console or the Local Group Policy Editor. To use this policy, Choose How BitLocker-protected Removable Drives Can be Recovered must be to Selected.
Configure User Storage of BitLocker 48-digit Recovery Password	Allow	*Allow* *Require* *Do Not Allow* This policy configures if a user is allowed, required, or not allowed to generate a 48-digit password. To use this policy, Choose How BitLocker-protected Removable Drives Can be Recovered must be to Selected.
Configure User Storage of BitLocker 256-bit Recovery Key	Allow	*Allow* *Require* *Do Not Allow* This policy configures if a user is allowed, required, or not allowed to generate a 256-bit recovery key. To use this policy, Choose How BitLocker-protected Removable Drives Can be Recovered must be to Selected.
Omit Recovery Options from the BitLocker Setup Wizard for Removable Media	Not Selected	*Selected* *Not Selected* When Selected, users are prevented from specifying recovery options when BitLocker is enabled. Recovery options for the drive are determined by policy settings. To use this policy, Choose How BitLocker-protected Removable Drives Can be Recovered must be to Selected.
Save BitLocker Recovery Information to AD DS for Removable Data Drives	Selected	*Selected* *Not Selected* Selected allows BitLocker recovery information to be stored in AD DS for removable data drives. The appropriate schema extensions and access control settings on the domain must be first configured before AD DS backup can succeed. To use this policy, Choose How BitLocker-protected Removable Drives Can be Recovered must be to Selected. Set this policy to Selected to use the policy BitLocker Recovery Information to Store in AD DS for Removable Data Drives.
BitLocker Recovery Information to Store in AD DS for Removable Data Drives	Recovery Passwords and Key Packages	*Recovery Passwords and Key Packages* *Recovery Passwords Only* This policy provides the option of storing recovery passwords and key packages, or storing the recovery password only in AD DS. The appropriate schema extensions and access control settings on the domain must be first configured before

		applying this policy. To use this policy, Choose How BitLocker-protected Removable Drives Can be Recovered must be to Selected. To use this policy, Save BitLocker Recovery Information to AD DS for Removable Data Drives must be set to Selected.
Do Not Enable BitLocker Until Recovery Information is Stored in AD DS for Removable Data Drives	Not Selected	*Selected* *Not Selected* Although BitLocker recovery information is automatically stored in the Dell Server, this policy additionally requires BitLocker drive encryption recovery information to be stored in AD DS. The appropriate schema extensions and access control settings on the domain must be configured before using this policy. This policy is used to prevent users from enabling BitLocker unless the computer is connected to the domain and the backup of the BitLocker recovery information to AD DS has succeeded. To use this policy, Choose How BitLocker-protected Removable Drives Can be Recovered must be to Selected.
Configure Use of Hardware-Based Encryption for Removable Data Drives	Selected	*Selected* *Not Selected* PARENT to the next 4 policies. Selected enables the configuration of hardware-based encryption on removable data drives.
Use Hardware-Based Encryption for Removable Data Drives	Selected	*Selected* *Not Selected* Selected enables hardware-based encryption on removable data drives. To use this policy, Configure Use of Hardware-Based Encryption for Removable Data Drives must be set to Selected.
Use BitLocker Software-Based Encryption on Removable Data Drives When Hardware Encryption is Not Available	Selected	*Selected* *Not Selected* Selected enables BitLocker software-based encryption on removable data drives if hardware-based encryption is not available. To use this policy, Configure Use of Hardware-Based Encryption for Removable Data Drives must be set to Selected.
Restrict Crypto Algorithms and Cipher Suites Allowed for Hardware-Based Encryption on Removable Data Drives	Not Selected	*Selected* *Not Selected* Selected allows only specific crypto algorithm and cipher suites for BitLocker hardware encryption. To use this policy, Configure Use of Hardware-Based Encryption for Removable Data Drives must be set to Selected.
Configure Specific Crypto Algorithms and Cipher Suites Settings on Removable Data Drives	2.16.840.1.101.3.4.1.2;2.16.840.1.101.3.4.1.42	*String -* *2.16.840.1.101.3.4.1.2;* *2.16.840.1.101.3.4.1.42* Specific Crypto Algorithms and Cipher Suites allowed. To use this policy, Configure Use of Hardware-Based Encryption for Removable Data Drives must be set to Selected.
See basic settings		

Policy	Default Setting	Description
Server Encryption		

This technology manages Dell's data centric encryption using certificate-based authentication instead of the typical user-based authentication instead of the typical user-based authentication. This technology allows for protection of devices such as Windows Servers that do not commonly have users logged in.		
Server Encryption	Off	*On* *Off* This policy enables or disables System Data Encryption (SDE) and Common encryption on the client server. Changing the value of this policy triggers a new sweep to encrypt/decrypt files.
Allow Software Server Encryption	Selected	*Selected* *Not Selected* If this policy is Selected, client servers are activated at the Enterprise level. This policy may be set to Not Selected to block activations during initial Dell Server setup and maintenance interruptions.
Max Network Failed Attempts	3	*1-10* Number of successive failed attempts for a client server to connect to the Dell Server before encryption keys are locked.
Retry Interval to connect to Dell Server	5	*1-60 minutes* Time interval for the client server to attempt to connect to the Dell Server.
Retry if Authentication Fails Upon Network Failure	Selected	*Selected* *Not Selected* If Selected, the client server continues to attempt to contact the Dell Server if the first attempt fails due to a network failure.
Retry Interval Upon Network Failure	10	*10-60 minutes* The length of time between attempts to contact the Dell Server if the first attempt fails due to a network failure. The *Retry if Authentication Fails Upon Network Failure* policy must be set to Selected for this policy to be enforced.
Server Maintenance Schedule	Not Selected	This policy must be selected to use all other Server Maintenance policies. If this policy is Not Selected, no Server Maintenance policies are enforced, regardless of other policy values. Selected allows a maintenance schedule to control application of policy that requires a reboot.
Server Maintenance Schedule Repeats	Weekly	*Daily, Weekly, Monthly, Quarterly, Annually* The schedule configuration defines when the task should run. Daily: Runs the task every day at the specified Server Maintenance Schedule Start Time. Weekly: Runs the task weekly on the days specified in Server Maintenance Day of the Week. Monthly: Runs the task monthly on the specified Server Maintenance Day of the Month. Quarterly: Runs the task quarterly on the specified Server Maintenance Day of the Month. Annually: Runs the task annually on the specified Server Maintenance Day of the Month.
Server Maintenance Schedule Start Time	21:00	Format is HH:mm. Example: 23:59 The time the task should run.
Server Maintenance Day of the Week	Saturday	*Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday* The day of the week the task should run.
Server Maintenance Day of the	1	*1-31* The day of the month the task should run. Example: 17.

Month		
Infinite Suppress	Not Selected	When Selected, an automatic reboot is suppressed indefinitely.
Port Control System	Disabled	Enable or Disable all Port Control System policies. If this policy is set to Disable, no Port Control System policies are applied, regardless of other Port Control System policies. **All PCS policies require a reboot before the policy takes effect.**
Port: Express Card Slot	Enabled	Enable, Disable, or Bypass ports exposed through the Express Card Slot.
Port: USB	Enabled	Enable, Disable, or Bypass port access to external USB ports. **Note:** USB port-level blocking and HID class-level blocking is **only** honored if we can identify the computer chassis as a laptop/notebook form-factor. We rely on the computer's BIOS for the identification of the chassis.
Port: eSATA	Enabled	Enable, Disable, or Bypass port access to external SATA ports.
Port: PCMCIA	Enabled	Enable, Disable, or Bypass port access to PCMCIA ports.
Port: Firewire (1394)	Enabled	Enable, Disable, or Bypass port access to external Firewire (1394) ports.
Port: SD	Enabled	Enable, Disable, or Bypass port access to SD card ports.
Port: Memory Transfer Device (MTD)	Enabled	Enable, Disable, or Bypass access to Memory Transfer Device (MTD) ports.
Class: Storage	Enabled	PARENT to the next 3 policies. Set this policy to Enabled to use the next 3 Subclass Storage polices. Setting this policy to Disabled disables all 3 Subclass Storage policies - no matter what their value.
Subclass Storage: External Drive Control	Full Access	CHILD of Class: Storage. Class: Storage must be set to Enabled to use this policy. This policy interacts with the EMS Access to unShielded Media policy. If you intend to have Full Access to media, also set this policy to Full Access to ensure that the media is not set to read only and the port is not blocked. Full Access: External drive port does not have read/write data restrictions applied Read Only: Allows read capability /write data is disabled Blocked: Port is blocked from read/write capability This policy is endpoint-based and cannot be overridden by user policy.
Subclass Storage: Optical Drive Control	UDF Only	CHILD of Class: Storage. Class: Storage must be set to Enabled to use this policy. Full Access: Optical Drive port does not have read/write data restrictions applied UDF Only: Blocks all data writes that are not in the UDF format (CD/DVD burning, ISO burning). Read data is enabled. Read Only: Allows read capability. Write data is disabled Blocked: Port is blocked from read/write capability This policy is endpoint-based and cannot be overridden by user policy. Universal Disk Format (UDF) is an implementation of the specification known as ISO/IEC 13346 and ECMA-167 and is an open vendor-neutral file system for computer data storage for a broad range of media. To encrypt data written to CD/DVD media: Set EMS Encrypt External Media = Selected, EMS Exclude CD/DVD Encryption = Not Selected, and Storage Class: Optical Drive Control = UDF Only.
Subclass Storage: Floppy Drive Control	Read Only	CHILD of Class: Storage. Class: Storage must be set to Enabled to use this policy. Full Access: Floppy Drive port does not have read/write data restrictions applied

		Read Only: Allows read capability. Write data is disabled Blocked: Port is blocked from read/write capability This policy is endpoint-based and cannot be overridden by user policy.
Class: Windows Portable Device (WPD)	Enabled	PARENT to the next policy. Set this policy to Enabled to use the Subclass Windows Portable Device (WPD): Storage policy. Setting this policy to Disabled disables the Subclass Windows Portable Device (WPD): Storage policy - no matter what its value. Control access to all Windows Portable Devices.
Subclass Windows Portable Device (WPD): Storage	Full Access	CHILD of Class: Windows Portable Device (WPD) . Class: Windows Portable Device (WPD) must be set to Enabled to use this policy. Full Access: Port does not have read/write data restrictions applied. Read Only: Allows read capability. Write data is disabled. Blocked: Port is blocked from read/write capability.
Class: Human Interface Device (HID)	Enabled	Control access to all Human Interface Devices (keyboards, mice). **Note:** USB port-level blocking and HID class-level blocking is **only** honored if we can identify the computer chassis as a laptop/notebook form-factor. We rely on the computer's BIOS for the identification of the chassis.
Class: Other	Enabled	Control access to all devices not covered by other Classes.
EMS Encrypt External Media	Not Selected	This policy must be selected to use all other removable media policies. Not Selected means that no encryption of removable media takes place, regardless of other removable media policy values.
EMS Exclude CD/DVD Encryption	Not Selected	Not Selected encrypts CD/DVD devices.
EMS Access to unShielded Media	Read Only	*Block, Read Only, Full Access* Note that this policy interacts with the Storage > Subclass Storage: External Drive Control policy. If you intend to set this policy to Full Access, ensure that Subclass Storage: External Drive Control is not set to Read Only or Blocked. More... When this policy is set to Block Access, you have no access to removable media unless it is encrypted. Choosing either Read-Only or Full Access allows you to decide what removable media to encrypt. If you choose not to encrypt removable media and this policy is set to Full Access, you have full read/write access to removable media. If you choose not to encrypt removable media and this policy is set to Read-Only, you can read or delete existing files on the unencrypted media, but files cannot be edited on, or added to, the media .
EMS Encryption Algorithm	AES256	*AES 256, AES 128, 3DES* Encryption algorithm used to encrypt removable media. Encryption algorithms in order of speed, fastest first, are AES 128, AES 256, 3DES.
EMS Automatic Authentication	Disabled	*Disabled, Local, Roaming* Local automatic authentication allows the encrypted media to be automatically authenticated when inserted in the originally encrypting computer when the owner of that media is logged in. When local automatic authentication is disabled, users must always manually authenticate to access encrypted media. Not selecting roaming automatic authentication helps to prevent users from forgetting their password when they take the media home or share it with a colleague. Not selecting roaming automatic authentication also promotes a sense of

		awareness from a security perspective for users that the data being written to that media is protected. When set to Roaming, the owner of the removable media is automatically authenticated if logged into a computer other than the one where the media was encrypted and the computer is running either the full Encryption client or EMS Service.
EMS Scan External Media	Not Selected	Selected allows removable media to be scanned every time it is inserted. When this policy is Not Selected and the EMS Encrypt External Media policy is Selected, only new and changed files are encrypted. See EMS Encryption Rules if changing this policy to Selected. Do not enable this policy without applying EMS Encryption Rules also. More... A scan occurs at every insertion so that any files added to the removable media without authenticating can be caught. Files can be added to the media if authentication is declined, but encrypted data cannot be accessed. The files added are not encrypted in this case, so the next time the media is authenticated (to work with encrypted data), any files that may have been added are scanned and encrypted.
EMS Access Encrypted Data on unShielded Device	Selected	Selected allows the user to access encrypted data on removable media whether the endpoint is encrypted or not. More... When this policy is Not Selected, the user can work with encrypted data when logged on to any encrypted device, regardless of the Dell Server the user activated against. The user cannot work with encrypted data using any unencrypted device.
EMS Device Whitelist		*String - Maximum of 150 devices with a maximum of 500 characters per PNPDeviceID. Maximum of 2048 total characters allowed. "Space" and "Enter" characters count in the total characters used.* This policy allows the specification of removable media devices to exclude from encryption [using the device's Plug and Play device identifier (PNPDeviceID)], thereby allowing users full access to the specified removable media devices. More... This policy is available on an Enterprise, Domain, Group, and User level. Note that local settings override inherited settings. If a user is in more than one group, all EMS Device Whitelist entries, across all Groups, apply. This policy is particularly useful when using removable media devices which provide hardware encryption. However, this policy should be used with caution. This policy does not check whether external media devices on this list provide hardware encryption. Whitelisting removable storage devices that do not have hardware encryption do not have enforced security and are not protected. *For example, the Kingston® DataTraveler® Vault Privacy model enforces that encryption is enabled to use the device. However, the Kingston DataTraveler Vault model has an unsecured partition and a secured partition. Because it is the same physical removable media device with only one PNPDeviceID, the two partitions cannot be distinguished, meaning that whitelisting this particular device would allow unencrypted data to leave the endpoint.* *Additionally, if a removable media device is encrypted and is subsequently added to the EMS Device Whitelist policy, it remains encrypted and requires a reformat of the device to remove encryption.* The following is an example of a PNPDeviceID, which contains

		the manufacturer identifier, product identifier, revision, and hardware serial number: USBSTOR\DISK&VEN_KINGSTON &PROD_DTVAULT_PRIVACY& REV_104\07005B831A0004B4&0 To whitelist a removable media device, provide a string value that matches portions of the device's PNPDeviceID. Multiple device PNPDeviceIDs are allowed. For example, to whitelist all Kingston DataTraveler Vault Privacy models, input the string: PROD_DTVAULT_PRIVACY To whitelist both models of Kingston DataTraveler, the Vault and Vault Privacy models, input the string: PROD_DTVAULT_PRIVACY; PROD_DT_VAULT Space characters are considered part of the substring to match to a PNPDeviceID. Using the previous PNPDeviceID as an example, a space before and after the semicolon would cause neither of the substrings to be matched, because the space character is not part of the PNPDeviceID. Instructions... *To find the PNPDeviceID for removable media:* 1. Insert the removable media device into an encrypted computer. 2. Open the *EMSService.log* in C:\Programdata\Dell\Dell Data Protection\Encryption\EMS. 3. Find PNPDeviceID= For example: 14.03.18 18:50:06.834 [I] [Volume "F:\"] PnPDeviceID = USBSTOR\DISK&VEN_SEAGATE&PROD_USB&REV_0409\2HC015KJ&0 VEN=Vendor; Green highlighted text is for the vendor to be excluded PROD=Product/Model Name; Adding text highlighted blue also excludes all of Seagate's USB drives REV=Firmware Revision; Adding text highlighted gray also excludes the specific model being used Serial number (in this example); Adding text highlighted yellow excludes just this device OR *To find the PNPDeviceID for removable media on Windows 7 or later:* 1. Insert the removable media device. 2. Open the Control Panel and go to Administrative Tools > Computer Management. 3. Select the Hardware tab, select the drive, and click Properties. 4. A new windows displays. Select the Device Instance Path in the Property menu. The PNPDeviceID is displayed in *Value* . Available Delimeters: Tabs Commas Semi colons Hex character 0x1E (Record separator character)
EMS Alpha Characters Required in Password	Selected	Selected requires one or more letters in the password.

EMS Mixed Case Required in Password	Selected	Selected requires at least one uppercase and one lowercase letter in the password.
EMS Number of Characters. Required in Password	8	*1-40 characters* Minimum number of characters required in the password.
EMS Numeric Characters Required in Password	Selected	Selected requires one or more numeric characters in the password.
EMS Password Attempts Allowed	3	*1-10* Number of times the user can attempt to enter the correct password.
EMS Special Characters Required in Password	Not Selected	Selected requires one or more special characters in the password.
EMS Access and Device Code Length	16	*8, 16, 32* Number of characters access and device codes have. 32 characters is the most secure, while 8 is the easiest to enter.
EMS Access Code Attempts Allowed	3	*1-10* Number of times the user can attempt to enter the access code.
EMS Access Code Failure Action	Apply Cooldown	*Apply Cooldown, Wipe Encryption Keys* Action to take following unsuccessful EMS Access Code Attempts Allowed: • Apply Cooldown to allow another round of attempts following the specified cooldown period (EMS Cooldown Time Delay and EMS Cooldown Time Increment policies) • Wipe Encryption Keys to delete the encryption keys on the media, making the encrypted data inaccessible until the owner takes the media to an encrypted computer for which he has a login.
EMS Access Code Required Message	String Authentication Failed. Please contact your system administrator.	*String - 5-512 characters - Authentication Failed: Please contact your system administrator.* Message that displays when a user needs to contact an administrator for an access code after authentication failure. More... Message policies must have non-blank values. "Space" and "Enter" characters used to add lines between rows count as characters used. Messages over the 512 character limit are truncated on the client. Optionally customize the second sentence of the message to include specific instructions about how to contact a help desk or security administrator for authentication failures.
EMS Cooldown Time Delay	30	*0-5000 seconds* Number of seconds the user must wait before attempting to enter the access code after failing the specified number of times.
EMS Cooldown Time Increment	20	*0-5000 seconds* Incremental time to add to the cooldown time each time the user fails to enter the correct access code in the specified number of attempts.
EMS Access Code Failed Message	String You are not authorized to use this media. Please contact your system administrator.	*String - 5-512 characters - You are not authorized to use this media. Please contact your system administrator.* Message that displays following unsuccessful Access Code Attempts Allowed. More... Message policies must have non-blank values. "Space" and "Enter" characters used to add lines between rows

		count as characters used. Messages over the 512 character limit are truncated on the client. Optionally customize the message to include specific instructions about how to contact the help desk or security administrator.
EMS Encryption Rules	String	Encryption rules to be used to encrypt/not encrypt certain drives, directories, and folders. A total of 2048 characters are allowed. "Space" and "Enter" characters used to add lines between rows count as characters used. Any rules exceeding the 2048 limit are ignored. See Encryption Rules for information. More... Storage devices which incorporate multi-interface connections, such as Firewire, USB, eSATA, etc. may require the use of both Encryption External Media and encryption rules to encrypt the endpoint. This is necessary due to differences in how the Windows operating system handles storage devices based on interface type. To ensure encrypting an iPod via Encryption External Media does not make the device unusable, use the following rules: -R#:\Calendars -R#:\Contacts -R#:\iPod_Control -R#:\Notes -R#:\Photos You can also force encryption of specific file types in the directories above. Adding the following rules will ensure that ppt, pptx, doc, docx, xls, and xlsx files are encrypted in the directories excluded from encryption via the previous rules: ^R#:\Calendars ;ppt.doc .xls.pptx .docx.xlsx ^R#:\Contacts ;ppt .doc.xls .pptx.docx .xlsx ^R#: \iPod_Control ;ppt.doc .xls.pptx .docx.xlsx ^R#:\Notes ;ppt.doc .xls.pptx .docx.xlsx ^R#:\Photos ;ppt.doc .xls.pptx .docx.xlsx Replacing these five rules with the following rule will force encryption of ppt, pptx, doc, docx, xls, and xlsx files in any directory on the iPod, including Calendars, Contacts, iPod_Control, Notes, and Photos: ^R#:\;ppt.doc.xls .pptx.docx.xlsx These rules disable or enable encryption for these folders and file types for all removable devices - not just an iPod. Use care when defining rules to exclude an iPod from encryption. These rules have been tested against the following iPods: iPod Video 30gb fifth generation iPod Nano 2gb second generation

		iPod Mini 4gb second generation Dell does not recommend the use of the iPod Shuffle, as unexpected results may occur. As iPods change, this information could also change, so caution is advised when allowing the use of iPods on Encryption External Media-enabled computers. Because folder names on iPods are dependent on the model of the iPod, Dell recommends creating an exclusion encryption policy which covers all folder names, across all iPod models.
EMS Block Access to UnShieldable Media	Selected	Block access to any removable media that is less than 55 MB and thus has insufficient storage capacity to host Encryption External Media (such as a 1.44MB floppy disk). More... All access is blocked if EMS Encrypt External Media and this policy are both Selected. If EMS Encrypt External Media is Selected, but this policy is Not Selected, data can be read from the unencryptable media, but write access to the media is blocked. If EMS Encrypt External Media is Off, then this policy has no effect and access to unencryptable media is not impacted.
SDE Encryption Enabled	Selected	If this policy is Not Selected, SDE encryption is disabled, regardless of other policy values. Selected means that all data not encrypted by other Intelligent Encryption policies are encrypted per the SDE Encryption Rules policy. Changing the value of this policy requires a reboot.
SDE Encryption Algorithm	AES256	*AES 256, AES 128, 3DES* Encryption algorithm used to for System Data Encryption. Encryption algorithms in order of speed, fastest first, are AES 128, AES 256, 3DES.
SDE Encryption Rules	String F#:\ -^%ENV:SYSTEMDRIVE%\System Volume Information -^%ENV:SYSTEMROOT%\;dll.exe.sys.ocx.man.cat .manifest.policy -^%ENV:SYSTEMROOT%\System32 -^%ENV:SYSTEMROOT%\SysWow64 -^%ENV:SYSTEMROOT%\WinSxS -^%ENV:SYSTEMROOT%\Fonts ^3@%ENV:SYSTEMROOT%\SYSTEM32\;exe -^3@%ENV:SYSTEMROOT%\SYSTEM32\cmd.exe;exe -^3@%ENV:SYSTEMROOT%\SYSTEM32\autochk.exe;exe -^3%ENV:SYSTEMDRIVE%\ProgramData\Dell\Kace -^3%ENV:SYSTEMDRIVE%\Program Files\Dell\Kace -^3%ENV:SYSTEMDRIVE%\Program Files (x86)\Dell\Kace	Encryption rules to be used to encrypt/not encrypt certain drives, directories, and folders. See Encryption Rules for information. SDE Encryption Rules may be changed as appropriate for your environment. However, these defaults have been tested extensively. Removing these exclusions may result in Windows issues, particularly after applying patch updates. Contact ProSupport for guidance if you are unsure about changing the values.
Encryption Enabled	Selected	This policy must be selected to use all Common encryption policies. Not Selected means that no Common encryption takes place, regardless of other policy values. Changing the value of this policy triggers a new sweep to encrypt/decrypt files.
Common Encrypted Folders	String %ENV:SYSTEMDRIVE%\;accdb.doc.docm.docx.mdb.pdf.ppam .pps.ppsm.ppsx.ppt.pptm.pptx.pub.puz.sldm.sldx.tif.tiff .vdx.vsd.vss.vst.vsx.vtx.xlam.xlm.xls.xlsb.xlsm.xlsx .xsf.zip.rar %ENV:USERPROFILE%\Desktop %ENV:USERPROFILE%\Download -^%ENV:SYSTEMDRIVE%\;dat	*String - maximum of 100 entries of 500 characters each (up to a maximum of 2048 characters)* A list of folders on computer drives to be encrypted or excluded from encryption, which can then be accessed by all managed users who have access to the computer. See Encryption Rules for information. *Important: Overriding directory protection can result in an unbootable computer and/or require reformatting drives.* More... The available drive letters are: #: Refers to all drives f#: Refers to all fixed (non-removable) drives r#: Refers to all removable drives

Common Encryption Algorithm	AES256	*AES 256 or AES 128* Encryption algorithm used to encrypt data at the endpoint (all users) level. System paging files are encrypted using AES 128. Encryption algorithms in order of speed, fastest first, are AES 128, AES 256, 3DES.
Application Data Encryption List	Exe List winword.exe excel.exe powerpnt.exe msaccess.exe winproj.exe outlook.exe acrobat.exe visio.exe mspub.exe winzip.exe winrar.exe onenote.exe onenotem.exe	*String - maximum of 100 entries of 500 characters each* Dell does not add explorer.exe or iexplorer.exe to the ADE list, as unexpected or unintended results may occur. Explorer.exe is the process used to create a new notepad file on the desktop using the right-click menu. Setting encryption by file extension, instead of the ADE list, provides more comprehensive coverage. Changes to this policy do not affect files already encrypted because of this policy. List process names of applications (without paths) whose new files you want encrypted, separated by carriage returns. Do not use wildcards. More... You can also specify these process names (separated by commas) via the registry value HKLM\SOFTWARE\Credant\CMGShield\ApplicationDataEncryptionList. The Encryption client encrypts all new files (not already being encrypted by Common Encrypted Folders and User Encrypted Folders) on the current computer hard drives created by these application processes whenever they are owned by a currently-logged-on managed user. This may include files excluded from encryption by Common Encrypted Folders and/or User Encrypted Folders. The following folders and their subfolders are always excluded from encryption by this policy: C:\Windows\system32 C:\Windows\Software Distribution C:\Windows\Security C:\System Volume Information\Program Files\Credant\(.dll.exe.sys.mac.ddp.wip.rty.nmd.inv) Dell strongly recommends not listing applications or installers that write system-critical files. Doing so could result in encryption of important system files, which could make a Windows computer unbootable. Common process names: outlook.exe winword.exe powerpnt.exe msaccess.exe wordpad.exe mspaint.exe excel.exe The following hard-coded system and installer process names are ignored if specified in this policy (you can also add to this list in the registry value HKLM\SOFTWARE\Credant\CMGShield\EUWPrivilegedList): hotfix.exe, a Windows update process update.exe, a Windows update process setup.exe, a third-party installer process msiexec.exe, a third-party installer process wuauclt.exe, a Windows update process wmiprvse.exe, a Windows system process migrate.exe, a Windows update process unregmp2.exe, a Windows update process ikernel.exe, a third-party installer process wssetup.exe, the Windows Encryption client installer svchost.exe, a Windows system process

Encrypt Temporary Files	Not Selected	When this policy is selected, the paths listed in the environment variables TEMP and TMP are encrypted. TEMP and TMP for the operating system are encrypted with the Common encryption key. To reduce encryption sweep time, the contents of the TEMP and TMP folders are cleared for initial encryption, as well as updates to this policy. However, if your organization uses a third-party application that requires the file structure within the \temp directory to be preserved, you should prevent this deletion. To disable temporary file deletion, create DeleteTempFiles (REG_DWORD) and set its value to 0 in the registry at HKLM\SOFTWARE\Credant\CMGShield.
Encrypt User Profile Documents	Not Selected	When this policy is selected, the following are encrypted: • The users profile (C:\Users\jsmith) with the User data encryption key • \Users\Public with the Common encryption key
Encrypt Windows Paging File	Selected	When this policy is selected, the Windows paging file is encrypted. A change to this policy requires a reboot.
Managed Services	null	*String - maximum of 100 entries of 500 characters each (up to a maximum of 2048 characters)* When a service is managed by this policy, the service is started only after the user is logged in and the Encryption client is unlocked. This policy also ensures that the Service managed by this policy is stopped before the Encryption client is locked during logoff. This policy can also prevent a user logoff if a service is unresponsive. More... Syntax is one service name per line. Spaces in the Service name are supported. Wildcards are not supported. Entries are not case-sensitive. For example, GoogleDesktop Manager is the same as googledesktopmanager. The service "log on as" setting has no bearing on whether or not the Encryption client can control it. It does not matter if a user logs on with user credentials verses the local system. The startup type (Automatic or Manual) does not affect the ability of the Encryption client to control it. Automatic or Manual startup is acceptable. Managed services are not started if an unmanaged user logs on.
Secure Post-Encryption Cleanup	Single Pass Overwrite	*No Overwrite, Single-pass Overwrite, Three-pass Overwrite, Seven-pass Overwrite* Once encryption is complete, this policy determines what happens to the unencrypted residue of the original files: • No Overwrite deletes it. This value yields the fastest encryption processing. • Single-pass Overwrite overwrites it with random data. • Three-pass Overwrite overwrites it with a standard pattern of 1s and 0s, then with its complement, and then with random data. • Seven-pass Overwrite overwrites it with a standard pattern of 1s and 0s, then with its complement, and then with random data five times. This value makes it most difficult to recover the original files from memory, and yields the most secure encryption processing.
Secure Windows Credentials	Selected	When this policy is selected, the Windows Credentials is secured by encrypting the entire registry with the exception of registry information required for computer boot. The information required for computer boot includes HKLM/SYSTEM and all sub-keys. This policy value is automatically set to Selected if SDE is enabled.

		More... A reboot is required when a change to this policy is delivered. To control this reboot, configure the following policies: Force Reboot on Update, Length of Each Reboot Delay, and Number of Reboot Delays Allowed.
Block Unmanaged Access to Domain Credentials	Selected	This policy prevents unmanaged applications from accessing the Windows domain credentials when a user is logged in.
Secure Windows Hibernation File	Not Selected	When enabled, the hibernation file is encrypted only when the computer enters hibernation. The Encryption client disengages protection when the computer comes out of hibernation, providing protection without impacting users or applications while the computer is in use.
Prevent Unsecured Hibernation	Not Selected	When enabled, the Encryption client does not allow computer hibernation if the client is unable to encrypt the hibernation data.
Workstation Scan Priority	Lowest	*Highest, High, Normal, Low, Lowest* Specifies the relative Windows priority of encrypted folder scanning. High and Highest prioritize scanning speed over computer responsiveness, Low and Lowest prioritize computer responsiveness over scanning speed and favor other resource-intensive activities, and Normal balances the two. The client checks for a changed Workstation Scan Priority before processing the next file. The scan priority levels are used in two different ways. 1. These values correspond with the values used by the Microsoft SDK to set thread execution priority. 2. The client uses these values to introduce a delay in the encryption sweep after every single file is processed. The values translate to the following millisecond delay ranges, where the encryption thread will sit idle and then return full control to the operating system: Highest=0 ms / Lowest=100 ms
Policy Proxy Connections	String	String - maximum of 1500 characters List fully qualified Policy Proxy hostnames, or IP addresses, separated by carriage returns. Ports cannot be specified in this policy. More... Once a valid entry is found, the remainder of the Policy Proxies listed are ignored. Entries are processed in the following order: 1. GKConnections Override (this registry entry overrides all other entries) 2. GKConnections (this registry entry is set automatically by the client, based on the this policy) 3. GK To override this policy and specify ports via the registry key, set HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\CMGShield\GKConnectionsOverride. The client communicates with Policy Proxies using the GKPORT (the default is 8000). If necessary, change that port via the registry key HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\CMGShield\GKPort. Inherited values for this policy accumulate. For the client to connect to a Policy Proxy specified in this policy, it must be in the same group as the Policy Proxy specified during client installation. Because the client supports up to 255 users per computer, this

		policy is available only at the Enterprise level.
Policy Proxy Polling Interval	720	1-1440 minutes The interval that the client attempts to poll Policy Proxy for policy updates, and send inventory information to Policy Proxy. The client also attempts to poll Policy Proxy each time a user logs on.
See basic settings		

Variables

Some Windows policies support the following variables. A pathname can consist entirely of one or more of these variables, or can include one or more of these variables at any point.

To get directory locations that these CSIDL values resolve to, go to http://msdn.microsoft.com/en-us/library/bb762494.aspx. All names listed on the MSDN page are CSIDL_<name>.

- Includes any of the following Windows CSIDL constants:

DESKTOP

INTERNET

PROGRAMS

CONTROLS

PRINTERS

PERSONAL

FAVORITES

STARTUP

RECENT

SENDTO

STARTMENU

STARTMENU

MYDOCUMENTS

MYMUSIC

MYVIDEO

DESKTOPDIRECTORY

DRIVES

NETWORK

NETHOOD

FONTS

TEMPLATES

COMMON_STARTMENU

COMMON_PROGRAMS

COMMON_STARTUP

COMMON_DESKTOPDIRECTORY

APPDATA

PRINTHOOD

LOCAL_APPDATA

ALTSTARTUP

COMMON_ALTSTARTUP

COMMON_FAVORITES

INTERNET_CACHE

COOKIES

HISTORY

COMMON_APPDATA

WINDOWS

SYSTEM

PROGRAM_FILES

PROGRAMFILES

MYPICTURES

PROFILE

SYSTEMX86

PROGRAM_FILESX86

PROGRAMFILESX86

PROGRAM_FILES_COMMON

PROGRAM_FILES_COMMONX86

COMMON_TEMPLATES

COMMON_DOCUMENTS

COMMON_ADMINTOOLS

ADMINTOOLS

CONNECTIONS

COMMON_MUSIC

COMMON_PICTURES

COMMON_VIDEO

RESOURCES

PROFILES

- Includes a numeric or text value stored in the registry for the current user. If you specify a path but not an item, the client uses the default value
- Includes a numeric or text value stored in the registry for the local computer. If you specify a path but not an item, the client uses the default value
- Includes the value of a Windows local environment variable
- Includes the % character

Windows Policies that Require Reboot

- SDE Encryption Enabled
- Encrypt Windows Paging File
- Secure Windows Credentials
- All PCS policies

Windows Policies that Require Logoff

- SDE Encryption Enabled
- User state change to Suspended
- EMS Encrypt External Media
- EMS Scan External Media
- EMS Encryption Algorithm
- EMS Exclude CD/DVD Encryption
- EMS Data Encryption Key

Encryption Rules

Important: *Before you begin, you must understand directory protection, as well as when and how to override directories and file types. If you do not completely understand the information included in this section, as well as the encryption settings that currently exist on your environment, do not attempt to override protected directories.*

Do not encrypt files with the extension tmp. Encrypting .tmp files may result in an unbootable computer and/or require reformatting drives.

Protected Directories

The Encryption client has several directories that are, by default, protected from encryption. The level of protection varies from folder to folder. If a folder is protected, then the only way to encrypt data within that directory is to use the override modifier described in Modifiers – What they are and what they do.

There are four levels (categories) of protection that directories and files can have: 0, 1, 2, and 3. Category 3 is the most protected level.

Modifiers - What they are and what they do

The **^** character is the “Override” command. It causes the listed policy to override protected directories. It may be followed by a “2” or a “3”, indicating the level of the override.

The @ character is the “At” command. It will cause the listed policy to be applied at the specified folder location only (subdirectories of that folder are not subject to that policy).

The **-** is the “Not” command. It will cause the listed policy to be an exclusion policy instead of an inclusion policy.

Using the Override Modifier

The Override Modifier can be used to allow for inclusion or exclusion in cases where there is a higher level of protection. The following are the different override levels supported:

^ Category 1 Override

^2 Category 2 Override

^3 Category 3 Override

Encrypting/Not Encrypting Extensions

To include or exclude file name extensions using encryption rules, use the following within your rules:

- After specifying your directory location, use a semi-colon (;) before listing your extensions.
- After specifying your directory location, you **do not need** to list a trailing backslash (****).
- The period is used as a delineator. It is not meant to be used as “dot-extension.” However, you can precede the first extension with a period.
- The **Override** command (^) can be used with extensions.
- The **At** command (@)can be used with extensions.
- The **Not** command (-) can be used with extensions.
- You can make any combination of the modifiers with an extension inclusion or exclusion.

Examples of Extension Inclusions/Exclusion

C:\;doc.xls.ppt.docx.xlsx.pptx

What this does: On the C: drive, this encrypts all doc, docx, xls, xlsx, ppt, and pptx files that do not exist within any protected directory.

^C:\;txt

What this does: On the C: drive, this encrypts all txt files that are not in a directory that has protection of Category 1 or better.

-C:\;bat.exe.dll

What this does: On the C: drive, this causes all files with the extension bat, exe, and dll to not be encrypted.

Encrypting/Not Encrypting Directories

To include or exclude directories using encryption rules, use the following within your rules:

- After specifying your directory location, you **do not need** to list a trailing backslash (****).
- If you list a directory for inclusion, every file contained within that directory is encrypted.

- The **Override** command (^) can be used with folders only when specifying an exclusion policy.
- The **At** command (@) can be used with folders.
- The **Not** command (-) can be used with folders.
- You can make any combination of the supported modifiers for folders. If the **Override** command (^) is used, the statement can only be an exclusion statement.

Examples of folder inclusion/exclusion

C:\CustomApplication\DataStore

What this does: On the C: drive, this causes every file within the directory of \CustomApplication\DataStore to be encrypted.

-C:\Documents and Settings\All Users

What this does: On the C: drive, this applies a Category 0 level of protection to the directory of \Documents and Settings\All Users.

-^2C:\CustomApplication\dll

What this does: On the C: drive, this applies a Category 2 level of protection to the directory of \CustomApplication\dll.

Sub-directories and Precedence of Directives

Encryption rules may be listed in any order. If more than one rule applies to a given folder or file, then the following general rules determine which one prevails:

1. The rule with the more specific path prevails.
2. If the rules have equal paths, specified extensions prevail.
3. If the rules both specify extensions, exclusion overrides inclusion.

Example of sub-directories

C:

-C:\MyApplicationFolder

What this does: (1st statement is an inclusion, 2nd statement is an exclusion) On the C: drive, encrypt all files in folders at the root level and below, **except** for files residing in the protected directories and any files residing in “MyApplicationFolder”.

Example 1 of competing directives:

C:

-C:\MyApplicationFolder

^C:\;doc.xls.ppt.docx.xlsx.pptx

What this does: (1st statement is an inclusion, 2nd statement is an exclusion, 3rd statement is an inclusion) On the C: drive, encrypt all files in folders at the root level and below, **except** for files residing in the protected directories and files residing in “MyApplicationFolder”. However, override and encrypt files with the extension doc, docx, xls, xlsx, ppt, and pptx in the protected directories **and** in the folder “MyApplicationFolder”.

Example 2 of competing directives:

C:

-C:\MyApplicationFolder

^C:\;doc.xls.ppt.docx.xlsx.pptx

-^C:\MyApplicationFolder;doc.xls.ppt.docx.xlsx.pptx

> **What this does:** (1st statement is an inclusion, 2nd statement is an exclusion, 3rd statement is an inclusion, 4th statement is an exclusion) On the drive of C:, encrypt all files in folders at the root level and below, **except** for files residing in the protected directories and files residing in "MyApplicationFolder". However, override and encrypt files with the extension doc, docx, xls, xlsx, ppt, and pptx in the protected directories, **but not** in the folder "MyApplicationFolder".

Example 3 of competing directives:

C:

-C:\MyApplicationFolder

^C:\;doc.xls.ppt.docx.xlsx.pptx

-^C:\MyApplicationFolder;doc.xls.ppt.docx.xlsx.pptx

-^C:\MyApplicationFolder\Templates

What this does: (1st statement is an inclusion, 2nd statement is an exclusion, 3rd statement is an inclusion, 4th statement is an exclusion, 5th statement is an exclusion) On the C: drive, encrypt all files in folders at the root level and below, **except** for files residing in the protected directories and files residing in "MyApplicationFolder". However, override and encrypt files with the extension doc, docx, xls, xlsx, ppt, and pptx in the protected directories, **but not** in the folder "MyApplicationFolder". Additionally, the folder "MyApplicationFolder\Templates" gains a category 2 protection causing no data to be encrypted there, since the inclusion statements are less than or equal to category 2.

Environment Variables, KNOWNFOLDERID constants, and CSIDL

Using encryption rules, you can make use of environment variables, KNOWNFOLDERID constants (Windows 7 and later), and CSIDL values (pre-Windows 7 computers) in addition to specifying your policy folder locations as absolute paths. To use variables in your encryption rules, follow these formatting rules:

- Before and after the use of the variable, use a percent sign (**%**).
- For environment variables, you must use "**ENV:**" preceding the variable name, all contained within the percent signs.
- For KNOWNFOLDERID constants, you must use "**FOLDERID_**" preceding the variable name. Percent signs are not used.
- For CSIDL variables, you must use "**CSIDL:**" preceding the variable name, all contained within the percent signs.
- Ensure that your variable contains a trailing backslash if you plan on appending another directory after the use of the variable.
- Variables can be used in both folder and extension inclusion or exclusion rules.

The following environment variables are supported:

All locally defined environment variables

The following KNOWNFOLDERID values are supported:

RoamingAppData

Cookies

Desktop

Favorites

InternetCache

LocalAppData

Music

Pictures

Documents

Programs

Recent

SendTo

StartMenu

Startup

Templates

The following CSIDL variables are supported:

APPDATA

COOKIES

DESKTOPDIRECTORY

FAVORITES

INTERNET_CACHE

LOCAL_APPDATA

MYMUSIC

MYPICTURES

PERSONAL

PROGRAMS

RECENT

SENDTO

STARTMENU

STARTUP

TEMPLATES

Some examples of variables used in folder and extension policy:

%ENV:SYSTEMDRIVE%\CustomApplication

What this does: This lists the folder \CustomApplication\ for encryption on the default drive where Windows is installed.

-%ENV:USERPROFILE%\Desktop

What this does: This lists the user who is logged in to have their desktop obtain a category 0 protection.

Application Data Encryption (ADE)

ADE encrypts any file written by a protected application, using a category 2 override. This means that any directory that has a category 2 protection or better, or any location that has specific extensions protected with category 2 or better, will cause ADE to not encrypt those files.

For example, ADE does not encrypt any files written into /Windows/System32 folder, because this directory has a default protection of category 2.

Example Policies for Common/User Key Encryption

The following set of encryption rules encrypts most of the drive, including standard Microsoft Office-type documents in the Documents and Settings folders. This policy set should only be used for Common encryption (not User encryption, removable media, or SDE). This is considered a strong policy set, and will typically require some adjustments for local conditions and requirements.

%ENV:SYSTEMDRIVE%

^%ENV:USERPROFILE%\;<insert standard office extensions here >

FOLDERID_Documents or **%CSIDL:PERSONAL%** (pre-Windows 7)

%ENV:USERPROFILE%\Desktop

^%ENV:USERPROFILE%\;mp3.mp4.mpeg.avi.wmv.wav

-^%ENV:USERPROFILE%\Desktop\;<system file extensions to exclude>

-%ENV:SYSTEMDRIVE%\;<system file extensions to exclude>

-%ENV:SYSTEMDRIVE%\config.msi

What this does:

Encrypts all of C:\, except for protected directories

Encrypts standard Microsoft Office documents across the drive, except for protected directories, although it will encrypt them in the USERPROFILE directory.

Encrypts all of My Documents

Encrypts all of the Desktop, except for any selected excluded extensions

Excludes common system files from encryption

Excludes all encryption from C:\config.msi directory, due to MSI upgrade migration issues

All paths are dynamic based on environment variables

%ENV:USERPROFILE% (inclusion or exclusion) variable should never be used with SDE Encryption.

System Data Encryption (SDE)

SDE is an intelligent file-based encryption method where the encryption key is auto-authenticated during the volume mount process. A unique SDE key is generated for each volume that is targeted for encryption by SDE. This allows the SDE key to be used to encrypt data that would not otherwise be possible with the Common or User keys due to time-based availability of the keys.

Due to the difference in how the SDE key can be used, there are several caveats to be aware of when considering use of this feature.

- The built-in exclusions covered in protected directories do not apply to SDE. By design, SDE excludes portions of the operating system that are necessary for booting and updating.

- If a file is targeted for encryption by any key other than SDE in addition to SDE, then SDE does not encrypt the file.
- All encryption rules apply when writing SDE policies.

Encryption Rules for SDE Encryption

The following is the default SDE policy. **Any changes to this policy should be considered carefully.**

The protection of the SystemRoot directory is specified so that only the root itself is protected, meaning that the sub-directories of the SystemRoot do not inherit this protection. This would be the equivalent of using the following policy:

-@C:

Encryption Rules for Encryption External Media

Removable Media Encryption policies operate off their own set of encryption rules, independent of Common encryption, User encryption, or SDE uses. User/Common encryption policies are only applied to fixed disks. If an endpoint is determined to be removable media, then Removable Media Encryption policies are applied.

What Happens When Policies Tie

- When an exclusion and inclusion statement both apply to a given directory or file, the exclusion policy prevails.
- If you apply a Common encryption policy and User encryption policy specifically to the same file or location, the file or location is Common key encrypted.
- If you apply a Common encryption policy and an SDE encryption policy specifically to the same file or location, the file or location is Common key encrypted.
- If you apply a User encryption policy and an SDE encryption policy specifically to the same file or location, the file or location is User key encrypted.

See Sub-directories and Precedence of Directives for more information.

Encryption Rules for Generic Drive Statements

Instead of having to specify each drive in an inclusion or exclusion rule by its drive letter assignment, you may use a generic rule to target either All Fixed Drives or all Removable Drives.

Fixed Drive Usage: Replace the drive letter with F#.

Example: F#:\ instead of C:\ or D:\

The Fixed Drive rule can only be used within a Common Encrypted Folder policy, User Encrypted Folder policy, and/or SDE policy.

Removable Drive Usage: Replace the drive letter with R#.

Example: R#:\ instead of F:\ or H:\

The Removable Drive rule can only be used within an Encryption External Media Encryption Rules policy.

Remove System Data Encryption (SDE)

To completely decrypt SDE encrypted files, apply the following policies:

SDE Encryption Enabled = Not Selected

Encrypt Windows Paging File = Not Selected

Secure Windows Credentials = Not Selected

Authentication

Authentication

Authentication policies allow you to configure user experience and Windows authentication.

Policy descriptions also display in tooltips in the Management Console.

Policy	Default Setting	Description
Pre-Boot Authentication This technology provides a secure, tamper-proof environment by preventing data from being read from the hard disk or operating system until the user enters the correct PBA login credentials. Pre-Boot Authentication serves as an extension of the BIOS or boot firmware to provide a trusted authentication layer, separate from the operating system.		
Authentication Method	Password	*Password* *Smart Card* Select the type of authentication to use when logging in to the PBA.
Support Information Text	String Please contact your system administrator.	*String 0-512 characters* Text to display on the PBA support information screen. Customize the message to include specific instructions about how to contact the help desk or Security administrator. Not entering text in this field results in no support contact information being available for the user. Text wrapping occurs at the word level, not the character level. If a single word is more than approximately 50 characters in length, it does not wrap and no scroll bar is present, therefore the text is truncated. The text in this policy is translatable.
PBA Title Text	0-17 characters	*0-17 characters* The text to display on the top of the PBA screen. Not entering text in this field results in no title being displayed. Text does not wrap, so entering more than 17 characters results in the text being truncated. The text in this policy is translatable.
Sync Users at PBA Activation	Not Selected	Select this option to sync all users of this computer with the PBA database during PBA activation.
See advanced settings		
Windows Authentication This technology sets definitions around user login, specifically what is required to login (password, smart card, fingerprint), password recovery options, and password requirements (number of attempts allowed, password length).		
Logon Authentication Policy for Administrators	Windows Password and None	The possible VALUES are: Windows Password None Fingerprints Contactless Card

Logon Authentication Policy for Users	Windows Password and None	The possible VALUES are: Windows Password None Fingerprints Contactless Card One-Time Password
See advanced settings		
Microsoft Passport This technology allows the use of Microsoft Passport, specifically authentication attempts and PIN usage.		
Microsoft Passport	Off	*On* *Off* Toggle to On to enable Microsoft Passport. If this policy is toggled to Off, no Microsoft Passport policies are enabled. Microsoft Passport is supported only on computers running Windows 10.
Maximum Windows Passport Authentication Attempts	3	*1-10 attempts* Number of chances the user has to authenticate with correct credentials.
Logon Authentication Method	PIN	Currently, logon authentication method is supported only with PIN.
PIN Length	8	*4-127 numeric characters* Minimum number of characters required in the PIN.

Advanced Authentication

Authentication policies allow you to configure user experience and Windows authentication.

Policy descriptions also display in tooltips in the Management Console.

Policy	Default Setting	Description
Pre-Boot Authentication This technology provides a secure, tamper-proof environment by preventing data from being read from the hard disk or operating system until the user enters the correct PBA login credentials. Pre-Boot Authentication serves as an extension of the BIOS or boot firmware to provide a trusted authentication layer, separate from the operating system.		
Authentication Method	Password	*Password* *Smart Card* Select the type of authentication to use when logging in to the PBA.

Support Information Text	String Please contact your system administrator.	*String 0-512 characters* Text to display on the PBA support information screen. Customize the message to include specific instructions about how to contact the help desk or Security administrator. Not entering text in this field results in no support contact information being available for the user. Text wrapping occurs at the word level, not the character level. If a single word is more than approximately 50 characters in length, it does not wrap and no scroll bar is present, therefore the text is truncated. The text in this policy is translatable.
PBA Title Text	0-17 characters	*0-17 characters* The text to display on the top of the PBA screen. Not entering text in this field results in no title being displayed. Text does not wrap, so entering more than 17 characters results in the text being truncated. The text in this policy is translatable.
Sync Users at PBA Activation	Not Selected	Select this option to sync all users of this computer with the PBA database during PBA activation.
Legal Notice Text	String 0-512 characters	*String 0-512 characters* Text to display before being allowed to log on to the computer. For example: By clicking OK, you agree to abide by the acceptable computer use policy. Not entering text in this field results in no text, OK, or Cancel buttons being displayed. Text wrapping occurs at the word level, not the character level. If a single word is more than approximately 50 characters in length, it does not wrap and no scroll bar is present, therefore the text is truncated. The text in this policy is translatable.

Self Help Questions (Pre-8.0 clients)	At least 3 selectable questions	Specify the questions to present to Windows users during recovery questions setup. Separate each question by a carriage return. These questions are used if the Windows password is forgotten. At least 3 questions must be specified. What is the name of your first pet? Who was your first employer? What was the first concert you attended? What was the make of the first car you owned? What was the last name of your third grade teacher? In what city or town did your mother and father meet? In what city or town was your first job?
Initial Access Code	String 1-100 characters	*String 1-100 characters* This policy is used to log on to a computer when network access to Dell Server and Active Directory (AD) are both unavailable. The Initial Access Code policy should only be used if absolutely necessary, it is not the recommended method to log in. Using the Initial Access Code policy does not provide the same level of security as the usual authentication method of logging in using user name, domain, and password. The Initial Access Code can only be used one time, immediately after activation. The first domain login that occurs after the Initial Access Code is entered is cached and the Initial Access Code entry field does not displayed again.
Encryption Administrator Password	String	*9-32 characters with at least 1 number and 1 letter* Computer-generated password used by the Dell Server and client for recovery and other internal processes. No user or administrator interaction is required. All values are automatically maintained in the Dell Server and can never be deleted. Entering a value for this policy does not affect the Override Count.
Non-Cached User Login Attempts Allowed	50	*Any number* This policy does not come into play when connected to the network (there is a connection to AD), because authentication with AD is attempted. This policy only comes into play when the computer is not connected to the network and an unknown user attempts to log in (meaning, a user that has not logged in to the computer before -- no credentials have been cached).

Cached User Login Attempts Allowed	10	*1-20 times* Number of times that a cached user can attempt to log in.
Self Help Question/Answer Attempts Allowed	3	*1-10 times* Number of times the user can attempt to enter the correct answer.
Enable One Step Logon	Selected	This policy simplifies the logon process when multi-factor authentication is enabled at both preboot and Windows logon. If selected (or not configured), authentication is required at preboot only, and users are automatically logged on to Windows. If not selected, authentication may be required multiple times.
Number of Shutdown/Restart Delays Allowed	5	*1-25 times* Number of times that a user is allowed to snooze/delay a shutdown/restart before being forced to shutdown/restart. TPM requires a reboot. SED requires a shutdown.
Length of Each Shutdown/Restart Delay	300 seconds	*300-30000 seconds* Number of seconds between each time the user is asked to shutdown/reboot. TPM requires a reboot. SED requires a shutdown.
Length of Forced Shutdown/Restart Notice	60 seconds	*60-1800 seconds* When user has reached the maximum number of authorized shutdown/restart snoozes/delays, this policy sets the number of seconds allowed before forcing a shutdown/restart. TPM requires a reboot. SED requires a shutdown.
Allow PBA to Remember User Name	Selected	*Selected* *Not Selected* Enables or disables the ability for users to select Remember Me on the PBA login screen.
Crypto Erase Password	String 0-100 characters	*String 0-512 characters* A word or code of up to 100 characters used as a fail-safe security mechanism. Entering this word or code in the user name or password field during PBA authentication initiates a crypto erase, which removes the keys from secure storage. Once this process is invoked, the drive is unrecoverable. Leave this field blank if you do not want a crypto erase password available in case of emergency.
Enable Client Check for PBA Commands	Not Selected	Allows the client to automatically check for PBA Device Control commands that are pushed from the Dell Server. When enabled, the PBA environment checks for new commands from the Dell Server every five minutes.

See basic settings		
Windows Authentication This technology sets definitions around user login, specifically what is required to login (password, smart card, fingerprint), password recovery options, and password requirements (number of attempts allowed, password length).		
Logon Authentication Policy for Administrators	Windows Password and None	The possible VALUES are: Windows Password None Fingerprints Contactless Card
Logon Authentication Policy for Users	Windows Password and None	The possible VALUES are: Windows Password None Fingerprints Contactless Card
In-session Authentication Policy for Administrators	Windows Password and None	The possible VALUES are: Windows Password None Fingerprints Contactless Card One-Time Password
In-session Authentication Policy for Users	Windows Password and None	The possible VALUES are: Windows Password None Fingerprints Contactless Card One-Time Password

Recovery Questions for Windows Authentication	At least 3 selectable questions	Specify the questions to present to Windows users during recovery questions setup. Separate each question by a carriage return. These questions are used if the Windows password is forgotten. At least 3 questions must be specified. What is your mother's maiden name? What was the name of the first school you attended? What is the name of your first pet? What is your father's middle name? What is your mother's middle name? Who was your first employer? Who was your first teacher? What city were you born in? What city was your mother born in? What city was your father born in? What was the first concert you attended? Who is your favorite TV show character? What was the name of your first stuffed animal? What was the make of the first car you owned? Where did you spend your honeymoon? Where did you meet your spouse? What is your oldest cousin's name? What is your oldest niece's name? What is your oldest nephew's name? What is your youngest child's nickname? What is your oldest child's nickname? What was the last name of your third grade teacher? In what city or town did your mother and father meet? In what city or town was your first job?
Allow Recovery Questions	Not Selected	*Selected* *Not Selected* Set to Selected to allow users to use recovery questions/answers to log on to Windows.
Log Events Level	Audit	*Errors* *Audit* *Details* Level of detail in Windows Event logs. Determines whether events such as fingerprint registration and authentication attempts are logged in the Windows Event log. Each higher level includes all previous levels. Events are logged on the computer where they occur. Normally, the auditing level provides sufficient detail, covering all logon, authentication, fingerprint management, and user management events. The details levels can fill the log file very quickly. Status

		events provide information about the state of several important systems on the computer. They are logged on configurable intervals and generally used when events are remotely collected.
False Accept Rate of Fingerprint	Medium High - 1 in 100,000	The False Accept Rate is the probability of receiving a false acceptance decision when comparing fingerprints scanned from different fingers. You can select one of the following FAR values: * Medium (1 in 10,000) * Medium High (1 in 100,000) * High (1 in 1,000,000) For example: if you select Medium High, on average, one false acceptance will occur when a fingerprint is compared against one hundred thousand fingerprints scanned from different fingers. The higher the setting, the lower the chance of receiving a false acceptance. However, at the High setting, the system may reject legitimate fingerprints. **NOTE**: The FAR is set on a per verification basis. When matching a fingerprint against fingerprints of multiple users (identification), the internally used FAR is automatically adjusted to maintain the same effective FAR as was selected for a single match.
Minimum Number of Fingerprints to Enroll	2	The minimum number of fingerprints required to be enrolled.
Maximum Number of Fingerprints to Enroll	10	The maximum number of fingerprints required to be enrolled.
Allow Users to Enroll Credentials	Selected	Set to Selected to allow users to enroll their own credentials without administrator involvement.
Allow Users to Modify Credentials	Selected	Set to Selected to allow users to modify their own credentials that have been previously set up or enrolled.

Reminder to Enroll Credentials (Admin)	In one day	Values for reminders: Disable Reminder At Next Logon In One Day In One Week Every Two Hours
Reminder to Enroll Credentials Expiration Date (Admin)	Now	The date (time is always 12 am) when authentication policy is going into full effect. Meaning, the client stops asking the local administrator to enroll credentials and forces them to enroll before they can logon. The default is “now”.
Reminder to Enroll Credentials (User)	In one day	Values for reminders: Disable Reminder At Next Logon In One Day In One Week Every Two Hours
Reminder to Enroll Credentials Expiration Date (User)	Now	The date (time is always 12 am) when authentication policy is going into full effect. Meaning, the client stops asking the user to enroll credentials and forces them to enroll before they can logon. The default is “now”.
Action Upon Smart Card Removal	Lock Workstation	*No Action* *Lock Workstation* *Force Logoff* *Disconnect if on a Remote Desktop session* The action that occurs when a smart card is removed from the computer.

Threat Prevention

Threat Prevention

Threat Prevention policies are available at the Enterprise, Endpoint Group, and Endpoint levels.

Policy descriptions also display in tooltips in the Management Console. In this table, master policies are in bold font.

Policy	Default Setting	Description
Advanced Threat Prevention This technology is powered by Cylance and protects your operating system by detecting and preventing malware pre-execution. Advanced Threat Prevention uses artificial intelligence and predictive mathematical models to quickly and accurately identify what is safe and what is a threat.		
Advanced Threat Prevention	Off	*On* *Off* Toggle ON to enable Advanced Threat Prevention. If

		this policy is toggled to OFF, Advanced Threat Prevention is disabled, regardless of other policies.
File Actions		
Unsafe Executable Auto Quarantine with Executable Control Enabled	Selected	*Selected* *Not Selected* If selected, Unsafe executable files are automatically quarantined or blocked to prevent their execution. Note: If you Auto Quarantine, it is highly recommended that before deployment, you test Auto Quarantine only on devices using a test policy to observe the behavior and ensure that no business-critical applications are blocked at execution.
Abnormal Executable Auto Quarantine with Executable Control Enabled	Selected	*Selected* *Not Selected* If selected, Abnormal executable files are automatically quarantined or blocked to prevent their execution. Note: If you Auto Quarantine, it is highly recommended that before deployment, you test Auto Quarantine only on devices using a test policy to observe the behavior and ensure that no business-critical applications are blocked at execution.
Memory Actions		
Memory Protection Enabled	Not Selected	*Selected* *Not Selected* This policy must be selected to use all other Memory policies. If this policy is Not Selected, no Memory Action policies are enforced, regardless of other policy values. NOTE: Before enabling Memory Protection, enable Compatibility Mode, to ensure applications function properly on the client computer. For instructions on how to enable Compatibility Mode, see Enable Compatibility Mode for Memory Protection.htm. Compatibility Mode does not apply to Mac clients.
See **advanced settings**		

Policy	Default Setting	Description
Threat Protection This technology protects computers by identifying and taking action against threats of malware and malicious activity involving files, folders, the registry, and processes.		
Threat Protection	Off	*On* *Off* Toggle to ON to enable Threat Protection. If toggled to OFF, no Threat Protection policies are applied. Threat Protection includes Malware Protection, Web Protection, and Client Firewall.
Exploit Protection	Selected	*Selected* *Not Selected* This policy is the "master policy" for all other Exploit Protection policies. If this policy is Not Selected, no Exploit Protection policies are enforced, regardless of other policy values. A Selected value means that Exploit Protection is enabled. Exploit Protection monitors for application vulnerabilities and keeps buffer overflow exploits

		from executing arbitrary code on the computer. This policy must be set to Selected to enable Exploit Protection. If this policy is Not Selected, no Exploit Prevention policies are applied.
Action on Malicious Activity for Files and Folders	Block and Report	*Block Only* *Report Only* *Block and Repor*t Prevents users from modifying or deleting Threat Protection system files and folders and sets the action to take upon attempt. Block Only: Blocks activity but does not report to the server. Report Only: Reports activity to the server but does not block activity. Block and Report (default): Blocks and reports activity to the server.
Action on Malicious Activity for Registry	Block and Report	*Block Only* *Report Only* *Block and Repor*t Prevents users from modifying or deleting Threat Protection registry keys and values and sets the action to take upon attempt. Block Only: Blocks activity but does not report to the Server. Report Only: Reports activity to the Server but does not block activity. Block and Report (default): Blocks and reports activity to the Server.
On-Access Protection	Selected	*Selected* *Not Selected* This policy is the "master policy" for all other On-Access Protection policies. If this policy is Not Selected, no On-Access Protection policies are enforced, regardless of other policy values. A Selected value means that On-Access Protection is enabled. This policy must be set to Selected to enable On-Access Protection. If this policy is Not Selected, no On-Access Protection policies are applied.
See advanced settings		
Policy	**Default Setting**	**Description**
Web Protection This technology protects computers by leveraging a web-based content ranking system to determine if a site that a user is browsing is considered safe or not. This technology also grants the administrator the ability to define what happens when an unsafe site is navigated to (allow, block, warn).		
Web Protection	Off	*On* *Off* Toggle to ON to enable Web Protection. If toggled to OFF, no Web Protection policies are applied.
Enforcement - Action to Apply to Sites Not Verified	Allow	*Block* *Allow* *Warn* Specifies the default action to apply to sites that have not been verified. Block: Prevents users from accessing the site and displays a message that the site is blocked. Allow: Permits users to access the site.

		Warn: Displays a warning to notify users of potential dangers associated with the site. Users must dismiss the warning before continuing.
Enforcement - Enable File Scanning for File Downloads	Selected	*Selected* *Not Selected* A Selected value scans all files (including .zip files) before downloading. This option prevents users from accessing a downloaded file until Threat Protection marks the file as clean. Downloaded files are sent to Threat Protection for scanning. Threat Protection performs a Reputation Service lookup on the file. If a downloaded file is detected as a threat, Threat Protection takes action on the file and alerts the user.
Enable Secure Search	Not Selected	*Selected* *Not Selected* A Selected value enables Secure Search, automatically blocking malicious sites in search results based on safety rating.
Block Links to Risky Sites in Search Results	Not Selected	*Selected* *Not Selected* A Selected value prevents users from clicking links to risky sites in search results.
See advanced settings		
Policy	Default Setting	Description
Client Firewall This technology protects computers by allowing administrators to determine which network traffic is permitted to pass between end user computers and the network.		
Client Firewall	Off	*On* *Off* Toggle to ON to enable Client Firewall. If toggled to OFF, no Client Firewall Settings or Rules are applied. Client firewall is a stateful firewall.
See advanced settings		
Policy	Default Setting	Description
Protection Settings This technology allows control over Threat Prevention settings such as display of threat event notifications on the client computer and Web Protection and Client Firewall logging.		
Suppress Popup Notifications	Not Selected	*Selected* *Not Selected* If Selected, popup notifications of Advanced Threat Prevention events are disabled on the computer.
Minimum Popup Notification Level	High	*High* *Medium* *Low* Severity level of events that result in popup notifications that display on the computer. High allows only notifications of critical events to display. Low displays all on-screen notifications for all events. Listed below are examples of events:

		High 1) Protection status has changed. (Protected means that the Advanced Threat Prevention service is running and protecting the computer and needs no user or administrator interaction.) 2) A threat is detected and policy is not set to automatically address the threat. **Medium** 1) Execution Control blocked a process from starting because it was detected as a threat. 2) A threat is detected that has an associated mitigation (for example, the threat was manually quarantined), so the process has been terminated. 3) A process was blocked or terminated due to a memory violation. 4) A memory violation was detected and no automatic mitigation policy is in effect for that violation type. **Low** 1) A file that was identified as a threat has been added to the Global Safe List or deleted from the file system. 2) A threat has been detected and automatically quarantined. 3) A file has been identified as a threat, but waived on the computer. 4) The status of a current threat has changed (for example, Threat > Quarantined, Quarantined > Waived, or Waived > Quarantined).
Log Files Location	<SYSTEM_DRIVE>:\ProgramData\DDP\Suite\Logs	String - File path Specifies the location for the log files. The default location is <SYSTEM_DRIVE>:\ProgramData\DDP\Suite\Logs.
Enable Activity Logging	Selected	*Selected* *Not Selected* This policy is the "master policy" for all other Threat Protection logging policies. If this policy is Not Selected, no Threat Protection logging takes place, regardless of other policy values. A Selected value enables Threat Protection logging.
Debug Logging for Web Protection	Not Selected	Selected Not Selected A Selected value enables verbose logging of Web Protection activity.
Debug Logging for Client Firewall	Not Selected	Selected Not Selected A Selected value enables verbose logging of Firewall activity.

Advanced Threat Prevention

Threat Prevention policies are available at the Enterprise, Endpoint Group, and Endpoint levels.

Policy descriptions also display in tooltips in the Management Console. In this table, master policies are in bold font.

Policy	Default Setting	Description

Advanced Threat Prevention This technology is powered by Cylance and protects your operating system by detecting and preventing malware pre-execution. Advanced Threat Prevention uses artificial intelligence and predictive mathematical models to quickly and accurately identify what is safe and what is a threat.		
Advanced Threat Prevention	Off	*On* *Off* Toggle ON to enable Advanced Threat Prevention. If this policy is toggled to OFF, Advanced Threat Prevention is disabled, and policies are set to defaults for activated devices. This results in Execution Control blocking threats, but Auto Quarantine, Memory Protection, and Script Control will be disabled.
File Actions		
Unsafe Executable Auto Quarantine With Executable Control Enabled	Selected	*Selected* *Not Selected* If selected, Unsafe executable files are automatically quarantined or blocked to prevent their execution. Note: If you Auto Quarantine, it is highly recommended that before deployment, you test Auto Quarantine only on devices using a test policy to observe the behavior and ensure that no business-critical applications are blocked at execution.
Unsafe Executable Auto Upload Enabled	Selected	*Selected* *Not Selected* If selected, any detected Unsafe file is automatically uploaded for a deeper analysis and additional details about the file.
Abnormal Executable Auto Quarantine With Executable Control Enabled	Selected	*Selected* *Not Selected* If selected, Abnormal executable files are automatically quarantined or blocked to prevent their execution. Note: If you Auto Quarantine, it is highly recommended that before deployment, you test Auto Quarantine only on devices using a test policy to observe the behavior and ensure that no business-critical applications are blocked at execution.
Abnormal Executable Auto Upload Enabled	Selected	*Selected* *Not Selected* If selected, any detected Abnormal file is automatically uploaded for a deeper analysis and additional details about the file.
Allow Execution of Files in Exclude Folders	Not Selected	*Selected* *Not Selected* If selected, executable files are allowed to run, even if they are in folders excluded in the Exclude Specific Folders policy.
Auto Delete	Not Selected	*Selected* *Not Selected* If selected, after the time period specified in the Days until Deleted policy, files that are quarantined on an endpoint are automatically deleted.
Days until Deleted	14	*14-365 days* Number of days until files that are quarantined on an endpoint are automatically deleted.
Memory Actions		

Memory Protection Enabled	Not Selected	*Selected* *Not Selected* This policy must be selected to use all other Memory policies. If this policy is Not Selected, no Memory Action policies are enforced, regardless of other policy values. NOTE: Before enabling Memory Protection, enable Compatibility Mode, to ensure applications function properly on the client computer. For instructions on how to enable Compatibility Mode, see Enable Compatibility Mode for Memory Protection. Compatibility Mode does not apply to Mac clients.
Enable Exclude executable files	Selected	*Selected* *Not Selected* Allow specific process files to be excluded from Memory Protection. This policy must be selected to use the Exclude executable files policy.
Exclude executable files	String \Windows\System32\CmgShieldService.exe \Windows\System32\EMSService.exe \Program Files\Dell\Dell Data Protection\Threat Protection\DellAVAgent.exe \Program Files\McAfee\Agent\cmdagent.exe \Program Files\McAfee\Agent\FrmInst.exe \Program Files\McAfee\Agent\macmnsvc.exe \Program Files\McAfee\Agent\macompatsvc.exe \Program Files\McAfee\Agent\maconfig.exe \Program Files\McAfee\Agent\masvc.exe \Program Files\McAfee\Agent\x86\FrmInst.exe \Program Files\McAfee\Agent\x86\macompatsvc.exe \Program Files\McAfee\Agent\x86\marepomirror.exe \Program Files\McAfee\Agent\x86\McScanCheck.exe \Program Files\McAfee\Agent\x86\McScript_InUse.exe \Program Files\McAfee\Agent\x86\mctray_back.exe \Program Files\McAfee\Agent\x86\Mue.exe \Program Files\McAfee\Agent\x86\policyupgrade.exe \Program Files\McAfee\Agent\x86\UpdaterUI.exe \Program Files\McAfee\Endpoint Security\Endpoint Security Platform\ESConfigTool.exe \Program Files\McAfee\Endpoint Security\Endpoint Security Platform\MFEConsole.exe \Program Files\McAfee\Endpoint Security\Endpoint Security Platform\mfeesp.exe \Program Files\McAfee\Endpoint Security\Endpoint Security Platform\mfeProvisionModeUtility.exe \Program Files\McAfee\Endpoint Security\Endpoint Security Platform\PwdUninstall.exe \Program Files\McAfee\Endpoint Security\Endpoint Security Platform\RepairCache\CCUninst.exe \Program Files\McAfee\Endpoint Security\Endpoint Security Platform\RepairCache\McAfee_Common_x64.exe \Program Files\McAfee\Endpoint Security\Endpoint Security Platform\RepairCache\McAfee_Common_x64.msi \Program Files\McAfee\Endpoint Security\Endpoint Security Platform\RepairCache\McAfee_Common_x86.msi \Program Files\McAfee\Endpoint Security\Endpoint Security Platform\RepairCache\setupCC.exe \Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\aacinfo.exe \Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\cacheinfo.exe \Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\fwinfo.exe	*String* Exclude specific process files from Memory Protection. This allows the specified files to run or be installed on any device on which this policy is enforced. All exclusions added must be specified using the relative path of that executable file (exclude the drive letter from the path). Correct (Windows): \Application\SubFolder\application.exe Correct (Mac): /Users/application.app/executable Incorrect: \Application\SubFolder\ Incorrect: C:\Application\SubFolder\application.exe

	\Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\mfecanary.exe \Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\mfefire.exe \Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\mfehidin.exe \Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\mfemms.exe \Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\mfevtps.exe \Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\mmsinfo.exe \Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\vtpinfo.exe \Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\aacinfo.exe \Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\cacheinfo.exe \Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\fwinfo.exe \Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\mfecanary.exe \Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\mfefire.exe \Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\mfehidin.exe \Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\mfemms.exe \Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\mfevtps.exe \Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\mmsinfo.exe \Program Files\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\vtpinfo.exe \Program Files\McAfee\Endpoint Security\Firewall\FWInstCheck.exe \Program Files\McAfee\Endpoint Security\Firewall\FwWindowsFirewallHandler.exe \Program Files\McAfee\Endpoint Security\Firewall\mfefw.exe \Program Files\McAfee\Endpoint Security\Firewall\RepairCache\McAfee_Firewall_x64.msi \Program Files\McAfee\Endpoint Security\Firewall\RepairCache\McAfee_Firewall_x86.msi \Program Files\McAfee\Endpoint Security\Firewall\RepairCache\setupFW.exe \Program Files\McAfee\Endpoint Security\Web Control\McChHost.exe \Program Files\McAfee\Endpoint Security\Web Control\mfewc.exe \Program Files\McAfee\Endpoint Security\Web Control\mfewch.exe \Program Files\McAfee\Endpoint Security\Web Control\mfewcui.exe \Program Files\McAfee\Endpoint Security\Web Control\RepairCache\McAfee_Web_Control_x86.msi \Program Files\McAfee\Endpoint Security\Web Control\RepairCache\setupWC.exe \Program Files\McAfee\marepomirror.exe \Program Files\McAfee\McScanCheck.exe \Program Files\McAfee\McScript_InUse.exe	

	\Program Files\McAfee\mctray_back.exe \Program Files\McAfee\Mue.exe \Program Files\McAfee\policyupgrade.exe \Program Files\McAfee\UpdaterUI.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\MaComServer.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\MFEConsole.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\mfeProvisionModeUtility.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\RepairCache\CCUninst.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\aacinfo.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\cacheinfo.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\fwinfo.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\mfecanary.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\mfefire.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\mfehidin.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\mfemms.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\mfevtps.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\mmsinfo.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\Release\vtpinfo.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\aacinfo.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\cacheinfo.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\fwinfo.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\mfecanary.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\mfefire.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\mfehidin.exe \Program Files (x86)\McAfee\Endpoint	

	Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\mfemms.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\mfevtps.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\mmsinfo.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform\VSCore_ENS_10.1\x64\vtpinfo.exe \Program Files (x86)\McAfee\Endpoint Security\Web Control\McChHost.exe \Program Files (x86)\McAfee\Endpoint Security\Web Control\mfewc.exe \Program Files (x86)\McAfee\Endpoint Security\Web Control\mfewch.exe \Program Files (x86)\McAfee\Endpoint Security\Web Control\mfewcui.exe \Program Files (x86)\McAfee\Endpoint Security\Web Control\RepairCache\McAfee_Web_Control_x64.msi \Program Files (x86)\McAfee\Endpoint Security\Web Control\RepairCache\setupWC.exe \Program Files (x86)\McAfee\Endpoint Security\Web Control\x64\mfewch.exe \Windows\System32\mfevtps.exe \Program Files\McAfee\Endpoint Security\Endpoint Security Platform\LogDebugSetter.exe \Program Files\McAfee\Endpoint Security\MfeUpgradeTool.exe	
Exploitation: Stack Pivot	Alert	*Ignore* *Alert* *Block* *Terminate* Specify the action to take when a stack pivot threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the Dell Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and terminate the application that made the call. Stack Pivot - The stack for a thread has been replaced with a different stack. Generally the system will only allocate a single stack for a thread. An attacker would use a different stack to control execution in a way that is not blocked by Data Execution Prevention (DEP). The Stack Pivot exploitation affects Windows and macOS operating systems.

Exploitation: Stack Protect	Alert	*Ignore* *Alert* *Block* *Terminate* Specify the action to take when a stack protect threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the Dell Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and terminate the application that made the call. Stack Protect - The memory protection of a thread's stack has been modified to enable execution permission. Stack memory should not be executable, so usually this means that an attacker is preparing to run malicious code stored in stack memory as part of an exploit, an attempt which would otherwise be blocked by Data Execution Prevention (DEP). The Stack Protect exploitation affects Windows and macOS operating systems.
Exploitation: Overwrite Code	Alert	*Ignore* *Alert* *Block* *Terminate* Specify the action to take when an overwrite code threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the Dell Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and terminate the application that made the call. Overwrite Code - Code residing in a process's memory has been modified using a technique that may indicate an attempt to bypass Data Execution Prevention (DEP). The Overwrite Code exploitation affects Windows operating systems. This policy does not apply to Mac clients.
Exploitation: Scanner Memory Search	Alert	*Ignore* *Alert* *Block* *Terminate* Specify the action to take when a scanner memory search threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the Dell Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and terminate the application that made the call. Scanner Memory Search, or RAM Scraping - A process is

		trying to read valid magnetic stripe track data from another process. Typically related to point-of-sale systems (POS). The Scanner Memory Search exploitation affects Windows operating systems. This policy does not apply to Mac clients.
Exploitation: Malicious Payload	Alert	*Ignore* *Alert* *Block* *Terminate* Specify the action to take when a malicious payload is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the Dell Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and terminate the application that made the call. Malicious Payload - A generic shellcode and payload detection associated with exploitation has been detected. The Malicious Payload exploitation affects Windows operating systems. This policy does not apply to Mac clients.
Process Injection: Remote Allocation of Memory	Alert	*Ignore* *Alert* *Block* *Terminate* Specify the action to take when a remote memory allocation threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the Dell Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and terminate the application that made the call. Remote Allocation of Memory - A process has allocated memory in another process. Most allocations will only occur within the same process. This generally indicates an attempt to inject code or data into another process, which may be a first step in reinforcing a malicious presence on a system. The Remote Allocation of Memory process injection affects Windows and macOS operating systems.

Process Injection: Remote Mapping of Memory	Alert	*Ignore* *Alert* *Block* *Terminate* Specify the action to take when a remote attempt to map memory threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the Dell Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and terminate the application that made the call. Remote Mapping of Memory - A process has introduced code and/or data into another process. This may indicate an attempt to begin executing code in another process and thereby reinforce a malicious presence. The Remote Mapping of Memory process injection affects Windows and macOS operating systems.
Process Injection: Remote Write to Memory	Alert	*Ignore* *Alert* *Block* *Terminate* Specify the action to take when a remote attempt to write to memory threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the Dell Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and terminate the application that made the call. Remote Write to Memory - A process has modified memory in another process. This is usually an attempt to store code or data in previously allocated memory but it is possible that an attacker is trying to overwrite existing memory to divert execution for a malicious purpose. The Remote Write to Memory process injection affects Windows and macOS operating systems.
Process Injection: Remote Write PE to Memory	Alert	*Ignore* *Alert* *Block* *Terminate* Specify the action to take when a remote attempt to write a portable executable to memory threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the Dell Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and terminate the application that made the call. Remote Write PE to Memory - A process has modified memory in another process to contain an executable image.

		Generally this indicates that an attacker is attempting to execute code without first writing that code to disk. The Remote Write PE to Memory process injection affects Windows operating systems. This policy does not apply to Mac clients.
Process Injection: Remote Overwrite Code	Alert	*Ignore* *Alert* *Block* *Terminate* Specify the action to take when a remote overwrite code threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the Dell Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and terminate the application that made the call. Remote Overwrite Code - A process has modified executable memory in another process. Under normal conditions executable memory is not modified, especially by another process. This usually indicates an attempt to divert execution in another process. The Remote Overwrite Code process injection affects Windows operating systems. This policy does not apply to Mac clients.
Process Injection: Remote Unmap of Memory	Alert	*Ignore* *Alert* *Block* *Terminate* Specify the action to take when a remote memory unmapping threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the Dell Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and terminate the application that made the call. Remote Unmap of Memory - A process has removed a Windows executable from the memory of another process. This may indicate an intent to replace the executable image with a modified copy for the purpose of diverting execution. The Remote Unmap of Memory process injection affects Windows operating systems. This policy does not apply to Mac clients.

Process Injection: Remote Thread Creation	Alert	*Ignore* *Alert* *Block* *Terminate* Specify the action to take when a remote thread creation threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the Dell Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and terminate the application that made the call. Remote Thread Creation - A process has created a new thread in another process. A process's threads are usually only created by that same process. This is generally used by an attacker to activate a malicious presence that has been injected into another process. The Remote Thread Creation process injection affects Windows and macOS operating systems.
Process Injection: Remote APC Scheduled	Alert	*Ignore* *Alert* *Block* *Terminate* Specify the action to take when a remote APC scheduled threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the Dell Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and terminate the application that made the call. Remote APC Scheduled - A process has diverted the execution of another process's thread. This is generally used by an attacker to activate a malicious presence that has been injected into another process. The Remote APC Scheduled process injection affects Windows operating systems. This policy does not apply to Mac clients.
Process Injection: Remote DYLD Injection (Mac OS X only)	Alert	*Ignore* *Alert* *Block* *Terminate* Specify the action to take when a remote DYLD injection threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the Dell Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and terminate the application that made the call. DYLD Injection - An environment variable has been set to

		cause a shared library to be injected into a launched process. Attacks can modify the plist of applications like Safari or replace applications with bash scripts, that cause their modules to be loaded automatically when an application starts. The DYLD Injection process injection affects macOS operating systems. This policy does not apply to Windows clients.
Escalation: LSASS Read	Alert	*Ignore* *Alert* *Block* *Terminate* Specify the action to take when an LSASS read threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the Dell Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and terminate the application that made the call. LSASS Read - Memory belonging to the Windows Local Security Authority process has been accessed in a manner that indicates an attempt to obtain users' passwords. The LSASS Read escalation affects Windows operating systems. This policy does not apply to Mac clients.
Escalation: Zero Allocate	Alert	*Ignore* *Alert* *Block* *Terminate* Specify the action to take when a zero byte allocation threat is detected. Ignore - No action is taken against identified memory violations. Alert - Record the violation and report the incident to the Dell Server. Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run. Terminate - Block the process call if an application attempts to call a memory violation process and terminate the application that made the call. Zero Allocate - A null page has been allocated. The memory region is typically reserved, but in certain circumstances it can be allocated. Attacks can use this to setup privilege escalation by taking advantage of some known null de-reference exploit, typically in the kernel. The Zero Allocate escalation affects Windows and macOS operating systems.
Execution Control		

Prevent Service Shutdown from Device	Not Selected	*Selected* *Not Selected* If selected, the Advanced Threat Prevention service is protected from being shut down either manually or by another process.
Kill Unsafe Running Processes and Sub-Processes	Not Selected	*Selected* *Not Selected* If selected, processes and sub-processes are quarantined and terminated regardless of their state when a threat is detected (exe or dll). Although a process or sub-process is terminated, the command prompt window remains open. If a file has been determined to be Safe and allowed to run and then a threat model update occurs that results in the file being identified as unsafe, the process is automatically terminated. Dell recommends that you review threat model updates before Selecting this policy. For more information, see Threat Model Updates.
Background Threat Detection	Run Once	*Disabled* *Run Recurring* *Run Once* If set to Run Recurring or Run Once, a full-disk scan is run to detect and analyze any dormant threats on the disk. An update to the Threat Model triggers a full-disk scan.
Watch for New Files	Selected	*Selected* *Not Selected* If selected, any new or modified files are detected and analyzed for dormant threats. Dell recommends enabling this policy. However, If Auto Quarantine is enabled for all Unsafe or Abnormal files, all malicious files are blocked at execution. Therefore, it is not necessary to enable this policy with Auto Quarantine mode unless you prefer to quarantine a file as it is added to a disk but before execution.
Set Maximum Archive File Size to Scan	150 MB	The default setting is 150 MB. Specify the maximum size of archive (compressed) files, including .jar files to be scanned. Because scanning compressed files can negatively affect computer performance, Dell recommends Quick-Scan - Scan Archives and Full-Scan - Scan Archives to run during off-work hours.
Protection Settings		
Enable Exclude Specific Folders (includes subfolders)	Selected	*Selected* *Not Selected* Allow specific folders to be excluded from Auto Quarantine and Auto Upload. This policy must be Selected to use the Exclude Specific Folders policy.
Exclude Specific Folders (includes subfolders)	String	*String* Folders specified in this policy are excluded from actions performed based on Background Threat Detection and Watch for New Files, when these policies are enabled. This exclusion extends to subfolders of folders that are specified in this policy. All exclusions must be specified using the Absolute path of that executable file. Windows requires an absolute path (requires a drive letter) Mac requires an absolute path (macOS does not use a drive letter) Correct (Windows): C:\Program Files\Dell Correct (Mac): /Mac\ HD/Users/Application\ Support/Dell Incorrect: C:\Program Files\Dell\Executable.exe

		Incorrect: \Program Files\Dell\ Spaces only must be escaped on Mac-based exclusions.
Application Control		
Application Control	Not Selected	*Selected* *Not Selected* If Selected, specified devices are locked down, restricting any changes. Only applications that exist on a device before the lock-down are allowed to execute on that device. Any new applications, as well as changes to the executables of existing applications, are denied. The Advanced Threat Prevention agent updater is also disabled. Additionally, certain File Action, Memory Action, and Execution Control policies are automatically set. These policies may be changed after they are automatically set, without disabling Application Control. See Policies Set by Application Control for a list of policies that are automatically set when the Application Control policy is Selected. To exclude specific folders from lockdown, specify the folders in the Application Control Allowed Folders policy.
Application Control Allowed Folders	String	*String* Specify folders to be excluded from Application Control lockdown.
Enable Change Window	Not Selected	*Selected* *Not Selected* If selected, Application Control is temporarily disabled to allow, edit, and run new applications or perform updates. This includes updating the Advanced Threat Prevention agent. After performing the necessary changes, deselect Enable Change Window. **Note:** Enable Change Window retains changes made to Application Control. Deselecting Application Control and resetting back to Selected resets Application Control to default values. This policy does not apply to Mac clients.
Script Control		
Script Control	Not Selected	*Selected* *Not Selected* If Selected, Script Control protects devices by blocking malicious scripts from running. **Note:** Script Control is currently only available for PowerShell and Active Scripts.
Script Control Mode	Alert	*Alert* *Block* Alert monitors scripts running in the environment. Recommended for initial deployment. Block allows scripts to run only from specific folders. This should be used only after testing in Alert mode.
Active Script	Alert	*Alert* *Block* Alert monitors Active Scripts running in the environment. Recommended for initial deployment. Block allows Active Scripts **to run only from specific folders. This should be used only after testing in Alert mode.**
Macros	Alert	*Alert*

		Block Alert monitors Office macros running in the environment. Recommended for initial deployment. Block allows Office macros **to run only from specific folders. This should be used only after testing in Alert mode.** **Note:** Starting with Office 2013, macros are disabled by default. Most of the time, users should not be required to enable macros to view the content of an Office document. Dell recommends enabling macros only for documents from trusted users. Otherwise, macros should always be disabled.
PowerShell	Alert	*Alert* *Block* Alert (default) - Monitors PowerShell scripts running in the environment. Recommended for initial deployment. Block - Allow PowerShell scripts to run only from specific folders. This should be used only after testing in Alert mode. This policy does not apply to Mac clients.
PowerShell Console	Allow	*Allow* *Block* Allow (default) - Allows the PowerShell v3 console to be launched. Block - Blocks the PowerShell v3 console from being launched. Provides additional security by protecting against the use of PowerShell one-liners. Note: If this policy is set to Block and you use a script that launches the PowerShell console, the script will fail. It is recommended that users change their scripts to invoke the PowerShell scripts, not the PowerShell console. This policy applies only to PowerShell v3 and does not apply to Mac clients.
Enable Approve Scripts in Folders (and Subfolders)	Not Selected	*Selected* *Not Selected* Allows scripts stored in specific folders to be automatically approved to run. This policy must be selected to use the Script Control Approve Scripts in Folders (and Subfolders policy).
Approve Scripts in Folders (and Subfolders)	String	*String* Folders specified in this policy are excluded from actions performed based on the Script Control policy. This exclusion extends to subfolders of folders that are specified with this policy. A folder must be specified using its ***relative*** path. A path may not include the drive letter. Example: \Cases\ScriptsAllowed A specified path may represent any of the following: - local drive path - mapped network drive path - universal naming convention (UNC) path
Quarantine	String	*String* The value of this policy includes a collection of hashes for portable executable that need to be automatically quarantined within the Endpoint Group or on the specific Endpoint. This policy will force quarantine files based on a SHA256 hash of the specific portable executable.

Waive	String	*String* The value of this policy includes a collection of hashes for portable executable that need to be allowed to run within the Endpoint Group or on the specific Endpoint. This policy will force allow files based on a SHA256 hash of the specific portable executable.
Global Allow	String	*String* This policy defines a change to the local math model to prevent problematic portable executable to properly run on the machine. This is used in situations where normal exclusions may not properly apply to the files that are needing to be waived. The value of this policy will consist of an XML blob that can be provided by support if it is required. The value of this policy must include the entire contents of the policy.xml file. Copy and paste the contents of policy.xml into the policy editor as shown in this example.
Global Quarantine List	String	*String* The value of this policy includes a collection of hashes for portable executable that need to be automatically quarantined within the enterprise. This policy will force quarantine files based on a SHA256 hash of the specific portable executable.
Global Safe List	String	*String* The value of this policy includes a collection of hashes for portable executable that need to be allowed to run within the enterprise. This policy will force allow files based on a SHA256 hash of the specific portable executable.
Agent Settings		
Suppress Popup Notifications	Not Selected	*Selected* *Not Selected* If Selected, popup notifications for Advanced Threat Prevention events do not display on the client computer.
Minimum Popup Notification Level	High	*High* *Medium* *Low* Severity level of events that result in popup notifications that display on the client computer. A setting of High allows only notifications of critical events to display. A setting of Low displays all on-screen notifications for all events. Listed below are examples of events that fall into the severity levels: High 1) Protection status has changed. (Protected means that the Advanced Threat Prevention service is running and protecting the computer and needs no user or administrator interaction.) 2) A threat is detected and policy is not set to automatically address the threat. Medium 1) Execution Control blocked a process from starting because it was detected as a threat. 2) A threat is detected that has an associated mitigation (for example, the threat was manually quarantined), so the process has been terminated. 3) A process was blocked or terminated due to a memory violation. 4) A memory violation was detected and no automatic mitigation policy is in effect for that violation type. Low 1) A file that was identified as a threat has been added to the Global Safe List or deleted from the file system. 2) A threat has been detected and automatically

		quarantined. 3) A file has been identified as a threat but waived on the computer. 4) The status of a current threat has changed (for example, Threat to Quarantined, Quarantined to Waived, or Waived to Quarantined).
Enable BIOS Assurance	Selected	*Selected* *Not Selected* If selected, BIOS integrity checks are performed on endpoints computers to validate that the BIOS has not been modified from the Dell factory version. A custom factory image cannot be used with this feature, as the BIOS has been modified. This feature is available only on Dell platforms. Platforms available with this feature include the newest release of select XPS, Latitude, Optiplex, Precision Workstations, and Venues. Speak to your Sales Associates for details or contact Dell ProSupport. This policy does not apply to Mac clients.
Enable Auto-upload of Log Files	Not Selected	*Selected* *Not Selected* If selected, log files are automatically uploaded at 12:00 am or when their size reaches 100 MB. If this policy is Not Selected, logs can still be manually uploaded.
Enable Standard UI	Not Selected	*Selected* *Not Selected* If Selected, the User Interface that will show individual details for threat events that have occurred on the local client is enabled.
See basic settings		
Policy	Default Setting	Description
Threat Protection This technology protects computers by identifying and taking action against threats of malware and malicious activity involving files, folders, the registry, and processes.		

Threat Protection	Off	*On* *Off* Toggle to ON to enable Threat Protection. If toggled to OFF, no Threat Protection policies are applied. Threat Protection includes Malware Protection, Web Protection, and Client Firewall.
Action on Malicious Activity for Files and Folders	Block and Report	*Block Only* *Report Only* *Block and Report* Prevents users from modifying or deleting Threat Protection system files and folders and sets the action to take upon attempt. Block Only: Blocks activity but does not report to the Dell Server. Report Only: Reports activity to the Dell Server but does not block activity. Block and Report (default): Blocks and reports activity to the Dell Server.
Action on Malicious Activity for Registry	Block and Report	*Block Only* *Report Only* *Block and Report* Prevents users from modifying or deleting Threat Protection registry keys and values and sets the action to take upon attempt. Block Only: Blocks activity but does not report to the Dell Server. Report Only: Reports activity to the Dell Server but does not block activity. Block and Report (default): Blocks and reports activity to the Dell Server.
Action on Malicious Activity for Processes	Block and Report	*Block Only* *Report Only* *Block and Report* Prevents users from stopping Threat Protection processes and sets the action to take upon attempt. Block Only: Blocks activity but does not report to the Dell Server. Report Only: Reports activity to the Dell Server but does not block activity. Block and Report (default): Blocks and reports activity to the Dell Server.
Exclude Processes	String	String - Example: avtask.exe Excludes specific process files from Threat Protection scans. Enter the exact resource name of a process to exclude.
Client Update		
Schedule	Selected	*Selected* *Not Selected* This policy is the "master policy" for all other Client Scheduling policies. If this policy is Not Selected, no Client Scheduling takes place, regardless of other policy values. A Selected value enables the Client Scheduling options.

Schedule Repeats	Daily	*Daily* *Weekly* *Monthly* The schedule configuration defines when the task should run. Schedule types are Daily, Weekly, and Monthly. Daily: Runs the task every day at the specified Schedule Start Time. Weekly: Runs the task weekly on the days specified in Day of the Week. Monthly: Runs the task monthly on the specified Day of the Month.
Schedule Start Time	String	String - format is [HH:mm tt]. Example: 11:59 PM The time the task should run.
Day of the Week	Wednesday	*Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday* The day of the week the task should run.
Day of the Month	1	*1-31* The day of the month the task should run. Example: 17.
Debug Logging for Malware and Exploit Protection	Not Selected	*Selected* *Not Selected* A Selected value enables debug logging of Malware and Exploit Protection activity.
Exploit Protection	Off	*On* *Off* Toggle to ON to enable Exploit Protection. If toggled to OFF, no Exploit Protection policies are applied. Exploit Protection protects the critical operating system resources from changes made by malware or other unauthorized processes.
On-Access Protection	Off	*On* *Off* Toggle to ON to enable **On-Access** Protection. If toggled to OFF, no **On-Access** Protection policies are applied. **On-Access** Protection protects the critical operating system resources from changes made by malware or other unauthorized processes at the time a resource is accessed.
Max Seconds for Scan	45	*10 to 9999* Specifies the maximum number of seconds for each file scan. Limits each file scan to the specified number of seconds. If a scan exceeds the time limit, the scan stops and logs a message.
On-Access Scan		
Scan Boot Sectors	Selected	*Selected* *Not Selected* Examines the disk boot sector. Consider disabling this policy if a disk contains a unique or abnormal boot sector that cannot be scanned.

Scan Processes on Enable	Not Selected	*Selected* *Not Selected* Rescans all processes that are currently in memory each time: - On-Access Scan is disabled and re-enabled. - The computer starts. When the on-access scanner is enabled, it always scans all processes when they are executed. Because some programs or executables start automatically when the computer starts, enabling this option can slow the computer and increase computer startup time.
Scan Trusted Installers	Not Selected	*Selected* *Not Selected* Scans MSI files or Windows Trusted Installer service files. Disable this option to improve the performance of large Microsoft application installers.
Scan When Copying Between Local Folders	Not Selected	*Selected* *Not Selected* Scans files whenever the user copies from one local folder to another. If disabled, only items in the destination folder are scanned. If enabled, items in both source and destination folders are scanned.
Reputation Service Sensitivity	Medium	*Disable* *Very Low* *Low* *Medium* *High* *Very High* When enabled, samples are submitted to the lab to determine if they are malware. Sensitivity level configures the sensitivity level to use when determining if a detected sample is malware. The higher the sensitivity level, the higher the number of malware detections. However, allowing more detections might result in more false positive results. Risk levels: Very low - The detections and risk of false positives are the same as with regular content files. A detection is made available to Threat Protection when the lab publishes it instead of waiting for the next file update. Use this setting for desktops and servers with restricted user rights and a strong security footprint. This setting results in an average of 10–15 queries per day, per computer. Low - This setting is the minimum recommendation for laptops or desktops and servers with a strong security footprint. This setting results in an average of 10–15 queries per day, per computer. Medium - Use this level when the regular risk of exposure to malware is greater than the risk of a false positive. The proprietary, heuristic checks result in detections that are likely to be malware. However, some detections might result in a false positive. With this setting, the lab checks that popular applications and operating system files do not result in a false positive. This setting is the minimum recommendation for laptops or desktops and servers. This setting results in an average of 20–25 queries per day, per computer. High - Use this setting for deployment to systems or areas which are regularly infected. This setting results in an average of 20–25 queries per day, per computer. Very high - Dell recommends using this level only for scanning volumes and directories that do not support

		executing programs or operating systems. Detections found with this level are presumed malicious, but have not been fully tested to determine if they are false positives. Use this setting for on-demand scans on non-operating system volumes. This setting results in an average of 20–25 queries per day, per computer.
On-Demand Protection - Full Scan	Selected	*Selected* *Not Selected* This policy is the "master policy" for all other On-Demand Protection: Full Scan policies. If this policy is Not Selected, no On-Demand Protection: Full Scan policies are enforced, regardless of other policy values. A Selected value means that On-Demand Protection: Full Scan is enabled. This policy must be set to Selected to enable On-Demand Protection: Full Scan settings. If this policy is Not Selected, no On-Demand Protection: Full Scan policies are applied. By default, every time Full Scan runs, it scans the following locations for threats: - the computer memory for installed rootkits, hidden processes, and other behavior that suggests malware is attempting to hide itself. This scan occurs before all other scans. - the memory of all running processes. - all drives and their subfolders on the computer. By default, the scanner scans all file types, regardless of extension.
Full Scan		
Boot Sectors	Selected	*Selected* *Not Selected* Examines the disk boot sector. Consider disabling this policy if a disk contains a unique or abnormal boot sector that cannot be scanned.

Unwanted Programs	Selected	*Selected* *Not Selected* Enables the scanner to detect potentially unwanted programs. The scanner uses configured information to detect potentially unwanted programs.
Decode MIME Files	Not Selected	*Selected* *Not Selected* Detects, decodes, and scans Multipurpose Internet Mail Extensions (MIME) encoded files.
Scan Archives	Selected	*Selected* *Not Selected* Examines the contents of archive (compressed) files, including .jar files. Because scanning compressed files can negatively affect computer performance, Dell recommends using this option in scans during off-work hours.
Files Migrated to Storage	Not Selected	*Selected* *Not Selected* Scans files that remote storage manages. When the scanner encounters a file with migrated content, it restores the file to the local computer before scanning.
Program Threats	Selected	*Selected* *Not Selected* Detects executable files that have code that resembles malware.
Macro Threats	Selected	*Selected* *Not Selected* Detects unknown macro viruses.
Scan Subfolders	Selected	*Selected* *Not Selected* Examines all subfolders of the specified folder.

Reputation Service Sensitivity	Medium	*Disable* *Very Low* *Low* *Medium* *High* *Very High* When enabled, samples are submitted to the lab to determine if they are malware. Sensitivity level configures the sensitivity level to use when determining if a detected sample is malware. The higher the sensitivity level, the higher the number of malware detections. However, allowing more detections might result in more false positive results. Risk levels: Very low - The detections and risk of false positives are the same as with regular content files. A detection is made available to Threat Protection when the lab publishes it instead of waiting for the next content file update. Use this setting for desktops and servers with restricted user rights and a strong security footprint. This setting results in an average of 10–15 queries per day, per computer. Low - This setting is the minimum recommendation for laptops or desktops and servers with a strong security footprint. This setting results in an average of 10–15 queries per day, per computer. Medium - Use this level when the regular risk of exposure to malware is greater than the risk of a false positive. The proprietary, heuristic checks result in detections that are likely to be malware. However, some detections might result in a false positive. With this setting, the lab checks that popular applications and operating system files do not result in a false positive. This setting is the minimum recommendation for laptops or desktops and servers. This setting results in an average of 20–25 queries per day, per computer. High - Use this setting for deployment to systems or areas which are regularly infected. This setting results in an average of 20–25 queries per day, per computer. Very high - Dell recommends using this level only for scanning volumes and directories that do not support executing programs or operating systems. Detections found with this level are presumed malicious, but have not been fully tested to determine if they are false positives. Use this setting for on-demand scans on non-operating system volumes. This setting results in an average of 20–25 queries per day, per computer.

Exclusions	String	String - Comma-separated list of parameters Specify files, folders, and drives to exclude from scanning. Comma separated list of parameters: <ExclusionType>,<ExclusionData>,<ExcludeSubfolders (only applies to FileOrFolder type)> Possible values: <FileOrFolder|FileType|ModifiedAge|AccessedAge|CreatedAge>,<PathToFileOrFolder|FileType|Age>,<true|false> Examples: FileOrFolder,C:\Users,false FileType,xml,false FileType,mp?,false ModifiedAge,120,true AccessedAge,150,false CreatedAge,300,true
Threat First Response	Clean file	*Clean file* *Delete file* *Continue scanning* Specifies the first action for the scanner to take when a threat is detected. Clean files - Removes the threat from the detected file, if possible. Delete files - Deletes files with potential threats. Continue scanning - Continues scanning files when a threat is detected. The scanner does not move items to the quarantine.
Threat First Response Fails	Delete file	*Clean file* *Delete file* *Continue scanning* Specifies the action for the scanner to take when a threat is detected if the first action fails. Clean files - Removes the threat from the detected file, if possible. Delete files - Deletes files with potential threats. Continue scanning - Continues scanning files when a threat is detected. The scanner does not move items to the quarantine.
Exploit First Response	Clean file	*Clean file* *Delete file* *Continue scanning* Specifies the first action for the scanner to take when a potentially unwanted program is detected. Clean files - Removes the threat from the detected file, if possible. Delete files - Deletes files with potential threats. Continue scanning - Continues scanning files when a threat is detected. The scanner does not move items to the quarantine.

Exploit First Response Fails	Delete file	*Clean file* *Delete file* *Continue scanning* Specifies the action for the scanner to take when an unwanted program is detected if the first action fails. Clean files - Removes the threat from the detected file, if possible. Delete files - Deletes files with potential threats. Continue scanning - Continues scanning files when a threat is detected. The scanner does not move items to the quarantine.
Use Scan Cache	Selected	*Selected* *Not Selected* A Selected value enables the scanner to use the existing clean scan results. A Selected value reduces duplicate scanning and improves performance.
System Utilization	Below Normal	*Low Priority* *Below Normal* *Normal* Enables the operating system to specify the amount of CPU time that the scanner receives during the scan. Each task runs independently, unaware of the limits for other tasks. Low Priority - Provides improved performance for other running applications. Select this option for computers with end user activity. Below Normal - Sets the computer utilization for the scan to the default. Normal - Enables the scan to complete faster. Select this option for computers that have large volumes and low user activity.
Scan on Battery Power	Not Selected	*Selected* *Not Selected* A Selected value allows the scan when the computer is using battery power. Not Selected postpones the scan until the computer is no longer using battery power.
Schedule Repeats	Daily	*Daily* *Weekly* *Monthly* The schedule configuration defines when the task should run. Schedule types are Daily, Weekly, and Monthly. Daily: Runs the task every day at the specified Full-Scan Schedule Start Time. Weekly: Runs the task weekly on the days specified in Full-Scan Schedule Day of the Week. Monthly: Runs the task monthly on the specified Full-Scan Schedule Day of the Month.
Schedule Start Time	String	String - format is [HH:mm tt]. Example: 11:59 PM The time the task should run.
Day of the Week	Wednesday	*Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday* The day of the week the task should run.
Day of the Month	1	*1-31* The day of the month the task should run. Example: 17.
Quick Scan		

On-Demand Protection - Quick Scan	Selected	*Selected* *Not Selected* This policy is the "master policy" for all other On-Demand Protection: Quick Scan policies. If this policy is Not Selected, no On-Demand Protection: Quick Scan policies are enforced, regardless of other policy values. A Selected value means that On-Demand Protection: Quick Scan is enabled. This policy must be set to Selected to enable On-Demand Protection: Quick Scan settings. If this policy is Not Selected, no On-Demand Protection: Quick Scan policies are applied. By default, every time Quick Scan runs, it scans the following locations for threats: - the memory of all running processes - the files that the Windows Registry references - the contents of the Windows folder - the contents of the Temp folder By default, the scanner scans all file types, regardless of extension.
Boot Sectors	Selected	*Selected* *Not Selected* Examines the disk boot sector. Consider disabling this policy if a disk contains a unique or abnormal boot sector that cannot be scanned.
Unwanted Programs	Selected	*Selected* *Not Selected* Enables the scanner to detect potentially unwanted programs. The scanner uses configured information to detect potentially unwanted programs.
Decode MIME Files	Not Selected	*Selected* *Not Selected* Detects, decodes, and scans Multipurpose Internet Mail Extensions (MIME) encoded files.
Scan Archives	Selected	*Selected* *Not Selected* Examines the contents of archive (compressed) files, including .jar files. Because scanning compressed files can negatively affect computer performance, Dell recommends using this option in scans during off-work hours.
Files Migrated to Storage	Not Selected	*Selected* *Not Selected* Scans files that remote storage manages. When the scanner encounters a file with migrated content, it restores the file to the local computer before scanning.
Program Threats	Selected	*Selected* *Not Selected* Detects executable files that have code that resembles malware.
Macro Threats	Selected	*Selected* *Not Selected* Detects unknown macro viruses.
Scan Subfolders	Selected	*Selected* *Not Selected* Examines all subfolders of the specified folder.

Reputation Service Sensitivity	Medium	*Disable* *Very Low* *Low* *Medium* *High* *Very High* When enabled, samples are submitted to the lab to determine if they are malware. Sensitivity level configures the sensitivity level to use when determining if a detected sample is malware. The higher the sensitivity level, the higher the number of malware detections. However, allowing more detections might result in more false positive results. Risk levels: Very low - The detections and risk of false positives are the same as with regular content files. A detection is made available to Threat Protection when the lab publishes it instead of waiting for the next content file update. Use this setting for desktops and servers with restricted user rights and a strong security footprint. This setting results in an average of 10–15 queries per day, per computer. Low - This setting is the minimum recommendation for laptops or desktops and servers with a strong security footprint. This setting results in an average of 10–15 queries per day, per computer. Medium - Use this level when the regular risk of exposure to malware is greater than the risk of a false positive. The proprietary, heuristic checks result in detections that are likely to be malware. However, some detections might result in a false positive. With this setting, the lab checks that popular applications and operating system files do not result in a false positive. This setting is the minimum recommendation for laptops or desktops and servers. This setting results in an average of 20–25 queries per day, per computer. High - Use this setting for deployment to systems or areas which are regularly infected. This setting results in an average of 20–25 queries per day, per computer. Very high - Dell recommends using this level only for scanning volumes and directories that do not support executing programs or operating systems. Detections found with this level are presumed malicious, but have not been fully tested to determine if they are false positives. Use this setting for on-demand scans on non-operating system volumes. This setting results in an average of 20–25 queries per day, per computer.

Exclusions	String	String - Comma-separated list of parameters Specify files, folders, and drives to exclude from scanning. Comma separated list of parameters: <ExclusionType>,<ExclusionData>,<ExcludeSubfolders (only applies to FileOrFolder type)> Possible values: <FileOrFolder|FileType|ModifiedAge|AccessedAge|CreatedAge>,<PathToFileOrFolder|FileType|Age>,<true|false> Examples: FileOrFolder,C:\Users,false FileType,xml,false FileType,mp?,false ModifiedAge,120,true AccessedAge,150,false CreatedAge,300,true
Threat First Response	Clean file	*Clean file* *Delete file* *Continue scanning* Specifies the first action for the scanner to take when a threat is detected. Clean files - Removes the threat from the detected file, if possible. Delete files - Deletes files with potential threats. Continue scanning - Continues scanning files when a threat is detected. The scanner does not move items to the quarantine.
Threat First Response Fails	Delete file	*Clean file* *Delete file* *Continue scanning* Specifies the action for the scanner to take when a threat is detected if the first action fails. Clean files - Removes the threat from the detected file, if possible. Delete files - Deletes files with potential threats. Continue scanning - Continues scanning files when a threat is detected. The scanner does not move items to the quarantine.
Exploit First Response	Clean file	*Clean file* *Delete file* *Continue scanning* Specifies the first action for the scanner to take when a potential exploit is detected. Clean files - Removes the threat from the detected file, if possible. Delete files - Deletes files with potential threats. Continue scanning - Continues scanning files when a threat is detected. The scanner does not move items to the quarantine.

Exploit First Response Fails	Delete file	*Clean file* *Delete file* *Continue scanning* Specifies the action for the scanner to take when an exploit is detected if the first action fails. Clean files - Removes the threat from the detected file, if possible. Delete files - Deletes files with potential threats. Continue scanning - Continues scanning files when a threat is detected. The scanner does not move items to the quarantine.
Use Scan Cache	Selected	*Selected* *Not Selected* A Selected value enables the scanner to use the existing clean scan results. A Selected value reduces duplicate scanning and improves performance.
System Utilization	Below Normal	*Low Priority* *Below Normal* *Normal* Enables the operating system to specify the amount of CPU time that the scanner receives during the scan. Each task runs independently, unaware of the limits for other tasks. Low Priority - Provides improved performance for other running applications. Select this option for computers with user activity. Below Normal - Sets the computer utilization for the scan to the default. Normal - Enables the scan to complete faster. Select this option for computers that have large volumes and low user activity.
Scan on Battery Power	Not Selected	*Selected* *Not Selected* A Selected value allows the scan when the computer is using battery power. Not Selected postpones the scan until the computer is no longer using battery power.
Schedule Repeats	Daily	*Daily* *Weekly* *Monthly* The schedule configuration defines when the task should run. Schedule types are Daily, Weekly, and Monthly. Daily: Runs the task every day at the specified Quick-Scan Schedule Start Time. Weekly: Runs the task weekly on the days specified in Quick-Scan Schedule Day of the Week. Monthly: Runs the task monthly on the specified Quick-Scan Schedule Day of the Month.
Schedule Start Time	String	String - format is [HH:mm tt]. Example: 11:59 PM The time the task should run.
Day of the Week	Wednesday	*Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday* The day of the week the task should run.
Day of the Month	1	*1-31* The day of the month the task should run. Example: 17.
Access Protection	Selected	*Selected* *Not Selected* Access Protection prevents other computers from making a connection and creating or altering autorun (autorun.inf) files from CDs. The rule prevents spyware and adware

		distributed on CDs from being executed and will automatically block and report the issue.
Script Scan Protection	Selected	*Selected* *Not Selected* This policy enables scanning JavaScript and VBScript scripts to prevent unwanted scripts from executing. **Note:** If Script Scan Protection is disabled when Internet Explorer is launched, and then is enabled, it doesn't detect malicious scripts in that instance of Internet Explorer.
Source Sites for Update	Hyperlink	To modify the source sites your clients access for Malware Protection signature updates, click the **Source Sites for Updates** link. To modify the priority level or availability of an external source site, click either NAIHttp or NAIFtp, edit the necessary fields, and click **OK**. To designate an internal signature update server, see Designate a Threat Protection Signature Update Server. Designating a signature update server within your network allows client computers to obtain signature updates without accessing the Internet.
See basic settings		

Policy	Default Setting	Description
Web Protection This technology protects computers by leveraging a web-based content ranking system to determine if a site that a user is browsing is considered safe or not. This technology also grants the administrator the ability to define what happens when an unsafe site is navigated to (allow, block, warn).		
Web Protection	Off	*On* *Off* Toggle to ON to enable Web Protection. If toggled to OFF, no Web Protection policies are applied.
Enforcement - Action to Apply to Sites Not Verified	Allow	*Block* *Allow* *Warn* Specifies the default action to apply to sites that have not been verified. Block: Prevents users from accessing the site and displays a message that the site is blocked. Allow: Permits users to access the site. Warn: Displays a warning to notify users of potential dangers associated with the site. Users must dismiss the warning before continuing.
Enforcement - Enable File Scanning for File Downloads	Selected	*Selected* *Not Selected* A Selected value scans all files (including .zip files) before downloading. This option prevents users from accessing a downloaded file until Threat Protection marks the file as clean. Downloaded files are sent to Threat Protection for scanning. Threat Protection performs a Reputation Service lookup on the file. If a downloaded file is detected as a threat, Threat Protection takes action on the file and alerts the user. NOTE: This policy does not apply when Web Protection is installed as an optional feature with Advanced Threat

		Prevention.
Enforcement - Enable HTML iFrames Support	Selected	*Selected* *Not Selected* A Selected value blocks access to malicious (Red) and warn (Yellow) sites that display in an HTML iframe.
Enforcement - Block Sites by Default if Reputation Service Server is not Reachable	Not Selected	*Selected* *Not Selected* A Selected value blocks access to websites if Web Control cannot reach the Reputation Service server.
Enforcement - Block Phishing Pages for All Sites	Selected	*Selected* *Not Selected* A Selected value blocks all phishing pages, overriding content rating actions.
Enforcement - Specify Reputation Service Risk Level to Block	Very High	*Disable* *Very Low* *Low* *Medium* *High* *Very High* Specifies the Reputation Service risk level to block when the Threat Protection on-demand scan feature is not installed and enabled. Web Protection uses the risk level to calculate the score when retrieving the checksum reputation from the Reputation Service.
IP Exclusions for Web Protection	String	String - IP or IP Range Configures Web Protection not to rate or act on the specified private IP address range. The format is the IP address or IP address range.
Enable Secure Search	Not Selected	*Selected* *Not Selected* A Selected value enables Secure Search, automatically blocking malicious sites in search results based on safety rating.
Set Default Search Engine	Google	*Google* *Yahoo* *Bing* *Ask* Specifies the default search engine to use for supported browsers: Google, Yahoo, Bing, Ask.
Block Links to Risky Sites in Search Results	Not Selected	*Selected* *Not Selected* A Selected value prevents users from clicking links to risky sites in search results.

Rating Action for Red Sites	Block	*Block* *Allow* *Warn* Specifies the action to apply to sites that are rated Red. Block: Prevents users from accessing the site and displays a message that the site is blocked. Block is the default for Red sites. Allow: Permits users to access the site. Warn: Displays a warning to notify users of potential dangers associated with the site. Users must dismiss the warning before canceling or proceeding to the site. Green-rated sites and downloads are automatically allowed.
Rating Action for Yellow Sites	Warn	*Block* *Allow* *Warn* Specifies the action to apply to sites that are rated Yellow. Block: Prevents users from accessing the site and displays a message that the site is blocked. Allow: Permits users to access the site. Warn: Displays a warning to notify users of potential dangers associated with the site. Users must dismiss the warning before canceling or proceeding to the site. Warn is the default for Yellow sites. Green-rated sites and downloads are automatically allowed.
Rating Action for Unrated Sites	Allow	*Block* *Allow* *Warn* Specifies the action to apply to sites that are Unrated. Block: Prevents users from accessing the site and displays a message that the site is blocked. Allow: Permits users to access the site. Allow is the default for Unrated sites. Warn: Displays a warning to notify users of potential dangers associated with the site. Users must dismiss the warning before canceling or proceeding to the site. Green-rated sites and downloads are automatically allowed.
Rating Action for Red Downloads	Block	*Block* *Allow* *Warn* Specifies the action to apply to file downloads that are rated Red. Block: Prevents users from downloading the file and displays a message that the download is blocked. Block is the default for Red downloads. Allow: Permits users to proceed with the download. Warn: Displays a warning to notify users of potential dangers associated with the download file. Users must dismiss the warning before ending or proceeding with the download.
Rating Action for Yellow Downloads	Warn	*Block* *Allow* *Warn* Specifies the action to apply to file downloads that are rated Yellow. Block: Prevents users from downloading the file and displays a message that the download is blocked. Allow: Permits users to proceed with the download. Warn: Displays a warning to notify users of potential dangers associated with the download file. Users must dismiss the warning before ending or proceeding with the download. Warn is the default for Yellow sites.

Rating Action for Unrated Downloads	Allow	*Block* *Allow* *Warn* Specifies the action to apply to file downloads that are Unrated. Block: Prevents users from downloading the file and displays a message that the download is blocked. Allow: Permits users to proceed with the download. Allow is the default for Unrated downloads. Warn: Displays a warning to notify users of potential dangers associated with the download file. Users must dismiss the warning before ending or proceeding with the download.
Web Event Logging		
Log Web Control iFrame Events	Not Selected	*Selected* *Not Selected* When this policy is selected, blocked Red (malicious) and Yellow (warn) sites that display in an HTML iFrame are logged.
Log Web Categories Green Rated Sites	Not Selected	*Selected* *Not Selected* When this policy is selected, content categories are logged for all green-rated sites. Selecting this policy may affect Server performance.
Enable Web Category Blocking	Not Selected	*Selected* *Not Selected* When this policy is selected, web sites can be blocked based on category. Web Categories that can be blocked When this policy is selected, the following categories can be blocked. Select the check box next to a category to block that category. Categories indicated with * are selected and blocked by default when this policy is selected. Art/Culture/Heritage Alcohol Anonymizers Anonymizing Utilities Business Chat Public Information Potential Criminal Activities Drugs Education/Reference Entertainment Extreme Finance/Banking Gambling Games Government/Military Potential Hacking/Computer Crime* Health Humor/Comics Discrimination Instant Messaging Stock Trading Internet Radio/TV Job Search Information Security Dating/Social Networking Mobile Phone Media Downloads

		Malicious Sites* Usenet News Nudity Non-Profit/Advocacy/NGO General News Online Shopping Provocative Attire P2P/File Sharing Politics/Opinion Personal Pages Portal Sites Remote Access Religion/Ideology Resource Sharing Search Engines Sports Streaming Media Shareware/Freeware Pornography* Spyware/Adware/Keyloggers* Tobacco Travel Violence Web Ads Weapons Web Mail Web Phone Auctions/Classifieds Forum/Bulletin Boards Profanity School Cheating Information Sexual Materials Gruesome Content Visual Search Engine Technical/Business Forums Gambling Related Messaging Game/Cartoon Violence Phishing* Personal Network Storage Spam URLs Interactive Web Fashion/Beauty Software/Hardware Potential Illegal Software Content Server Internet Services Media Sharing Incidental Nudity Marketing/Merchandising Parked Domain Pharmacy Restaurants Real Estate Recreation/Hobbies Blogs/Wiki Digital Postcards Historical Revisionism Technical Information Dating/Personals Motor Vehicles Professional Networking Social Networking

		Text Translators Web Meetings For Kids History Moderated Text/Spoken Only Controversial Opinions Residential IP Addresses Browser Exploits* Consumer Protection Illegal UK Major Global Religions Malicious Downloads* Potentially Unwanted Programs
See basic settings		

Policy	Default Setting	Description
Client Firewall This technology protects computers by allowing administrators to determine which network traffic is permitted to pass between end user computers and the network.		
Client Firewall	Off	*On* *Off* Toggle to ON to enable Client Firewall. If toggled to OFF, no Client Firewall Settings or Rules are applied. Client firewall is a stateful firewall.
Settings and Rules		See Client Firewall Settings and Rules.
See basic settings		

Client Firewall Settings and Rules

In the Client Firewall policy, Settings and Rules, click **View/Edit**.

In the Settings window, you can set Client Firewall Options and Client Firewall Rules.

Return to Client Firewall Policies

Client Firewall Options

Setting	UI Control	Description
Protection Options		
Allow traffic for unsupported protocols	Check box	Allows all traffic that uses unsupported protocols. When disabled, all traffic using unsupported protocols is blocked.
Allow only outgoing traffic until firewall services have started	Check box	Allows outgoing traffic but no incoming traffic until the Firewall service starts. If this option disabled, Firewall allows all traffic before services

		are started.
Allow bridged traffic	Check box	Allows traffic with a local MAC address. The MAC address is an address in the list of VMs that Firewall supports, not the local system's MAC address. Use this option to allow traffic through a bridged environment with virtual machines.
Enable IP spoof protection	Check box	Blocks network traffic from non-local host IP addresses or from local processes that attempt to spoof their IP address.
Enable firewall intrusion alerts	Check box	Displays alerts automatically when Firewall detects a potential attack.
Setting	**UI Control**	**Description**
Tuning Options		
Enable Adaptive mode	Check box	Creates rules automatically to allow traffic. **NOTE:** Enable this option ***temporarily*** while tuning a deployment.
Log all blocked traffic to client activity log	Check box	*Enabled by default* Logs all blocked traffic to the Firewall event log (FirewallEventMonitor.log) on the Endpoint Security Client.
Log all allowed traffic to client activity log	Check box	*Disabled by default* Logs all allowed traffic to the Firewall event log (FirewallEventMonitor.log) on the Endpoint Security Client. **NOTE:** Enabling this option might negatively impact performance.
Setting	**UI Control**	**Description**
Network Reputation		
Incoming network - reputation threshold	Drop-down menu	*High Risk* *Unverified* *Do not block* *Medium Risk* Specifies the rating threshold for blocking incoming or outgoing traffic from a network connection. High Risk - This source/destination sends or hosts potentially malicious content/traffic that is considered risky. Unverified - This site appears to be a legitimate source or destination of content/traffic, but also displays properties suggesting that further inspection is necessary. Do not block - This site is a

		legitimate source or destination of content/traffic. Medium Risk - This source/destination shows behavior that is considered suspicious. Any content/traffic from the site requires special scrutiny.
Outgoing network - reputation threshold	Drop-down menu	*High Risk* *Unverified* *Do not block* *Medium Risk* Specifies the rating threshold for blocking incoming or outgoing traffic from a network connection. High Risk - This source/destination sends or hosts potentially malicious content/traffic that is considered risky. Unverified - This site appears to be a legitimate source or destination of content/traffic, but also displays properties suggesting that further inspection is necessary. Do not block - This site is a legitimate source or destination of content/traffic. Medium Risk - This source/destination shows behavior that is considered suspicious. Any content/traffic from the site requires special scrutiny.
Setting	**UI Control**	**Description**
Stateful Firewall		
Number of seconds (1-240) before TCP connections time out	Up/down number selector	Specifies the time, in seconds, that an unestablished TCP connection remains active if no more packets matching the connection are sent or received. The default number is 60; the valid range is 1–240.
Number of seconds (1-300) before UDP and ICMP echo virtual connections time out	Up/down number selector	Specifies the time, in seconds, that a UDP or ICMP Echo virtual connection remains active if no more packets matching the connection are sent or received. This option resets to its configured value every time a packet that matches the virtual connection is sent or received. The default number is 60; the valid range is 1–300.
Setting	**UI Control**	**Description**

DNS Blocking		
Domain name	Button/text input field	Defines domain names to block. When applied, this setting adds a rule near the top of the firewall rules that blocks connections to the IP addresses resolving to the domain names. Add - To add a domain name to block, click **Add**, then enter a domain name. You can use the * and ? wildcards. For example, *domain.com. Separate multiple domains with a comma (,) or a carriage return. Duplicate entries are automatically removed. Delete - To remove a domain name from the blocked list, select the domain name and click **Delete**.

Return to top

Client Firewall Rules

Client Firewall applies the rule at the top of the firewall rules list.

1. Client Firewall applies the rule at the top of the firewall rules list. If the traffic meets this rule's conditions, Client Firewall allows or blocks the traffic. It doesn't try to apply any other rules in the list.
2. If the traffic doesn't meet the first rule's conditions, Client Firewall continues to the next rule in the list until it finds a rule that the traffic matches.
3. If no rule matches, the firewall automatically blocks the traffic.

To modify Core Networking or Default Rules, expand either **Core Networking Rules** or **Default Rules**, select the rule to modify, and edit the desired settings, and click **OK**. The settings are described in the table below.

Alternatively, click one of the following buttons to perform the desired action:

Add Rule - Adds a firewall rule.

Duplicate - Creates a copy of the selected item.

Delete - Removes a selected firewall item.

Setting	UI Control	Description
Description		
Name	Text input field	Specifies the descriptive name of the item.
Status	Check box	Select **Enable rule** to make the rule active.

Actions	Radio button/Check box	*Allow* *Block* *Treat match as intrusion* *Log matching traffic* Allow - Allows traffic through the firewall if the item is matched. Block - Stops traffic from passing through the firewall if the item is matched. Treat match as intrusion - Treats traffic that matches the rule as an attack and generates an event that is sent to the Reputation Service. The *Block* action for the rule must be selected for an event to be generated. Log matching traffic - Preserves a record of matching traffic in the Firewall activity log on the Endpoint Security Client.
Direction	Drop-down menu	*In* *Out* *Either* In - Monitors incoming traffic. Out - Monitors outgoing traffic. Either - Monitors both incoming and outgoing traffic.
Notes	Text input field	Provides more information about the rule.
Setting	**UI Control**	**Description**
Networks		
Network protocol	Radio button/Check box	*Any protocol* *IP protocol* *Non-IP protocol* Any protocol - Allows both IP and non-IP protocols. IP protocol - Excludes non-IP protocols. IPv4 protocol or IPv6 protocol. If neither check box is selected, any IP protocol applies. Both IPv4 and IPv6 are selectable. Non-IP protocol - Includes non-IP protocols only.
Connection types	Check box	*Wired* *Wireless* *Virtual* Indicates if one or all connection types apply. A Virtual connection type is an adapter presented by a VPN or a virtual machine application, such as VMware, rather than a physical adapter.

Specify Networks	Button/Drop-down menu/text input field	To add a network, click **Add**, then specify the following: *Name* - Specifies the network address name (required). *Type* - Select either Local Network or Remote Network. Click **Add**, then specify the following: *Network type* - Specifies the origin or destination of traffic. Select from the network types Single IP, Subnet, Local subnet, Range, or Fully qualified domain name *IP address* - Specifies the IP address to add to the network. Wildcards are valid.
Transport		
Transport protocol	Drop-down menu	Select the transport protocol from the menu.
Executables		
Name	String	The name that you use for the executable to add or edit.
File path	String	The file path to the executable.

File description	String	*Description of the executable.*
Fingerprint	String	*The MD5 hash of the process.*
Enable digital signature check	Check box	Enables or disables the digital signature check that guarantees code has not been altered or corrupted since it was signed with a cryptographic hash. If enabled, specify: Allow any signature – Allows files signed by any process signer. Signed by – Allows only files signed by the specified process signer.

Return to top

Return to Client Firewall Policies

Policies Set by Application Control

The following policies are set when Advanced Threat Prevention > Application Control is selected.

Policy	Setting When Application Control policy is Selected
Unsafe Executable Auto Quarantine With Executable Control Enabled	Selected
Abnormal Executable Auto Quarantine With Executable Control Enabled	Selected
Memory Protection Enabled	Selected
Exploitation: Stack Pivot	Terminate
Exploitation: Stack Protect	Terminate
Exploitation: Overwrite Code	Terminate
Exploitation: Scanner Memory Search	Terminate
Exploitation: Malicious Payload	Terminate
Process Injection: Remote Allocation of Memory	Terminate

Process Injection: Remote Mapping of Memory	Terminate
Process Injection: Remote Write to Memory	Terminate
Process Injection: Remote Write PE to Memory	Terminate
Process Injection: Remote Overwrite Code	Terminate
Process Injection: Remote Unmap of Memory	Terminate
Process Injection: Remote Thread Creation	Terminate
Process Injection: Remote APC Scheduled	Terminate
Process Injection: Remote DYLD Injection (Mac OS X only)	Terminate
Escalation: LSASS Read	Terminate
Escalation: Zero Allocate	Terminate
Watch for New Files	Selected

Advanced Threat Events tab fields and filters

The Advanced Threat Events tab displays information about events for the entire enterprise based on information available in the Dell Server.

The tab displays if the Advanced Threat Prevention service is provisioned and licenses are available.

To access the Enterprise Advanced Threats tab, follow these steps:

1. In the left pane, click **Populations > Enterprise**.
2. Select the **Advanced Threat Events** tab.

Use the following filters to select content to display on the Advanced Threat Events tab:

Type - Threat Found, Threat Blocked, Threat Terminated, Memory Violation Blocked, Memory Violation Terminated, Memory Violation (Detected), Threat Removed, Threat Quarantined, Threat Waived, Threat Changed, Protection Status Changed.

Severity - Severity level of the event: Critical, Major, Minor, Caution, or Informational.

Timeframe (in days) - 1, 7, 14, 30, 60, 90

Columns - Allows you to select the following additional columns to display:

Hostname - The fully qualified name of the computer

Data - Details about the event

Created - Date and time that the event was captured

Machine Name - Name of the computer on which the threat event was detected

Path - Path to the file in which the threat was detected

Sha256 - The file's 256-character Secure Hash Algorithm can be compared with an expected result to indicate whether the file has been tampered with.

Score - The threat file's score, indicating the confidence level that the file is malware. The higher the number, the greater the confidence.

Manage Enterprise Advanced Threats - Protection

The Protection tab provides information about files and scripts that are potentially harmful.

Threats

The table lists all events found across the organization. An event may also be a threat but is not necessarily so.

View additional information about a specific threat either by clicking on the threat name link to view details displayed on a new page or by clicking anywhere in the row of the threat to view details at the bottom of the page.

To view additional threat information in the table, click the drop-down arrow on a column header to select and add columns. Columns display metadata about the file, such as Classifications, Cylance Score (confidence level), AV Industry conviction (links to VirusTotal.com for comparison with other vendors), Date first found, Data last found, SHA256, MD5, File information (author, description, version), and Signature details.

Filter Events Table Data

Click the **Threat Filters** list at the upper right side of the table to view data about events by Priority, Status: Last 24 Hours, and Status: Total.

The number of events occurring in each subcategory are shown in parentheses.

Priority: Unsafe - Select a priority to view only events that match the selected priority. High, Medium, or Low.

Status: Last 24 Hours - Select a status to view only events that have had changes to this status in the last 24 hours.

Status: Total - Select a status to only events with that status.

The predictive threat model used to protect devices receives periodic updates to improve detection rates. To understand differences in how a new threat model affects information about files in your organization, see Threat Model Updates.

Commands

Select a threat to act on it. On this page, you can do the following to the selected threat data:

Export **-** Export threat data to a CSV file.

Select the rows to export, and then click **Export.**

Open the file with Microsoft Excel or similar application, which allows you to sort and organize the data.

Global Quarantine **-** Add a file to the global quarantine list. The threat is permanently quarantined from all devices.

Add the selected file to the Global Quarantine list to prevent it from being run on any device in the organization. Adding a file to Quarantine removes it from lists of Unsafe files.

1. Select a threat.
2. Click **Global Quarantine**.
3. Enter a reason that this file should be global quarantined and click **Yes**.

Safe - Add a file to the safe list. The file is permanently treated as safe across all devices.

1. Select the file to list as safe.
2. Click **Safe**.
3. Select the category that fits the file.

4. Enter a reason why the file should be listed as safe, and click **Yes**.

   Note: Occasionally, a “good” file may be reported as unsafe (this could happen if the features of that file strongly resemble those of malicious files). Waiving or safelisting the file can be useful in these instances.

Edit Global List **-** Add or remove files from the global quarantine list.

1. Click **Edit Global List**.
2. Select the items to change.
3. Select **Safe** to add the selected items to the safelist, or select **Remove from list** to remove the selected files from the Global Quarantine list.

Manually Add File to the Global Quarantine list

1. Click **Edit Global List**.
2. Click **Add File.**
3. Enter the file's SHA256 hash number (required).
4. Enter the file's MD5 number, if available.
5. Enter the file name, if available.
6. Enter the reason the file should be quarantined.
7. Click **Submit**.

View Threat Details - Click a threat name to display details of the threat details on a new page. Click anywhere in the threat’s row to display the same threat details on the left side of this page, under the table.

File Details

Details: [*file name*]

At the bottom of the page, this section displays details about the file that triggered an event. To display this information, select the row that displays the file name in the Advanced Events table.

Click the file name next to Details: to display the same information about the event on a new page.

Overview

The overview contains summary information about the file.

Threat Indicators

Threat Indicators are observations about a file that has been analyzed.

These indicators help administrators understand the reason for a file’s classification and provide insight into its attributes and behavior. Threat Indicators are grouped into categories.

Devices

In the Devices pane, the administrator can view a list of devices that have unsafe or abnormal files and quarantine or waive them.

The device list can be filtered by file state: Unsafe, Quarantined, Waived, or Abnormal.

Waiving a file will allow that file to run on the device.

Detailed Threat Data

If the file has been uploaded for analysis, the Detailed Threat Data pane may display a comprehensive summary of the static and dynamic characteristics of the file including additional file metadata, file structure details, and dynamic behaviors such as files dropped, registry keys created or modified, and URLs with which it attempted to communicate.

Note: If no results display in the Detailed Threat Data pane, the file has not yet been uploaded for analysis. Debug logging may provide information about why the file was not uploaded.

Script Control Table

The table lists details about Active and PowerShell scripts that have been blocked or have triggered an alert and the affected devices.

Columns display the file name, interpreter (PowerShell or ActiveScript), last found, drive type (such as internal hard drive), SHA256, Number of devices on which the script is found, and Number of occurrences that were blocked or triggered alerts.

To filter column data, click the filter icon on a column header and select values to include or exclude.

Manage Enterprise Advanced Threats - Agents

After an Advanced Threat Prevention client is installed on an endpoint computer, it is recognized by the Dell Server as an agent.

Agents Table Data, Explained

- Name - The name of the agent on the endpoint computer.
- State - State of the agent, online or offline. A computer is in the offline state after three failed attempts in a 15-minute period to contact the Cylance server.
- Offline Date - If applicable, the date on which the agent went offline.
- Files Analyzed - Number of files analyzed on the endpoint computer.
- Unsafe - Number of files deemed Unsafe on the device. An unsafe file has characteristics that greatly resemble malware.
- Quarantined - Number of files Quarantined on the device.
- Waived - Number of Waived files on the device.
- Abnormal - Number of Quarantined files on the device.
- Exploit Attempts - Number of exploit attempts on the device.

Commands

To export details about an agent or remove an agent from the list:

Export - Creates and downloads a CSV file that contains device information (Name, State, Policy, etc.).

Remove - Removes selected agents from the Agent Table. This does not uninstall the agent from the device.

Manage Enterprise Advanced Threats - Certificate

The Certificate tab allows you to upload a certificate for the purpose of safelisting it.

Certificates must be in .cer or .crt format.

To upload a certificate, follow these steps:

1. Navigate to **Populations > Enterprise > Advanced Threats tab > Certificate tab**.
2. Click **Browse**.
3. Select a certificate and click **Open**.
4. Click **Upload Certificate**.
5. Click **OK** once the upload is successful.

For instructions about how to safelist a certificate, see Manage Enterprise Advanced Threats - Global List.

Manage Enterprise Advanced Threats - Cylance Score and Threat Model Updates

A Cylance score is assigned to each file that is deemed Abnormal or Unsafe. The score represents the confidence level that the file is malware. The higher the number, the greater the confidence.

Threat Model Updates

The predictive threat model used to protect devices receives periodic updates to improve detection rates.

Two columns on the Protection page in the Management Console show how a new threat model affects your organization. Display and compare the Production Status and New Status columns to see which files on devices might be impacted by a model change.

To view the Production Status and New Status columns:

1. In the left pane, click **Populations > Enterprise**.
2. Select the **Advanced Threats** tab.
3. Click the **Protection** tab.
4. Click the down-arrow on a column header in the table.
5. Hover over **Columns**.
6. Select the **Production Status** and **New Status** columns.

Production Status - Current model status (Safe, Abnormal or Unsafe) for the file.

New Status - Model status for the file in the new model.

For example, a file that was considered Safe in the current model might change to Unsafe in the new model. If your organization needs that file, you can add it to the Safe list. A file that has never been seen or score by the current model might be considered Unsafe by the new model. If your organization needs that file, you can add it to the Safe list.

Only files found on device in your organization and that have a change in its Cylance Score are displayed. Some files might have a score change but still remain within its current Status. For example, if the score for a file goes from 10 to 20, the file status may remain Abnormal and the file appears in the updated model list (if this file exists on devices in your organization).

The information for the model comparison comes from the database, not your devices. So no re-analysis is done for the model comparison. However, when a new model is available and the proper Agent is installed, a re-analysis is done on your organization and any model changes are applied.

Compare Current Model with New Model

You can now review differences between the current model and the new model.

The two scenarios you should be aware of are:

Production Status = Safe, New Status = Abnormal or Unsafe

- Your Organization considers the file as Safe
- Your Organization has Abnormal and/or Unsafe set to Auto-Quarantine

Production Status = Null (not seen or scored), New Status = Abnormal or Unsafe

- Your Organization considers the file as Safe
- Your Organization has Abnormal and/or Unsafe set to Auto-Quarantine

In the above scenarios, the recommendation is to Safelist the files to allow in your organization.

Identify Classifications

To identify classifications that could impact your organization, Dell recommends the following approach:

1. Apply a filter to the New Status column to display all Unsafe, Abnormal, and Quarantined files.
2. Apply a filter to the Production Status column to display all Safe files.
3. Apply a filter to the Classification column to only show Trusted - Local threats.
   Trusted - Local files have been analyzed by Cylance and found to be safe. Safelist these items after review. If you have a lot of files in the filtered list, you may need to prioritize using more attributes. For example, add a filter to the Detected By column to review threats found by Execution Control. These were convicted when a user attempted to execute an application and need more urgent attention than dormant files convicted by Background Threat Detection or File Watcher.

Manage Enterprise Advanced Threats - Global List

The Global Quarantine, Safe, and Unassigned tables provide a view of files in list as well as options to perform actions on these files.

Global Quarantine

Global Quarantine lists files that are permanently quarantined from all devices.

Add a file to the global quarantine list

Add the selected file to the Global Quarantine list to prevent it from being run on any device in the organization. Adding a file to Quarantine removes it from lists of Unsafe or Unassigned files.

1. Select **Global Quarantine (n)**.
2. Select a threat.
3. Click **Add File**.
4. Enter a reason that this file should be global quarantined and click **Yes**.

Manually Add File to the Global Quarantine list

1. Select **Global Quarantine (n)**.
2. Click **Add File.**
3. Enter the file's SHA256 hash number. (required)
4. Enter the file's MD5 number, if available.
5. Enter the file name, if available.

6. Enter the reason the file should be quarantined.
7. Click **Submit**.

Remove a file from the global quarantine list

Remove the selected file from the Global Quarantine list to allow it to run on any device in the organization.

1. Select **Global Quarantine (n)**.
2. Select a file.
3. Click **Remove from List**.

Safelist a file from the global quarantine list

Safelist the selected file from the Global Quarantine list to allow it to run on any device in the organization.

1. Select **Global Quarantine (n)**.
2. Select a file.
3. Click **Safe**.

Safe

Safelisted files and certificates are permanently treated as safe across all devices. Any certificate that is safelisted is a known safe certificate for the Advanced Threat Prevention tenant.

Add a file to the safe list

Safelisting a file allows that file to run on any device across the entire organization.

Note: Occasionally, a “good” file may be reported as unsafe (this could happen if the features of that file strongly resemble those of malicious files). Waiving or safelisting the file can be useful in these instances.

1. Select **Safe (n)**.
2. Click **Add File.**
3. Enter the file's SHA256 hash number. (required)
4. Enter the file's MD5 number, if available.
5. Enter the file name, if available.
6. Enter the reason the file should be safelisted.
7. Click **Submit**.

Remove a file from the safe list

1. Select **Safe (n)**.
2. Select **Files (n)**.
3. Select the file to remove from the safe list.
4. Click **Remove from List**.

Add a certificate to the safe list

Safelisting a certificate allows access to that certificate, as needed, across the entire organization.

1. Select **Safe (n)**.
2. Select **Certificates (n)**.
3. Select the certificate to list as safe.
4. Click **Add Certificate**.
5. Select the category that fits the certificate.
6. Enter a reason why the certificate should be listed as safe, and click **Submit**.

Note: You must upload a certificate for it to be available to safelist. For more information, see **Manage Enterprise Advanced Threats - Certificate.**

Remove a certificate from the safe list

1. Select **Safe (n)**.
2. Select **Certificates (n)**.
3. Select the certificate to remove from the safe list.
4. Click **Remove from List**.

Unassigned

Unassigned files can be added to the global quarantine or safe list.

Add an unassigned file to the global quarantine list

Add the selected file to the Global Quarantine list to prevent it from being run on any device in the organization. Adding a file to Quarantine removes it from lists of Unsafe or Unassigned files.

1. Select **Unassigned (n)**.
2. Select a file.
3. Click **Global Quarantine**.
4. Enter a reason that this file should be global quarantined and click **Yes**.

Manually Add File to the Global Quarantine list

1. Select **Unassigned (n)**.
2. Click **Add File.**
3. Enter the file's SHA256 hash number. (required)
4. Enter the file's MD5 number, if available.
5. Enter the file name, if available.
6. Enter the reason the file should be quarantined.
7. Click **Submit**.

Add an unassigned file to the safe list

Safelisting a file allows that file to run on any device across the entire organization.

1. Select **Unassigned (n)**.
2. Select a file.
3. Click **Safe**.

4. Select the category that fits the file.
5. Enter a reason why the file should be listed as safe, and click **Yes**.

   Note: Occasionally, a “good” file may be reported as unsafe (this could happen if the features of that file strongly resemble those of malicious files). Waiving or safelisting the file can be useful in these instances.

Manually Add File to the Safe list

1. Select **Unassigned (n)**.
2. Click **Add File.**
3. Enter the file's SHA256 hash number. (required)
4. Enter the file's MD5 number, if available.
5. Enter the file name, if available.
6. Enter the reason the file should be safelisted.
7. Click **Submit**.

Add the selected file to the Global Quarantine list to prevent it from being run on any device in the organization. Adding a file to Quarantine removes it from lists of Unsafe or Unassigned files.

1. Select **Global Quarantine (n)**.
2. Select a threat.
3. Click **Add File**
4. Enter a reason that this file should be global quarantined and click **Yes**.

Manually Add File to the Global Quarantine list

1. Select **Global Quarantine (n)**.
2. Click **Add File.**
3. Enter the file's SHA256 hash number. (required)
4. Enter the file's MD5 number, if available.
5. Enter the file name, if available.
6. Enter the reason the file should be quarantined.
7. Click **Submit**.

Manage Enterprise Advanced Threats - Options

The Options tab allows you to integrate with Security Information Event Management (SIEM) software using the Syslog feature as well as export Advanced Threat data. SIEM software allows administrators to run customized analytics on threat data within their environments. Software options include Splunk, available to Splunkbase users at https://splunkbase.splunk.com/app/3233.

Syslog events are persisted at the same time Agent events are persisted to the Cylance server. For more information about supported event types, see Syslog Event Types.

To integrate with SIEM, select **Syslog/SIEM** on the **Options** tab, and complete the form that displays. For a list of syslog server IP addresses to allow, see Syslog IP Addresses.

With SIEM integration, to export data about threats, select **Threat Data Report** on the **Options** tab. For instructions and a description of exportable data, see Threat Data Report.

Threat Data Report

Select **Threat Data Report** on the **Options** tab to enable threat data export to .csv files.

The following types of data are available for export:

Threats - Lists all threats discovered in your organization. This information includes file name and File Status (unsafe, abnormal, waived, and quarantined).

Devices - Lists all devices in your organization that have an Agent installed. This information includes device name, operating system version, agent version, and policy applied.

Events - Lists all events related to the Threat Events graph on the dashboard for the last 30 days. This information includes file hash, device name, file path, and the date the event occurred.

Indicators - Lists each threat and the associated threat characteristics.

Cleared - Lists all files that have been cleared in your organization. This information includes files that were waived, added to the safe list, or deleted from the quarantine folder on a device.

Export Data

To access the exported data:

1. Select **Generate token.**
2. Copy the URL of the desired data and paste it into a web browser address field.
3. In the URL, replace [Token] with the generated token displayed in *Token*.

To disable access to the exported data, select **Delete** or **regenerate** to invalidate the current token. After regenerating a token, provide it to persons who should have continued access to the exported data.

Advanced Threat Prevention Classifications

The Advanced Threat Prevention Classifications pane shows a heat map of threats. The color indicates the priority classification of the threat. The size of the box indicates the relative number of endpoints that have a particular threat. This classification helps administrators determine which threats and devices to address first. Click a threat to view threat and device details.

Threat classifications include the following:

Malware

- Trojan
- Downloader

Potentially Unwanted Programs (PUP)

- Adware
- Hacking Tool
- Portable Application

Enable Compatibility Mode for Memory Protection

Compatibility Mode allows applications to run on the client computer while Memory Protection or Memory Protection and Script Control policies are enabled. Compatibility Mode is enabled through a registry setting or a command on the client computer. Compatibility Mode does not apply to Mac clients.

To enable Compatibility Mode with a registry setting:

1. In the Remote Management Console, disable the Memory Protection Enabled policy. If the Script Control policy is enabled, disable it.
2. Save the policy changes, and Commit_Policies.
3. Using the Registry Editor on the client computer, go to HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop.
4. Right-click **Desktop**, click **Permissions**, then take ownership and grant yourself Full Control.
5. Right-click **Desktop**, then select **New > Binary Value**.
6. For the name, type *CompatibilityMode*.
7. Open the registry setting and change the value to *01*.
8. Click **OK**, then close Registry Editor.
9. In the Management Console, enable the Memory Protection Enabled policy. If the Script Control policy was enabled, enable it.
10. Save the policy changes, and Commit_Policies.

To add the registry setting with a command:

1. In the Management Console, disable the Memory Protection Enabled policy. If the Script Control policy is enabled, disable it.
2. Save the policy changes, and Commit_Policies.
3. Select one command line option to run on the client computer:

   (For one computer) Psexec:
   psexec -s reg add HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop /v CompatibilityMode /t REG_BINARY /d 01

   (For multiple computers) Invoke-Command cmdlet:
   $servers = "testComp1","testComp2","textComp3"
   $credential = Get-Credential -Credential {UserName}\administrator
   Invoke-Command -ComputerName $servers -Credential $credential -ScriptBlock {New-Item -Path HKCU:\Software\Cylance\Desktop -Name CompatibilityMode -Type REG_BINARY -Value 01}

4. In the Management Console, enable the Memory Protection Enabled policy. If the Script Control policy was enabled, enable it.

5. Save the policy changes, and Commit Policies.

Disconnected Mode Policy Examples

Examples for Global Allow, Quarantine List, and Safe List policies are shown below.

Global Allow policy example

```
<?xml version="1.0" encoding="utf-8"?>
<disconnected_policy>
  <policy_name>Default</policy_name>
  <policy_company>Acme</policy_company>
  <policy_company_id>uxSYabW9P2nMbGLzuqJhvT9Y</policy_company_id>
  <policy_utctimestamp>Date(-62135596800000+0000)</policy_utctimestamp>

  <filetype_actions>
    <suspicious_files file_type="executable" actions="7" />
    <threat_files file_type="executable" actions="7" />
  </filetype_actions>
  <memoryviolation_actions>
    <memory_violation violation_type="stackpivot" action="Alert" />
    <memory_violation violation_type="stackprotect" action="Block" />
    <memory_violation violation_type="stackpivot" action="Terminate" />
    <memory_violation violation_type="overwritecode" action="None" />
    <memory_violation violation_type="outofprocessallocation" action="Scuba"
/>
    <memory_violation violation_type="outofprocessmap" action="Alert" />
    <memory_violation violation_type="outofprocesswrite" action="Block" />
    <memory_violation violation_type="outofprocesswritepe"
action="Terminate" />
    <memory_violation violation_type="outofprocessoverwritecode"
action="None" />
    <memory_violation violation_type="outofprocessunmapmemory"
action="Alert" />
    <memory_violation violation_type="outofprocesscreatethread"
action="Alert" />
    <memory_violation violation_type="outofprocessapc" action="Alert" />
```

```
    <memory_violation violation_type="lsassread" action="Alert" />
    <memory_exclusion_list>
      <path>temp\files\exe1.exe</path>
      <path>stuff\folder\exe2.exe</path>
    </memory_exclusion_list>
  </memoryviolation_actions>

  <appcontrol>
<changewindow_enabled>0</changewindow_enabled>
<lockdown lockdown_type="executionfromexternaldrives" action="deny" />
<lockdown lockdown_type="pechange" action="deny" />
  </appcontrol>

  <policy>
    <option name="auto_blocking" value="0" />
    <option name="auto_uploading" value="1" />
    <option name="threat_report_limit" value="500" />
    <option name="low_confidence_threshold" value="-600" />
    <option name="full_disc_scan" value="0" />
    <option name="watch_for_new_files" value="0" />
    <option name="memory_exploit_detection" value="0" />
    <option name="trust_files_in_scan_exception_list" value="0" />
    <scan_exception_list>
      <path>C:\temp</path>
      <path>C:\stuff</path>
    </scan_exception_list>
  </policy>

  <exclusion_list>
<checksum>3fdc391ef0e200af3e4c206e785e1de0</checksum>
<error_rate>1E-05</error_rate>
<size>509</size>
<exclusionlisthash>XjxtEUkQvOFIxTZof+f6Jb149fhxFbOHUzc3S/5Hif6zqeiZrvOaM9QvG
ruM1un/uiOGeMwiNB3lLCBD9PtwbgaYUpiz8Ne88wOmKhnerXo5TJRy+4HzPWDotDXSz+d5AHP74
zbbHfH7m47KG9bFAsPa4KNhFLqSOD3g/AI7ZCWLL/IOFyWcFMTLLkeLRycDIyZpzf8QDskQVsAt8
Ub1h2UGY4BGgKwCQfYz9J/yJWuF1XGy9A7rMAHzYdqh0B5s4Y2iB2jrdlHuGSxtNPu9gTuMldfxE
```

BgcXq7XUWxuJUTbo1Fv2jsCHYpd/hg1d+3SkNbI9qykHmK9gnCH2r7IHPlK5zvR9Y1eVxTshl6Jo
xQMDD+M0VkrL3tHqlS1mJi9NI979dd8GiYnAqtkFsMg+FhOT2PkVkBSzLgkCF+rHWoeDdo+MVX79
X9XjJqT1kRwSM2p30IPi4g+NH6X/YPs6Fz7wb95jMx6ILX/L7pHGOdM0fSeSfwO/XIOyk5FhogOJ
qY86SkJs437CS7+pW+nz82lXuFqNP4pZaG2xf2iepTDo89dAMQJGWEoCnlR1z0lPI8782TLLRm5O
KytCrhUMut+P28K8LuPOTdTgSCnf2uVrcecQTz/BZOyqX5B6vy7g1P2H0HmEV1uVfhWMjABRoSK+
aI5VXd5qNRaY4zfn0w5Z6LOiIYDtvESgkLuw0bzHrsf5ADKEkwv9Ig09DxhDYzLdJlZp/DNMsnJG
tvntZ/cezXbGtzJuGSFq7lem5L00cavDQ3vRo3GlfettwN2CT9Z2MssLJhweTS8utTabMBFfIsM8
dx3sdN26lAsx9rDyR7fLn4BJ2WnMXv8FRoTZJ3oXxOQFUsCM1Rnhw7ottTaLEiPf7Rd4jdxbsErB
nK1CYfyYAePaD6ycle1h6bYMyWxUUD2ZqyVBiu3La/4MKalmI9V2IzEsYObxp9RRXkY3HcTzPHk5
e8Zp+YbPQAr88RNpC277sCRiBWYlb00OH/hx5yc61rae/pzrGjusBT53KaiG6mlLpvRYrqDQ7fW0
cpFa2eC1czQ+o8LN/gNVT7FtFhKgd8pnQW00CidxeSULfzRk6TS9rLCgXBDtRyK1fRrkkOCrHZU/
YvC2BXaWVAx60giDsKxBUYQsgXQbaGwPG279ChdwnjWlVMWCqdvOoGEBMDApjbkqqkwgHJpkCJIF
4zOTChpVfM17PfKw/uycxoqMzpdb+AOQnTX+MzRm9BkTN9T9aFh+CRleDqc/xhP59RBUUT3GAP+r
k3789EQXdUVp9tC7hmXTjjg85jWSEe6IcGE5RY7NQXdXZGJScLmyiUVq+0lZjO3xkAUZ5eq0lUJo
5KYaneGeYQFe7VzSmyzPMao6YPfpnRxOuLvMANIhKf9q0zL1IPgJfVTwU9AHoLcUE2ztor3bdrRn
Z3+e5HqZkEpHtMGruMjiP4ZLmA7tJNhj63KspEEKJfCSkXGw74+cepc6J5ThPJWNd33IZmgcwqE2
7/sXxsb5xzYFgfBUZmr12KnU7JMbg95bZTatxN8PtIQS2NTdnyXK/f7j7i74FQZXNksONgfyEelF
DOTlqlI7SLKw1uffUEk2QGv54bUQANLhbAvLbLR1b6v352rw3ANgECdQbqXcvKE/jYKUzHSW3qqI
PcPnrguYVoJuydKNiJVmoaqPLJ3LC6m7+PdGBuqEdVo+MK/PMJdTVb47zW1RSYX0t9SJ/4xWEByb
UMsHXRZTux6nlca5qCxHDiHb50I677Bi+Y0YLddza7iA7z4mPTRmqEX6jEo5ZorZ4kcTIbNHj77p
4kzouYDg3s+o+9KvoxcI0iw8MAOtKrRVZTN24jjSUAETJ66rb3JdzcfJJeb7w4QVOUckL2kfyaS4
ASp80fzpOxJl3hSLw2bnR2n0WukMhj3kWvY+GeXDBfGzHfDGeLV0pF/+hQTPR/XWuOSsnH1wUeJE
XS3al6lyhcRCS7XbVPt+85NYGuk2ntf6zmST/v6a3E2exxerUDAmHfCK/0VQKrqlYec1hkH1SbvC
Q==</exclusionlisthash>

<exclusionlisthash_secondary>rT7UrQItY0RfpDEVEDwSXdiGq3fUgEJ9OpQMEUEacRRy1OF
AS2W51m9f3hbzrOA7lvoiKZLy9/h0koV2d5vyIj+xC275ucwOvqhKpKPQH8mfcD3vT498DuteV0i
1Tmzq/WFLlhdqK75CF8ys17UVZZabbExD2s9W49gUft5W9UozOW5K1mC9V5E79YCf83s0wra6qrZ
qENI98WNpD9UbyN1UQN72g5mQligT8ViuoEMagB6JQaTI8CgCLe6NK8DFvuykGOYVtLfKCtmCqt0
eg1Im0oFxLiVrouovcCdNpfzWOXflQSEVEbVeqfPxEuTrHRWZBzFxOYLrT86tSsH8ll+XC3uFjN7
uI/HB8daE3saFPmIAZUC9sq3rMU8Roy9+iRw3lebL0P51RTSHxC9Mz8xr85gt3m4MyqSO8mNNBxI
zwxeUCishz8A17VB5ai/R5Hy17zMTwIXU2x5Pcnpd2UqyeLQbXWpnkeRpl7f0rdwBM0FDCpZqExn
FYQswvOb8kPnruC0/iIgx/zNSFeuFlT8dSbCZNvgh07Ohh4sl0v9U9Ir7nBe9ZreDgdZMdZ1wCTq
XBk/yxJB74+95uRYasNznVAG2yD1IIwtWNvygHrmw5sZgk097K2quTOHjDp0thnhaSGdOK5pF2TF
Em8zegjewP65pR5Jdys1lvKquzbx3NZ3LtR0XyVIMBzcF9NDLP8v4UkwaKg9EL73o2yPjqgDVwt9
AhXlh4VdSEv5M+JRfo+EguQB9I/DleTbWUGAEMMn1cADZj9yY0fB/SEsDVAWiLbiP/PYcUXz6g4C
v2uF9jk2Tn7KEbvuFWfIlnq2+z/qUNUH0Uj44jgqswv6G/q5VfbW5dM0MtTGmZd5jE8PNy3R/uyg
m4ZoTvnOUu93FIC8dpmVjlsyii9XhM8XN/YX9om5wXAJ9CuTgRWbuUK4lvW9ROiEokQRFu76Y8OT
Evx6kpCEFgAVZlhbfe0fmGo+CD1wI+dg0tze2BN7jk/ItXgiPKp/+/fLoH3HR8mZSWX8bW8uRpBg
qo3xq57tpP9JxcyPQetG9fungtlBjzAd53Frro8XYXbzOd71honuEsFYv4T03ojU8w7a9EBbJ7Sv
RfDDi27mT/YmZNr3Y39FRlT7qQ44Ng5cjgp9etwVIego1xpfBXECF2PxOuA/S7u06QakK+Ngkl+b
Fw5MBbG/NLHALbkV+jbL6NKmUMWHYO4ruPzSoUYE84f9V0WFBZpWMxnx/j/ZZZMwv8+p8kF3dAR9
SjK38coPVCnLCJ8uDJPoLDXS79u+pfQbsqgdPL+dwDeQAlIhHzjpNlpM5UeHYGUiwHFbOr8GTdq2
GSEacfW510uv1dNeIk1wo2a2zlcBMH0V57f3/aVi0ZDtDKL5N1TO81xSPa6/hck4RGjIRInr632O
mMh/dtx+40q7c8269KQSnXvpaVS8kyf2GvLMHCWurEg+NyCB0N5+UonnC+0i9KialfIByLBuPCNQ
ppds0mkjhbCmJqPtCxgLaJVYop2qddzsry9PFW97tDEJcUilrQc7a5NTFWExc4a8LLpT+dtXNxEv
ZAg2VSsffawcZ894um6Gw55IBRmLHeyso0Y3zBWOGq5G3KA31fFyk9OAfxgdwIkHA6jB9nSRzi/e
a7HSRUHNRfp26Bc0/c4K/dDDA23NdTOT14AIuU+3d822EH9l/McuVa1FAK1gzPwcOrL8lT3x9vrR
JwUOCw0EamqgAzQNrE3tIbPsVuOhevtZhjm+NDzRZcxuk4Tu38Tojo5H2xCucaEWdYxz0CKzCch/
vH8FIpr0J9s1Jbl0Ac1m+frnuUZImePkSXdmvkX4SpD4hoCy0L1F4eVGMniFfjfCIhQyBwphCoqG
Ko1wP7WOQA/9fDZc7z0vka2u6Uz3Sy/ekJHZ0yI7OzP4nAzTq7bnBQR2KCXgLaUP2mq0VjyFS9zP
msxloHU8fjs2kDP4jH2e+qXSAJwQ0112Y+9mEvdktSkAJq24c5HSO4F80p1Ae8YhpuAECKXqCC+P
0YiksNToTGA==</exclusionlisthash_secondary>

  </exclusion_list>

</disconnected_policy>

Quarantine List and Safe List policy examples

Quarantine List

The Global Quarantine List contains hashes of files to be quarantined as shown in this example:

```
0A5F695900F1FC75070BB8B7C7A55B5BCFAAD6FE

525E7A55B5BCB6B16F25B5DD6CE11DFC6DD0B4E6
```

Safe List

The Global Safe List contains hashes of files to be quarantined as shown in this example:

```
0A5F695900F1FC75070BB8B7C7A55B5BCFAAD6FE

525E7A55B5BCB6B16F25B5DD6CE11DFC6DD0B4E6
```

Threat Protection Policy Overview

Threat Protection policies are divided into the following categories:

- Threat Protection
- Client Firewall
- Web Protection

When you set the *Threat Protection* policy to Selected, you can then set policies for these client options:

- Actions to take when malicious activity is identified (Block, Report, Block and Report)

  Policies allow you to set the action to take when users attempt to modify or delete Threat Protection system files, registry keys, and processes. The default setting for these policies is Block and Report: *Action on Malicious Activity for Files and Folders*, *Action on Malicious Activity for Registry*, and *Action on Malicious Activity for Processes*.

- Exclusion of specified processes from Threat Protection scans
- Logging locations and debug/verbose logging of certain activities

  Activity logging is enabled by default. Debug logging is disabled by default.

- Client update scheduling

  Client updates ensure that client computers are always protected from the latest threats through content files that include definitions of threats such as viruses and spyware, that are used to detect threats. The *Client Update Schedule* policy is selected (Enabled) by default. The *Client Update Schedule Repeats* policy, which determines the frequency of client updates, is set to Daily by default.

The following policies represent the different types of scans included in Threat Protection:

On-Access Protection – When a user accesses files, folders, and programs, the on-access scanner intercepts the operation and scans the item. Default: Selected (Enabled).

On-Demand Protection - Full Scan – Based on a schedule set in policy, the on-demand scanner runs a thorough check of all areas of the computer. Default: Selected (Enabled).

By default, every time Full Scan runs, it scans the following for threats:

- Computer memory for installed rootkits, hidden processes, and other behavior that suggests malware is attempting to hide itself. This scan occurs before all other scans.
- Memory of all running processes.

- All drives on the computer and their subfolders.

By default, the scanner scans all file types, regardless of extension.

On-Demand Protection - Quick Scan – Based on a schedule set in policy, the on-demand scanner runs a quick check of areas of the computer that are most susceptible to threats. Default: Selected (Enabled).

By default, every time Quick Scan runs, it scans the following for threats:

- Memory of all running processes.
- Files that the Windows Registry references.
- Contents of the Windows folder.
- Contents of the Temp folder.

By default, the scanner scans all file types, regardless of extension.

Access Protection – Prevents other computers from making a connection and creating or altering autorun (autorun.inf) files from CDs. The rule prevents spyware and adware distributed on CDs from being executed and automatically blocks and reports such issues. Default: Selected (Enabled).

Exploit Protection – Monitors for application vulnerabilities and keeps buffer overflow exploits from executing arbitrary code on the computer. Default: Selected (Enabled).

Script Scan Protection – Enables scanning JavaScript and VBScript scripts to prevent unwanted scripts from executing. Default: Selected (Enabled).

Actions taken if a threat, unwanted program, or exploit is detected are controlled by policy and include the following:

Full-Scan Threat First Response - Specifies the first action for the scanner to take when a threat is detected. Default: Clean file.

Full-Scan Threat First Response Fails - Specifies the action for the scanner to take when a threat is detected if the first action fails. Default: Delete file.

Full-Scan Unwanted Program First Response - Specifies the first action for the scanner to take when a potentially unwanted program is detected. Default: Clean file.

Full-Scan Unwanted Program First Response Fails - Specifies the action for the scanner to take when an unwanted program is detected if the first action fails. Default: Delete file.

Quick-Scan Threat First Response - Specifies the first action for the scanner to take when a threat is detected. Default: Clean file.

Quick-Scan Threat First Response Fails - Specifies the action for the scanner to take when a threat is detected if the first action fails. Default: Delete file.

Quick-Scan Exploit First Response - Specifies the first action for the scanner to take when a potential exploit is detected. Default: Clean file.

Quick-Scan Exploit First Response Fails - Specifies the action for the scanner to take when an exploit is detected if the first action fails. Default: Delete file.

When the *Full-Scan Reputation Service Sensitivity* or *Quick-Scan Reputation Service Sensitivity* policies are enabled, samples are submitted to the Reputation Service lab to determine if they are malware. The sensitivity level is used when determining if a detected sample is malware. The higher the sensitivity

level, the higher the number of malware detections. However, allowing more detections might result in more false positive results.

The following values can be set:

Disable - Samples are not submitted to the Reputation Service lab.

Very Low - A detection is made available to Threat Protection when the Reputation Service lab publishes it instead of waiting for the next file update. Average of 10-15 queries per day, per computer.

Low - This setting is the minimum recommendation for laptops or desktops and servers with a strong security footprint. This setting results in an average of 10-15 queries per day, per computer.

Medium - Use this level when the regular risk of exposure to malware is greater than the risk of a false positive. This setting is the minimum recommendation for laptops or desktops and servers. Average of 20-25 queries per day, per computer.

High - Use this setting for deployment to systems or areas which are regularly infected. This setting results in an average of 20-25 queries per day, per computer.

Very High - Dell recommends using this level only for scanning volumes and directories that do not support executing programs or operating systems. Detections found with this level are presumed malicious, but have not been fully tested to determine if they are false positives. Use this setting for on-demand scans on non-operating system volumes. This setting results in an average of 20-25 queries per day, per computer.

For more detail about Threat Protection policies, see Windows Threat Protection.

Client Firewall Policies

The Client Firewall is a stateful firewall that checks all incoming and outgoing traffic against its list of rules. If the traffic matches all criteria in a rule, the Client Firewall acts according to the rule, blocking or allowing traffic through the firewall.

Configurable options and rules define how the Client Firewall works. When the master policy, *Client Firewall*, is set to **On**, you can select **View/Edit** in the *Settings and Rules* policy to view or configure an extensive set of Client Firewall options and rules.

Options include which subsets of traffic to block or allow and logging settings, as well as timeout parameters for TCP, UDP, and ICMP connections.

Client firewall rules define specific handling of network traffic. Each rule provides a set of conditions that traffic must meet and an action to allow or block that traffic. When Client Firewall finds traffic that matches a rule's conditions, it performs the associated action.

Client Firewall uses precedence to apply rules and applies the rule at the top of the firewall rules list.

1. If the traffic meets the conditions of the rule at the top of the list, Client Firewall allows or blocks the traffic. It does not try to apply any other rules in the list.
2. If the traffic does not meet the first rule's conditions, Client Firewall continues to the next rule in the list until it finds a rule that the traffic matches.
3. If no rule matches, the firewall automatically blocks the traffic.

For a list of Client Firewall rules and their descriptions, see Client Firewall Settings and Rules.

Web Protection Policies

Web Protection monitors web browsing and downloads to identify threats and enforce action set by policy when a threat is detected, based on ratings for websites. When you set the master policy, *Web Protection*, to **On**, you can set other policies for Web Protection.

The Reputation Service analyzes each website and assigns a color-coded safety rating based on test results. The color indicates the level of safety for the site:

Red – Malicious

Yellow – Potentially malicious

Green - Safe

Through the following policies, you can assign actions to implement when a user accesses a website or attempts a download, based on website ratings:

Rating Action for Red Sites - Specifies the action to apply to sites that are rated Red. Default: Block.

Rating Action for Yellow Sites - Specifies the action to apply to sites that are rated Yellow. Default: Warn.

Rating Action for Unrated Sites - Specifies the action to apply to sites that are Unrated. Default: Allow.

Rating Action for Red Downloads - Specifies the action to apply to file downloads that are rated Red. Default: Block.

Rating Action for Yellow Downloads - Specifies the action to apply to file downloads that are rated Yellow. Default: Warn.

Rating Action for Unrated Downloads - Specifies the action to apply to file downloads that are Unrated. Default: Allow.

Configurable actions for website access or download attempts include the following:

Block – Prevents users from accessing the site or downloading a file from the site. A message is displayed.

Allow – Permits users to access the site or proceed with the download.

Warn – Displays a warning to notify users of potential dangers associated with the site or download file. Users must dismiss the warning before ending the web session or proceeding with the download.

To exclude a private IP address or range of addresses from Web Protection content rating actions, specify the IP address or IP address range in the *IP Exclusions for Web Protection* policy.

To block all phishing pages, without regard to policy values that control content rating actions, select the *Enforcement - Block Phishing Pages for All Sites* policy.

Designate a Threat Protection Signature Update Server

Both an HTTP and FTP signature update server are pre-configured with your Dell Server installation. You can also, optionally, designate an internal signature update server or servers within your network.

Designating a signature update server within your network allows client computers to obtain signature updates without accessing the Internet. Rather than individual clients contacting an external update server, they contact your internal update server, which maintains current signatures through contact with the external signature update server.

To designate a signature update server, follow these steps:

1. As an administrator on the server to be the internal update server, run the appropriate command:

   ```
   VSSETUP_86.EXE /SetRelayServerEnable=1
   ```

or
VSSETUP_64.EXE /SetRelayServerEnable=1

2. Restart the internal update server.
3. In the Management Console, navigate to **Populations > Enterprise** and select **Malware Protection** on the Security Policies tab.
4. In Malware Protection advanced settings, click **Source Sites for Updates**.
5. Click **Add**.
6. Enter a Name for the internal update server.
7. To enable connections to the internal update server, select **Enabled**. To enable later, clear the *Enabled* check box.
8. In *Order*, set the sequence in which clients will contact the internal update server in relation to other update servers. Dell recommends that you set the Order for internal update servers to precede the Order for external update servers.
9. Select the type of repository or path to the update server: HTTP repository, FTP repository, UNC path, or Local path.
10. Enter the URL or path to the internal update server.
11. Complete the remaining fields in the form, and click **OK**.
12. Repeat these steps to designate additional internal update servers.

To revert an internal update server to non-update server status, enter the appropriate command:

VSSETUP_86.EXE /SetRelayServerEnable=0
or
VSSETUP_64.EXE /SetRelayServerEnable=0

Removable Media Encryption

Removable Media Encryption

A note about Removable Media policies: Mac Media Encryption policies are device-based policies. This is different behavior than Windows Media Encryption, which are user-based.

Policy descriptions also display in tooltips in the Management Console. In this table, master policies are in bold font.

Policy	Default Setting	Description
Windows Media Encryption This technology works on Windows computers using Dell Encryption External Media to encrypt data on removable devices, which can be accessed using a user-defined password. These policies allow configuration of the Encryption External Media password requirements and the removable media allowed.		
Windows Media Encryption	Off	This policy must be selected to use all other removable media policies. Not Selected means that no encryption of removable media takes place, regardless of other policy values.
EMS Scan External Media	Not Selected	Selected allows removable media to be

		scanned every time it is inserted. When this policy is Not Selected and the Windows Media Encryption policy is Selected, only new and changed files are encrypted. More... A scan occurs at every insertion so that any files added to the removable media without authenticating can be caught. Files can be added to the media if authentication is declined, but encrypted data cannot be accessed. The files added are not encrypted in this case, so the next time the media is authenticated (to work with encrypted data), any files that may have been added are scanned and encrypted.
EMS Access to unShielded Media	Read Only	Block, Read Only, Full Access This policy interacts with the Port Control System - Class: Storage > Subclass Storage: External Drive Control policy. If you intend to set this policy to Full Access, ensure that Subclass Storage: External Drive Control is not set to Read Only or Blocked. More... When this policy is set to Block Access, you have no access to media unless it is encrypted. Choosing either Read-Only or Full Access allows you to decide what media to encrypt. If you choose not to encrypt removable media and this policy is set to Full Access, you have full read/write access to media. If you choose not to encrypt media and this policy is set to Read-Only, you can read or delete existing files on the unencrypted removable storage, but files cannot be edited on, or added to, the media .
EMS Block Access to UnShieldable Media	Selected	Block access to any removable media that is less than 55 MB and thus has insufficient storage capacity to host Encryption External Media (such as a 1.44MB floppy disk). More... All access is blocked if Windows Media Encryption and this policy are both Selected. If Windows Media Encryption is Selected, but this policy is Not Selected, data can be read from the unencryptable media, but write access to the media is blocked. If Windows Media Encryption is Off, then this policy has no effect and access to unencryptable media is not impacted.
See advanced settings		

Policy	Default Setting	Description
Mac Media Encryption This technology works on Mac computers using Dell Encryption External Media to encrypt data on removable devices, which can be accessed using a user-defined password. These policies allow configuration of the Encryption External Media password requirements and the removable media allowed.		
Mac Media Encryption	Off	Toggle On to enable Mac Removable Media Encryption policies. If this policy is toggled to OFF, no Mac Removable Media Encryption takes place, regardless of other policies. HFS Plus is supported and must be enabled. For instructions to enable HFS Plus, see the Encryption Enterprise for Mac Administrator Guide. Media containing Time Machine backups are not supported. However, media recognized by computers as Time Machine backup destinations are automatically whitelisted, to allow backups to continue. All other removable media with Time Machine backups are handled based on *EMS Access to unShielded Media* and *EMS Block Access to UnShieldable Media* policies.
EMS Scan External Media	Not Selected	Selected allows removable media to be scanned every time it is inserted. When this policy is Not Selected and the Windows Media Encryption policy is Selected, only new and changed files are encrypted. More... A scan occurs at every insertion so that any files added to the removable media without authenticating can be caught. Files can be added to the media if authentication is declined, but encrypted data cannot be accessed. The files added are not encrypted in this case, so the next time the media is authenticated (to work with encrypted data), any files that may have been added are scanned and encrypted.
EMS Access to unShielded Media	Read Only	*Block, Read Only, Full Access* When this policy is set to Block Access, you have no access to removable media unless it is encrypted. Choosing either Read-Only or Full Access allows you to decide what media to encrypt. If you choose not to encrypt removable storage and this policy is set to Full Access, you have full read/write access to removable media. If you choose not to encrypt

		removable media and this policy is set to Read-Only, you cannot read or delete existing files on the unencrypted media, but no files can be edited on, or added to, the media unless it is encrypted.
EMS Block Access to UnShieldable Media	Selected	Block access to any removable media that is less than 55 MB and thus has insufficient storage capacity to host Encryption External Media (such as a 1.44MB floppy disk). All access is blocked if EMS Encrypt External Media and this policy are both selected. If EMS Encrypt External Media is True, but this policy is False, data can be read from the unencryptable media, but write access to the media is blocked. If EMS Encrypt External Media is False, then this policy has no effect and access to unencryptable media is not impacted.
See advanced settings		
Policy	**Default Setting**	**Description**
Media Encryption Settings This technology allows definition of what media encryption events to retain in logs.		
Event Retention		"security", "fail", "30" "security", "success", "30" "application", "error", "30" "application", "warn", "15" "application", "info", "5" "application", "debug", "5" Defines the amount of time (in days) that Encryption External Media, and PCS event types are maintained in the event log. Each event type is defined by category and level. You may set different retention times for each event level in each category. The Security category represents events related to user authentication, authorization, or encryption. This includes events for Dell-encrypting devices, updating security policies, or failed authentication attempts. Security events are further differentiated by a fail or success indicating the outcome of the event. The Application category (application type event, rather than a security type event) represents events related to general application actions. These events are further differentiated by a set of severity levels - error, warn, info, and debug. You should use longer retention times for more

		severe levels.

Removable Media Policies that Require Logoff

- Windows Media Encryption
- EMS Scan External Media
- EMS Encryption Algorithm
- EMS Exclude CD/DVD Encryption
- EMS Data Encryption Key

Advanced Removable Media Encryption

A note about Removable Media Encryption policies: Mac Media Encryption policies are device-based policies. This is different behavior than Windows Media Encryption, which are user-based.

Policy descriptions also display in tooltips in the Management Console. In this table, master policies are in bold font.

Policy	Default Setting	Description
Windows Media Encryption This technology works on Windows computers using Dell Encryption External Media to encrypt data on removable devices, which can be accessed using a user-defined password. These policies allow configuration of the Encryption External Media password requirements and the removable media allowed.		
Windows Media Encryption	Off	This policy must be selected to use all other removable media policies. Not Selected means that no encryption of removable media takes place, regardless of other policy values.
EMS Exclude CD/DVD Encryption	Not Selected	**False encrypts CD/DVD devices.**
EMS Allow Read-access to unShielded Media (5.4.x Only)	Selected	This policy applies to 5.4.x Windows Encryption clients only. More... If a user chooses not to encrypt media and this policy is set to True, they are able to read or delete existing files on the media that are not encrypted, but the client does not allow any files to be edited on or added to the media unless it is Dell-encrypted.
EMS Encryption Algorithm	AES256	AES 256, AES 128, 3DES Encryption algorithm used to encrypt removable media. Encryption algorithms in order of speed, fastest first, are AES 128, AES 256, 3DES.
EMS Data Encryption Key	User Roaming	Common, User, User Roaming Choose a key to be used by the Encryption client to encrypt all data encrypted by the Encryption External Media. More... You cannot save a policy where this policy has the same value as either User Data Encryption Key policy or Application Data Encryption Key policy, the error message *Policy Constraint Violation: The value for EMS Data Encryption Key conflicts with User Data Encryption Key and/or Application Data Encryption Key* will display.
EMS Automatic Authentication	Disabled	*Disabled, Local, Roaming* Local automatic authentication allows the encrypted media to be automatically authenticated when inserted in the originally encrypting computer when the owner of that media is logged in. When automatic

		authentication is Disabled, users must always manually authenticate to access encrypted media. Not Selecting Roaming automatic authentication helps to prevent users from forgetting their password when they take the media home or share it with a colleague. Not selecting Roaming automatic authentication also promotes a sense of awareness from a security perspective for users that the data being written to that media is protected.
EMS Access Encrypted Data on unShielded Device	Selected	Selected allows the user to access encrypted data on removable media whether the endpoint is Dell-encrypted or not. More... When this policy is False, the user can work with encrypted data when logged on to any Dell-encrypted endpoint . The user cannot work with encrypted data using any device that is not Dell-encrypted.
EMS Device Whitelist		*String - Maximum of 150 devices with a maximum of 500 characters per PNPDeviceID. Maximum of 2048 total characters allowed. "Space" and "Enter" characters count in the total characters used.* This policy allows the specification of removable media devices to exclude from encryption [using the device's Plug and Play device identifier (PNPDeviceID)], thereby allowing users full access to the specified removable media devices. More... This policy is available on an Enterprise, Domain, Group, and User level. Local settings override inherited settings. If a user is in more than one group, all EMS Device Whitelist entries, across all Groups, apply. This policy is particularly useful when using removable media devices which provide hardware encryption. However, this policy should be used with caution. This policy does not check whether external media devices on this list provide hardware encryption. Whitelisting removable storage devices that do not have hardware encryption do not have enforced security and are not protected. *For example, the Kingston® DataTraveler® Vault Privacy model enforces that encryption is enabled to use the device. However, the Kingston DataTraveler Vault model has an unsecured partition and a secured partition. Because it is the same physical removable media device with only one PNPDeviceID, the two partitions cannot be distinguished, meaning that whitelisting this particular device would allow unencrypted data to leave the endpoint.* *Additionally, if a removable media device is encrypted and is subsequently added to the EMS Device Whitelist policy, it remains encrypted and requires a reformat of the device to remove encryption.* The following is an example of a PNPDeviceID, which contains the manufacturer identifier, product identifier, revision, and hardware serial number: `USBSTOR\DISK&VEN_KINGSTON &PROD_DTVAULT_PRIVACY& REV_104\07005B831A0004B4&0` To whitelist a removable media device, provide a string value that matches portions of the device's PNPDeviceID. Multiple device PNPDeviceIDs are allowed. For example, to whitelist all Kingston DataTraveler Vault Privacy models, input the string: `PROD_DTVAULT_PRIVACY` To whitelist both models of Kingston DataTraveler, the Vault and Vault Privacy models, input the string: `PROD_DTVAULT_PRIVACY; PROD_DT_VAULT` Space characters are considered part of the substring to match to a PNPDeviceID. Using the previous PNPDeviceID as an example, a space before and after the semicolon would cause neither of the substrings to be matched, because the space character is not part of the PNPDeviceID. Instructions... *To find the PNPDeviceID for removable media:*

		1. Insert the removable media device into an encrypted computer. 2. Open the *EMSService.log* in C:\Programdata\Dell\Dell Data Protection\Encryption\EMS. 3. Find PNPDeviceID= For example: 14.03.18 18:50:06.834 [I] [Volume "F:\"] PnPDeviceID = USBSTOR\DISK&VEN_SEAGATE&PROD_USB&REV_0409\2HC015KJ&0 VEN=Vendor; Green highlighted text is for the vendor to be excluded PROD=Product/Model Name; Adding text highlighted blue also excludes all of Seagate's USB drives REV=Firmware Revision; Adding text highlighted gray also excludes the specific model being used Serial number (in this example); Adding text highlighted yellow excludes just this device OR *To find the PNPDeviceID for removable media on Windows 7 or later:* 1. Insert the removable media device. 2. Open the Control Panel and go to Administrative Tools > Computer Management. 3. Select the Hardware tab, select the drive, and click Properties. 4. A new windows displays. Select the Device Instance Path in the Property menu. The PNPDeviceID is displayed in *Value* . Available Delimeters: Tabs Commas Semi colons Hex character 0x1E (Record separator character)
EMS Alpha Characters Required in Password	Selected	Selected requires one or more letters in the password.
EMS Mixed Case Required in Password	Selected	Selected requires at least one uppercase and one lowercase letter in the password.
EMS Number of Characters Required in Password	8	1-40 characters Minimum number of characters required in the password.
EMS Numeric Characters Required in Password	Selected	Selected requires one or more numeric characters in the password.
EMS Password Attempts Allowed	3	1-10 Number of times the user can attempt to enter the correct password.
EMS Special Characters Required in Password	Not Selected	Selected requires one or more special characters in the password.
EMS Access and Device Code Length	16	8, 16, 32 Number of characters access and device codes have. 32 characters is the most secure, while 8 is the easiest to enter.
EMS Access Code Attempts Allowed	3	1-10 Number of times the user can attempt to enter the access code.
EMS Access Code Failure Action	Apply Cooldown	*Apply Cooldown, Wipe Encryption Keys* Action to take following unsuccessful EMS Access Code Attempts Allowed: • Apply Cooldown to allow another round of attempts following the specified cooldown period (EMS Cooldown Time Delay and EMS Cooldown Time Increment policies)

		• Wipe Encryption Keys to delete the encryption keys on the removable storage, making the encrypted data inaccessible until the owner takes the media to an encrypted computer for which he has a login.
EMS Access Code Required Message	String Authentication Failed. Please contact your system administrator.	String - 5-512 characters - Authentication Failed: Please contact your system administrator. Message that displays when a user needs to contact you for an access code (after authentication failure). More... Message policies must have non-blank values. "Space" and "Enter" characters used to add lines between rows count as characters used. Messages over the 512 character limit are truncated on the client. Optionally customize the second sentence of the message to include specific instructions about how to contact a help desk or security administrator for authentication failures.
EMS Cooldown Time Delay	30	*0-5000 seconds* Number of seconds the user must wait before attempting to enter the access code after failing the specified number of times.
EMS Cooldown Time Increment	20	*0-5000 seconds* Incremental time to add to the cooldown time each time the user fails to enter the correct access code in the specified number of attempts.
EMS Access Code Failed Message	String You are not authorized to use this media. Please contact your system administrator.	*String - 5-512 characters - You are not authorized to use this media. Please contact your system administrator.* Message that displays following unsuccessful Access Code Attempts Allowed. More... Message policies must have non-blank values. "Space" and "Enter" characters used to add lines between rows count as characters used. Messages over the 512 character limit are truncated on the client. Optionally customize the message to include specific instructions about how to contact the help desk or security administrator.
EMS Encryption Rules		Encryption rules to be used to encrypt/not encrypt certain drives, directories, and folders. A total of 2048 characters are allowed. "Space" and "Enter" characters used to add lines between rows count as characters used. Any rules exceeding the 2048 limit are ignored. See Encryption Rules for information. More... Storage devices which incorporate multi-interface connections, such as Firewire, USB, eSATA, etc. may require the use of both EMS and encryption rules to encrypt the endpoint. This is necessary due to differences in how the Windows operating system handles storage devices based on interface type. To ensure encrypting an iPod via EMS does not make the device unusable, use the following rules: -R#:\Calendars -R#:\Contacts -R#:\iPod_Control -R#:\Notes -R#:\Photos You can also force encryption of specific file types in the directories above. Adding the following rules will ensure that ppt, pptx, doc, docx, xls, and xlsx files are encrypted in the directories excluded from encryption via the previous rules: ^R#:\Calendars ;ppt.doc .xls.pptx .docx.xlsx ^R#:\Contacts ;ppt .doc.xls .pptx.docx

		.xlsx ^R#: \iPod_Control ;ppt.doc .xls.pptx .docx.xlsx ^R#:\Notes ;ppt.doc .xls.pptx .docx.xlsx ^R#:\Photos ;ppt.doc .xls.pptx .docx.xlsx Replacing these five rules with the following rule will force encryption of ppt, pptx, doc, docx, xls, and xlsx files in any directory on the iPod, including Calendars, Contacts, iPod_Control, Notes, and Photos: ^R#:\;ppt.doc.xls .pptx.docx.xlsx These rules disable or enable encryption for these folders and file types for all removable devices - not just an iPod. Use care when defining rules to exclude an iPod from encryption. These rules have been tested against the following iPods: iPod Video 30gb fifth generation iPod Nano 2gb second generation iPod Mini 4gb second generation Dell does not recommend the use of the iPod Shuffle, as unexpected results may occur. As iPods change, this information could also change, so caution is advised when allowing the use of iPods on EMS-enabled computers. Because folder names on iPods are dependent on the model of the iPod, Dell recommends creating an exclusion encryption policy which covers all folder names, across all iPod models.
See basic settings		

Mac Media Encryption

This technology works on Mac computers using Dell Encryption External Media to encrypt data on removable devices, which can be accessed using a user-defined password. These policies allow configuration of the Encryption External Media password requirements and the removable media allowed.

Mac Media Encryption	Off	Toggle On to enable Mac Removable Media Encryption policies. If this policy is toggled to OFF, no Mac Removable Media Encryption takes place, regardless of other policies.
EMS Encryption Algorithm	AES256	AES 256, AES 128, 3DES Encryption algorithm used to encrypt removable storage. Encryption algorithms in order of speed, fastest first, are AES 128, AES 256, 3DES.
EMS Data Encryption Key	User Roaming	Common, User, User Roaming ***Although Common is available, it is not implemented in this release.*** Choose a key to be used by the Encryption client to encrypt all data encrypted by the Encryption External Media.
EMS Alpha Characters Required in Password	Selected	Selected requires one or more letters in the password.
EMS Mixed Case Required in Password	Selected	Selected requires at least one uppercase and one lowercase letter in the password.
EMS Number of Characters. Required in Password	8	1-40 characters Minimum number of characters required in the password.
EMS Numeric Characters Required	Selected	Selected requires one or more numeric characters in the password.

in Password		
EMS Password Attempts Allowed	3	1-10 Number of times the user can attempt to enter the correct password.
EMS Special Characters Required in Password	Not Selected	Selected requires one or more special characters in the password.
EMS Access and Device Code Length	16	8, 16, 32 Number of characters access and device codes have. 32 characters is the most secure, while 8 is the easiest to enter.
EMS Access Code Attempts Allowed	3	1-10 Number of times the user can attempt to enter the access code.
EMS Access Code Failure Action	Apply Cooldown	Apply Cooldown, Wipe Encryption Keys Action to take following unsuccessful Access Code Attempts Allowed: • Apply Cooldown to allow another round of attempts following the specified cooldown period (Cooldown Time Delay and Cooldown Time Increment policies) • Wipe Encryption Keys to have the Encryption client delete the encryption keys on the removable storage, making the encrypted data inaccessible until the owner takes the media to a Dell-encrypted computer for which he has a login.
EMS Access Code Required Message	String Authentication Failed. Please contact your system administrator.	String - 5-512 characters - Authentication Failed: Please contact your system administrator. Message that displays when a user needs to contact you for an access code (after authentication failure). More... Message policies must have non-blank values. "Space" and "Enter" characters used to add lines between rows count as characters used. Messages over the 512 character limit are truncated on the client. Optionally customize the second sentence of the message to include specific instructions about how to contact a help desk or security administrator for authentication failures.
EMS Cooldown Time Delay	30	0-5000 seconds Number of seconds the user must wait between the first and second rounds of access code entry attempts.
EMS Cooldown Time Increment	20	0-5000 seconds Incremental time to add to the previous cooldown time after each unsuccessful round of access code entry attempts.
EMS Access Code Failed Message	String You are not authorized to use this media. Please contact your system administrator.	String - 5-512 characters - You are not authorized to use this media. Please contact your system administrator. Message that displays following unsuccessful Access Code Attempts Allowed. More... Message policies must have non-blank values. "Space" and "Enter" characters used to add lines between rows count as characters used. Messages over the 512 character limit are truncated on the client. Optionally customize the message to include specific instructions about how to contact the help desk or security administrator.
EMS Encryption Rules		Encryption rules to be used to encrypt/not encrypt certain drives, directories, and folders. A total of 2048 characters are allowed. "Space" and "Enter" characters used to add lines between rows count as characters used. Any rules exceeding the 2048 limit are ignored. See Encryption Rules for information. More... Storage devices which incorporate multi-interface connections, such as Firewire, USB, eSATA, etc. may require the use of both EMS and encryption rules to encrypt the endpoint. This is necessary due to differences in how the Windows operating system handles storage devices based on interface type. To ensure encrypting an iPod via EMS does not make the device

		unusable, use the following rules: -R#:\Calendars -R#:\Contacts -R#:\iPod_Control -R#:\Notes -R#:\Photos You can also force encryption of specific file types in the directories above. Adding the following rules will ensure that ppt, pptx, doc, docx, xls, and xlsx files are encrypted in the directories excluded from encryption via the previous rules: ^R#:\Calendars ;ppt.doc .xls.pptx .docx.xlsx ^R#:\Contacts ;ppt .doc.xls .pptx.docx .xlsx ^R#: \iPod_Control ;ppt.doc .xls.pptx .docx.xlsx ^R#:\Notes ;ppt.doc .xls.pptx .docx.xlsx ^R#:\Photos ;ppt.doc .xls.pptx .docx.xlsx Replacing these five rules with the following rule will force encryption of ppt, pptx, doc, docx, xls, and xlsx files in any directory on the iPod, including Calendars, Contacts, iPod_Control, Notes, and Photos: ^R#:\;ppt.doc.xls .pptx.docx.xlsx These rules disable or enable encryption for these folders and file types for all removable devices - not just an iPod. Use care when defining rules to exclude an iPod from encryption. These rules have been tested against the following iPods: iPod Video 30gb fifth generation iPod Nano 2gb second generation iPod Mini 4gb second generation Dell does not recommend the use of the iPod Shuffle, as unexpected results may occur. As iPods change, this information could also change, so caution is advised when allowing the use of iPods on EMS-enabled computers. Because folder names on iPods are dependent on the model of the iPod, Dell recommends creating an exclusion encryption policy which covers all folder names, across all iPod models.
EMS Automatic Authentication	Local	Disabled, Enable Local, Enable Roaming Local automatic authentication allows the Dell-encrypted media to be automatically authenticated when inserted in the originally encrypting computer when the owner of that media is logged in. When the User Roaming key is applied to Encryption External Media, Roaming Automatic Authentication allows Dell-encrypted media to be automatically authenticated when it is inserted in any Dell-encrypted computer the media owner is logged into. When automatic authentication is disabled, users must always manually authenticate to access Dell-encrypted media. Disabling Roaming Authentication helps to prevent users from

		forgetting their password when they take the media home or share it with a colleague. Disabling Roaming Authentication also promotes a sense of awareness from a security perspective for users that the data being written to that media is protected.
EMS Access Encrypted Data on unShielded Device	Selected	Selected allows the user to access encrypted data on removable storage whether the endpoint is encrypted or not. When this policy is Not Selected, the user can work with encrypted data when logged on to any encrypted endpoint. The user cannot work with encrypted data using any unencrypted device.
EMS Device Whitelist		*String - Maximum of 150 devices with a maximum of 500 characters per PNPDeviceID. Maximum of 2048 total characters allowed. "Space" and "Enter" characters count in the total characters used.* This policy allows the specification of removable media devices to exclude from encryption [using the device's Plug and Play device identifier (PNPDeviceID)], thereby allowing users full access to the specified removable media devices. More... This policy is available on an Enterprise, Domain, Group, and User level. Local settings override inherited settings. If a user is in more than one group, all EMS Device Whitelist entries, across all Groups, apply. This policy is particularly useful when using removable media devices which provide hardware encryption. However, this policy should be used with caution. This policy does not check whether external media devices on this list provide hardware encryption. Whitelisting removable storage devices that do not have hardware encryption do not have enforced security and are not protected. *For example, the Kingston® DataTraveler® Vault Privacy model enforces that encryption is enabled to use the device. However, the Kingston DataTraveler Vault model has an unsecured partition and a secured partition. Because it is the same physical removable media device with only one PNPDeviceID, the two partitions cannot be distinguished, meaning that whitelisting this particular device would allow unencrypted data to leave the endpoint.* *Additionally, if a removable media device is encrypted and is subsequently added to the EMS Device Whitelist policy, it remains encrypted and requires a reformat of the device to remove encryption.* The following is an example of a PNPDeviceID, which contains the manufacturer identifier, product identifier, revision, and hardware serial number: `USBSTOR\DISK&VEN_KINGSTON &PROD_DTVAULT_PRIVACY& REV_104\07005B831A0004B4&0` To whitelist a removable media device, provide a string value that matches portions of the device's PNPDeviceID. Multiple device PNPDeviceIDs are allowed. For example, to whitelist all Kingston DataTraveler Vault Privacy models, input the string: `PROD_DTVAULT_PRIVACY` To whitelist both models of Kingston DataTraveler, the Vault and Vault Privacy models, input the string: `PROD_DTVAULT_PRIVACY; PROD_DT_VAULT` Space characters are considered part of the substring to match to a PNPDeviceID. Using the previous PNPDeviceID as an example, a space before and after the semicolon would cause neither of the substrings to be matched, because the space character is not part of the PNPDeviceID. Instructions... 1. Insert removable media. 2. Open System Profiler. 3. Under Hardware, select the device and find the Product ID and Vendor ID, as follows: Capacity:2.06 GB (2,055,019,008 bytes)

		Removable Media:Yes Detachable Drive:Yes BSD Name:disk2 **Product ID:0x5406** **Vendor ID:0x0781 (SanDisk Corporation)** Version: 0.10 Serial Number:0000188C36725BC8 Speed:Up to 480 Mb/sec Manufacturer:SanDisk Location ID:0x24100000 Current Available (mA):500 Current Required (mA):200 Partition Map Type:MBR (Master Boot Record) S.M.A.R.T. status:Not Supported 4. The following whitelist rules can be used: USBVendorName=abc USBVendorNum=0x02 USBVendorNum=2,USBProductNum=3 USBVendorNum=2,USBProdName=abc For this example, add the following key/pair string to the EMS Device Whitelist policy, as shown below: "USBVendorNum=0x0781,USBProductNum=0x05406" (including quotes) 5. When satisfied with the EMS Device Whitelist rules, save and commit the policy.
EMS Trust for Unsupported File Systems	Ignore	*Ignore, Provisioning Rejected, Unshieldable* Specifies how media are handled when formatted by file systems that are not supported with Encryption External Media.
Restricted user list for access to unencrypted media	Dictionary	Users matching this dictionary are restricted from unencrypted media use. Example: <key>AccessUnencryptedMediaRestrictionUsers</key> <dict> <key>dsAttrTypeStandard:AuthenticationAuthority</key> <array> <string>;Kerberosv5;;username1@domainName.com;domainName.com*</string> <string>;Kerberosv5;;@domainName.org;domainName.org</string> </array> </dict>
Restrict Access to Unencrypted Media	Full	*Full, Read Only, Block* Specify how media encrypted with Encryption External Media is handled for users matching unencrypted media restriction.
See basic settings		

Removable Media Policies that Require Logoff

- Windows Media Encryption
- EMS Scan External Media
- EMS Encryption Algorithm
- EMS Exclude CD/DVD Encryption
- EMS Data Encryption Key

Mac Encryption

Mac Encryption

Policy descriptions also display in tooltips in the Management Console. In this table, master policies are in bold font.

Policy	Default Setting	Description
Dell Volume Encryption This technology allows the use of either Mac FileVault full disk encryption or Dell's proprietary Dell Volume Encryption.		
Dell Volume Encryption	On	*On* *Off* Toggle ON to enable Dell Volume Encryption policies. If this policy is toggled to OFF, no Dell Volume Encryption takes place, regardless of other policies.
Encrypt Using FileVault for Mac	Not Selected	*If selected,* FileVault is enabled to encrypt all volumes including System Volumes and Fusion Drives.
Workstation Scan Priority	Normal	*Highest, High, Normal, Low, Lowest* Specifies the relative priority of encrypted folder scanning. High and Highest prioritize scanning speed over computer responsiveness, Low and Lowest prioritize computer responsiveness over scanning speed and favor other resource-intensive activities, and Normal balances the two. The Encryption client checks for a changed Workstation Scan Priority before processing the next file. This policy applies to Dell Encryption, not FileVault encryption.
See advanced settings		

Policy	Default Setting	Description
Mac Global Settings This technology defines Mac encryption behavior, including targeted volumes, polling intervals, and restart policies.		
Volumes Targeted for Encryption	All Fixed Volumes	*System Volume Only* *All Fixed Volumes* The System Volume Only setting secures only the currently running system volume.
Policy Proxy Connections		*String - maximum of 1500 characters* List fully qualified Policy Proxy hostnames, or IP addresses, separated by carriage returns. More... Once the Encryption client finds a valid entry, the remainder of the entries are ignored. Entries are processed in the following order: 1. GKConnections Override (this registry entry overrides all other entries)

		2. GKConnections (this registry entry is set automatically by the Encryption client, based on the this policy) 3. GK This policy works in conjunction with the Policy Proxy Polling Interval policy. You cannot specify ports in this policy. The Encryption client communicates with Policy Proxies using the GKPORT specified during client installation (the default is 8000). Inherited values for this policy accumulate. For the Encryption client to connect to a Policy Proxy specified in this policy, it must be in the same group as the Policy Proxy specified during client installation. Because the Shield supports up to 255 users per endpoint, this policy is available only at the Enterprise level.
Policy Proxy Polling Interval	360	*1-1440 minutes* The interval that the Encryption client attempts to poll Policy Proxy for policy updates, and send inventory information to Policy Proxy. Setting the Policy Proxy Polling Interval below 60 minutes is not recommended, due to potential degradation of performance. The Encryption client also attempts to poll Policy Proxy each time a user logs on.
Force Restart on Policy Updates	Selected	If this policy is set to Selected, the Encryption client will force a computer restart after the specified delay upon receiving a policy update requiring a restart. The delay is specified by the *Length of Each Restart Delay* and *Number of Restart Delays Allowed* policies. If this policy is set to Not Selected, the Encryption client will neither force nor prompt for a restart. The policy requiring the restart will take effect the next time the user restarts their computer.
Length of Each Restart Delay	15	If *Force Restart on Policy Updates* is set to Selected, this value is the number of minutes the user can delay the restart before another restart prompt is displayed. If *Force Restart on Policy Updates* is set to Not Selected, this policy is ignored. More... The Encryption client displays the

		restart prompt for five minutes each time. If the user does not respond to the prompt, the prompt is dismissed and next delay begins. If the five-minute timer expires and no restart delays remain, the computer restarts immediately. **Tip:** Calculate the maximum possible delay as follows (a maximum delay would involve the user responding to each delay prompt immediately prior to the 5-minute mark): (Number of Reboot Delays Allowed x Length of Each Reboot Delay) + (5 minutes x [Number of Reboot Delays Allowed + 1]).
Number of Restart Delays Allowed	3	If *Force Restart on Policy Update* is set to Selected, this value is the number of times the user can delay the restart. If this policy is set to "0", the Encryption client prompts the user to restart immediately and forces the restart if the user does not acknowledge the prompt within five minutes. If *Force Restart on Policy Updates* is set to Not Selected, this policy is ignored.

Advanced Mac Encryption

Policy descriptions also display in tooltips in the Management Console. In this table, master policies are in bold font.

Policy	Default Setting	Description
Dell Volume Encryption This technology allows the use of either Mac FileVault full disk encryption or Dell's proprietary Dell Volume Encryption.		
Dell Volume Encryption	On	*On* *Off* Toggle ON to enable Dell Volume Encryption policies. If this policy is toggled to OFF, no Dell Volume Encryption takes place, regardless of other policies.
Workstation Scan Priority	Normal	Highest, High, Normal, Low, Lowest Specifies the relative Mac priority of encrypted folder scanning. High and Highest prioritize scanning speed over computer responsiveness, Low and Lowest prioritize computer responsiveness over scanning speed and favor other resource-intensive activities, and Normal balances the two. The Encryption client checks for a changed Workstation Scan Priority before processing the next file.
Encryption Algorithm	AES256	*AES-256, AES-128* Encryption algorithm used to encrypt data at the endpoint (all users) level. Encryption algorithms in order of speed, fastest

		first, are AES 128, AES 256. NOTE: This policy applies to Dell Encryption, not FileVault encryption.
Firmware Password Mode	Required	*Required, Optional* Specify if the firmware password in older hardware is optional or required for Dell Volume Encryption.
FileVault 2 Policy Conflict Behavior	Ignore	*Ignore, Report, Convert* Specify behavior when volume is Dell encrypted and policy is for FV2 encryption. Ignore – Default behavior, Dell encrypted volumes are reported as protected if the policy requires FV2 encryption. Report – Conflicted volumes are reported as unprotected. Convert – Dell encrypted volumes are converted to FV2 volumes and reported as unprotected while converting.
See basic settings		
Mac Global Settings This technology defines Mac encryption behavior, including targeted volumes, polling intervals, and restart policies.		
Max Password Delay	300	*0-32400 seconds* Limits the maximum delay in seconds that can be set in the system preferences “max password delay after screen saver or sleep” of the Security panel.
Delay Authentication	Not Selected	If Selected, users are not prompted to activate or authenticate to the Dell Server until required, such as to use media encrypted with Encryption External Media.
No Auth User List	Dictionary	Users matching this dictionary are not required to activate or authenticate to the Dell Server. Example: <key>NoAuthenticateUsers</key> <dict> <key>dsAttrTypeStandard:AuthenticationAuthority</key> <string>;Kerberosv5;;@students.school.edu; students.school.edu</string> </dict>
FileVault 2 PBA User List	Dictionary	Users matching this dictionary are allowed to add themselves to FileVault Preboot Authentication. Example: <key>FV2PBAUsers</key> <dict> <key>dsAttrTypeStandard:AuthenticationAuthority</key> <string>;Kerberosv5;;*@students.school.edu; students.school.edu*</string> </dict>

Port Control

Port Control

Policy descriptions also display in tooltips in the Management Console. In this table, master policies are in bold font.

Policy	Default Setting	Description

Windows Port Control This technology allows for control of all the physical ports on a Windows computer (disable/enable/bypass), and can be customized by port type.		
Windows Port Control	Disabled	Enable or Disable all Port Control System policies. If this policy is set to Disable, no Port Control System policies are applied, regardless of other Port Control System policies. **All** PCS policies require a reboot before the policy takes effect.
Port: Express Card Slot	Enabled	Enable, Disable, or Bypass ports exposed through the Express Card Slot.
Port: USB	Enabled	Enable, Disable, or Bypass port access to external USB ports. USB port-level blocking and HID class-level blocking is **only** honored if we can identify the computer chassis as a laptop/notebook form-factor. We rely on the computer's BIOS for the identification of the chassis.
Port: eSATA	Enabled	Enable, Disable, or Bypass port access to external SATA ports.
Class: Storage	Enabled	PARENT to the next 3 policies. Set this policy to Enabled to use the next 3 Subclass Storage polices. Setting this policy to Disabled disables all 3 Subclass Storage policies - no matter what their value.
See advanced settings		
Windows Device Control This technology allows for control of all the devices on a Windows computer (disable/enable), and can be customized by device type.		
Class: Windows Portable Device (WPD)	Enabled	PARENT to the next policy. Set this policy to Enabled to use the Subclass Windows Portable Device (WPD): Storage policy. Setting this policy to Disabled disables the Subclass Windows Portable Device (WPD): Storage policy - no matter what its value. Control access to all Windows Portable Devices.
Subclass Windows Portable Device (WPD): Storage	Full Access	CHILD of Class: Windows Portable Device (WPD) . Class: Windows Portable Device (WPD) must be set to Enabled to use this policy. Full Access: Port does not have read/write data restrictions applied. Read Only: Allows read capability. Write data is disabled. Blocked: Port is blocked from read/write capability.
Class: Human Interface Device (HID)	Enabled	Control access to all Human Interface Devices (keyboards, mice).

		USB port-level blocking and HID class-level blocking is **only** honored if we can identify the computer chassis as a laptop/notebook form-factor. We rely on the computer's BIOS for the identification of the chassis.
See advanced settings		

Advanced Port Control

Policy descriptions also display in tooltips in the Management Console. In this table, master policies are in bold font.

Policy	Default Setting	Description
Windows Port Control This technology allows for control of all the physical ports on a Windows computer (disable/enable/bypass), and can be customized by port type.		
Subclass Storage: External Drive Control	Full Access	CHILD of Class: Storage. Class: Storage must be set to Enabled to use this policy. This policy interacts with EMS Access to unShielded Media policy. If you intend to have Full Access to media, also set this policy to Full Access to ensure that the media is not set to read only and the port is not blocked. Full Access: External Drive port does not have read/write data restrictions applied Read Only: Allows read capability. Write data is disabled Blocked: Port is blocked from read/write capability This policy is endpoint-based and cannot be overridden by user policy.
Subclass Storage: Optical Drive Control	UDF Only	CHILD of Class: Storage. Class: Storage must be set to Enabled to use this policy. Full Access: Optical Drive port does not have read/write data restrictions applied UDF Only: Blocks all data writes that are not in the UDF format (CD/DVD burning, ISO burning). Read data is enabled. Read Only: Allows read capability. Write data is disabled Blocked: Port is blocked from read/write capability This policy is endpoint-based and cannot be overridden by user policy. Universal Disk Format (UDF) is an implementation of the specification known as ISO/IEC 13346 and ECMA-167 and is an open vendor-neutral file

		system for computer data storage for a broad range of media. To encrypt data written to CD/DVD media: Set EMS Encrypt External Media = True, EMS Exclude CD/DVD Encryption = False, and Storage Class: Optical Drive Control = UDF Only.
Subclass Storage: Floppy Drive Control	Read Only	CHILD of Class: Storage. Class: Storage must be set to Enabled to use this policy. Full Access: Floppy Drive port does not have read/write data restrictions applied Read Only: Allows read capability. Write data is disabled Blocked: Port is blocked from read/write capability This policy is endpoint-based and cannot be overridden by user policy.
Port: PCMCIA	Enabled	Enable, Disable, or Bypass port access to PCMCIA ports.
Port: Firewire (1394)	Enabled	Enable, Disable, or Bypass port access to external Firewire (1394) ports.
Port: SD	Enabled	Enable, Disable, or Bypass port access to SD card ports.
Port: Memory Transfer Device (MTD)	Enabled	Enable, Disable, or Bypass access to Memory Transfer Device (MTD) ports.
See basic settings		
Windows Device Control This technology allows for control of all the devices on a Windows computer (disable/enable), and can be customized by device type.		
Class: Other	Enabled	Control access to all devices not covered by other Classes.
See basic settings		

Global Settings

Global Settings policies are available at the Enterprise, Endpoint Groups, and Endpoints levels. All Global Settings policies are endpoint-based, meaning the policies follow the endpoint, not the user.

Audit Control policies are available at the Enterprise, Endpoint Groups, Endpoints, User Groups, and Users levels.

Policy descriptions also display in tooltips in the Management Console.

Policy	Default	Description
Settings This technology allows control over general settings such as polling intervals, support dialogs, in-app feedback, auto updates, data auditing, and client retention periods.		
Device Lease Period	30	Defines the period of inactivity (in days) before any activated entity (a user, endpoint, or policy proxy) is

		automatically removed from management. The inactivity period is based on the number of days since the Dell Server last received inventory information from the activated entity. Once removed, the entity is no longer included in reports, statistics, and other administrative views. If the activated entity communicates with the Dell Server after the inactivity period has expired, it returns to being in a managed state. The Dell Server always keeps encryption keys in escrow, even for removed endpoints. This ensures recoverability of data through various workflows, such as re-activation and forensic analysis.
Enable In-App Feedback	Not selected	When selected, a user can submit feedback and satisfaction ratings to Dell via a link within the application to a web form.
Server Polling Interval	360 minutes	*1-1440 minutes* How often in minutes the Manager client attempts to contact the Dell Server for updates.
Custom Support Dialog	String	Customizable text that provides information for users to contact IT support for the organization. This allows a maximum of 10,000 characters, which can be four lines with a maximum of 2500 characters each. The text cannot contain line feeds, Enters, or similar characters unless they are escaped.
Dell Data Security Auto Updates		
Enable Software Auto Updates	Not Selected	*Selected* *Not Selected* Selected enables the client update agent to automatically check for updates to Dell security software. If this policy is not selected, no Dell Auto Updates take place, regardless of other policies. If this policy is set, the Update Staging Location must have a network location in its value.
Update Staging Location	String	*String* Network location (UNC) where Dell Server stages Dell update packages. If a network location is not specified in this policy, the Enable Software Auto Updates policy should not be published.
See advanced settings		
Audit Control Policies		
Client Retention Period	30 days	*1-365 days. 30 days default.* Specifies the number of days that the client will hold on to audit data without transmission.

Client Retention Storage	512	*Megabytes of storage space* Specifies the maximum storage space used by the client for audit data without transmission.
See advanced settings		

Advanced Global Settings

Global Settings policies are available at the Enterprise, Endpoint Groups, and Endpoints levels. All Global Settings policies are endpoint-based, meaning the policies follow the endpoint, not the user.

Audit Control policies are available at the Enterprise, Endpoint Groups, Endpoints, User Groups, and Users levels.

Policy descriptions also display in tooltips in the Management Console.

Policy	Default	Description
Settings This technology allows control over general settings such as polling intervals, support dialogs, in-app feedback, auto updates, data auditing, and client retention periods.		
DDP Auto Updates		
Update Check Period	10080	*1-43200 minutes (30 days)* The period in minutes between checks for updates.
See basic settings		