

Deep Instinct™ v4.0 Endpoint Security and Application Security

Deployment Guide



Table of Contents

Legal Notice	1
1. Preface	2
1.1. About this document	2
1.2. Additional relevant documentation	2
1.3. Intended audience	2
1.4. Customer support	2
2. Introduction	3
2.1. Deep Instinct™ system overview	3
3. System requirements	5
3.1. Management Server requirements	5
3.2. D-Clients	5
3.2.1. Windows devices	5
3.2.2. macOS devices	6
3.2.3. Linux devices	7
3.2.4. iOS and iPadOS devices	
3.2.5. Android devices	9
3.2.6 Chrome OS devices	10
3.3 Application Security	10
4 Deployment and installation	11
4.1 Before you deploy	11
4.1. Beruired network ports	
4.1.2 Plan the deployment in stages	 15
4.1.2. Fish the deployment in stages information of the stages in the st	16
4.1.3. Exclusions on analytical software management of a software manag	. 10
4.2.1 Prerequisites	/
4.2.7. Remote deployment of Windows D-Client	,
4.2.2. Remote deployment of Windows D-Client	. 25
4.2.3. Local Deployment of Windows D-Chent	. 45 19
4.2.4. D Clicht installation for Windows VDI	. . . 5/
4.2.3. Installation error codes	55
4.3. Deployment to macOS Devices	55
4.3.1. matos D-client deployment	104
4.3.2. Enabling permissions from the D-cheft console	104
4.5.5. Hacos deployment resources	116
4.4. LITIUX D-CITETIC ITStallation	116
4.4.1. Linux deployment resources	110
4.4.2. Remote deployment with a Linux deployment tool	117
4.4.3. D-Client local installations	110
4.5. MODILE D-CHERIL INStallations	121
4.5.1. D-Client deployment with SOTI MobiControl	122
4.5.2. Local deployment for mobile D-Clients	12/
4.6. Application Security deployment	1/4
4.6.1. Application Security deployment using a predefined Docker image	1/5
4.6.2. Application Security deployment using a customized Docker image	1/8
5. Post-installation	183
5.1. Deployment monitoring	183



5.2. Application Security integration	183
5.2.1. Integration using ICAP	183
5.2.2. Integration using REST API	185
5.3. Client deployment validation	192
5.3.1. EICAR test	193
6. Uninstalling D-Client	194
6.1. Uninstalling D-Client from the Management Console	194
6.2. Uninstalling D-Client from the device	196
6.2.1. Uninstall Windows D-Client	196
6.2.2. Manually Uninstall macOS D-Client	219
7. D-Client upgrades	220
7.1. Upgrading Windows and macOS D-Clients	220
7.2. Upgrading D-Client for Windows VDI	221
7.3. Migrating to a new Linux D-Client	226
7.4. Upgrading Android, Chrome OS, iOS and iPadOS D-Clients	226
8. Troubleshooting options	227
8.1. Debug log collection	227
8.2. Disable/enable D-Client	227
8.3. Changing the Management Server address	227
8.3.1. Changing the Management Server address on a Windows device	227
8.3.2. Changing the Management Server address on a macOS device	228
8.3.3. Changing the Management Server address on a Linux device	230
9. Glossary	232



Legal Notice

Copyright © 2023 Deep Instinct Ltd. All rights reserved.

Deep Instinct and the Deep Instinct Logo are trademarks or registered trademarks of Deep Instinct Ltd. or its affiliates in other countries. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Deep Instinct Ltd. and its licensors, if any.

This document contains proprietary information and as such is protected by Deep Instinct's Non-Disclosure Agreement (NDA), with all that is included in this agreement.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANT-ABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. DEEP INSTINCT (USA) INC. AND ITS AFFILIATES SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSE-QUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUB-JECT TO CHANGE WITHOUT NOTICE.



1. Preface

1.1. About this document

This Deployment Guide provides the information required for deploying and integrating Deep Instinct's security solution in your organization. The scope of the document focuses on the outlining requirements and deployment instructions related to the implementation of the resources provided by Deep Instinct for the purpose of deploying your security solution.

1.2. Additional relevant documentation

Additional documentation for Deep Instinct[™] v4.0 can be found on the customer Portal (also accessible from the Management Console menu). For additional techni-cal information, visit the Deep Instinct Support Center.

Additional technical resources available for this version include:

- Deep Instinct[™] v4.0 Release Notes
- Deep Instinct[™] v4.0 Administrator Guide

1.3. Intended audience

This guide is intended for security system integrators and IT administrators in the organization responsible for deploying and integrating security solutions.

1.4. Customer support

This guide provides information for configuring and managing the Deep Instinct solution using the Management Console. Deep Instinct Support will provide all services to assist the administrator with the information described in this manual, as well as full support for all other issues related to the Management Console. The level and priority of the support provided are based on the severity level of the problem and the Service Level Agreement, as described in the Support and Maintenance Services Agreement.

For more information or support contact: support@deepinstinct.com.



2. Introduction

2.1. Deep Instinct[™] system overview

Deep Instinct provides real-time detection and prevention of zero-day threats and advanced persistent threat (APT) attacks for mobile devices and endpoints. The proactive protection provides unprecedented accuracy in detection and real-time prevention, protecting the organization's entire assets from any threat (known and unknown).

Deep Instinct utilizes the following key components to implement its security solution:

- Deep Instinct[™] Neural Network: The deep learning neural networks are located at the Deep Instinct labs. It is the core component of the deep learning cyber defense solution developed by Deep Instinct. It continuously learns, reflecting the ever-evolving cyber threat arena. The output of its continuous deep learning process is a lightweight prediction model (D-Brain). The D-Brain is then distributed to all managed D-Clients.
- D-Brain (Prediction Model): D-Brain is a lightweight prediction model, which is the output
 of the core component of the deep learning cyber defense solution developed by Deep
 Instinct. It is installed on the D-Clients (endpoint security) and on the containerized applications (application security). Once installed, the prediction model is used to autonomously
 detect and prevent cyber threats on the devices, enabling on-device zero-day and APT
 protection.
- D-Cloud (Reputation Services): The D-Cloud Intel is a file-based reputation engine (verdict system) that provides an additional layer of protection. The D-Cloud is a database composed of billions of files, collected from various data sources, and labelled into different verdicts and classes. Files can be reclassified using the D-Cloud database of intellectual information on known files and the right verdict is updated in real-time.
- D-Client: A lightweight client software installed on devices for endpoint protection. It encapsulates the Deep Instinct prediction model enabling on-device Deep Static and Deep Behavioral Analysis and other key protection engines. The D-Client communicates with the management server for receiving policy and software updates, and for sending events.
- **Application Security**: centralized agentless solution for web application protection that provides malware verdict services through on-demand scanning capabilities of files.
- Management Server and Console: Management and monitoring server is hosted in the cloud. It provides the security administrator with an effective visualization of security events for easy monitoring, including management tools for configuring the organization's security policy.





Deep Instinct™ solution diagram



3. System requirements

3.1. Management Server requirements

Minimum Management Server version: v4.0

Supported browsers:

Deep Instinct[™] Management Console supports the latest versions of the following browsers:

- Google Chrome
- Microsoft Edge
- Firefox

3.2. D-Clients

3.2.1. Windows devices

Windows D-Client requirements

Operating system	 Windows 7 SP1, 8.1, 10, 11 Windows Server 2008 R2 SP1, 2012, 2012 R2, 2016, 2019, 2022 <i>Note:</i> Deep Instinct recommends that you install all security updates by Microsoft. However, the updates from KB2813430, KB4474419, and KB4490628 are required.
.Net Frame- work	Version 3.5 or higher



Certificates	When upgrading/installing the Windows D-Client without an internet connection you need to pre-install the following certificates:
	 AAA Certificate Services
	Thumbprint: d1eb23a46d17d68fd92564c2f1f1601764d8e349
	 COMODO RSA Certification Authority
	Thumbprint: afe5d244a8d1194230ff479fe2f897bbcd7a8cb4
	 DigiCert Assured ID Root CA
	Thumbprint: 0563b8630d62d75abbc8ab1e4bdfb5a899b24d43
	 Go Daddy Class 2 Certification Authority
	Thumbprint: 2796bae63f1801e277261ba0d77770028f20eee4
	 USERTrust RSA Certification Authority
	Thumbprint: 2b8f1b57330dbba2d07a6c51f70ee90ddab9ad8e
	Note: All Microsoft-supported Windows versions typically contain these cer- tificates, and D-Client installation automatically installs these certificates if they are missing (requires an internet connection).
CPU	Dual-core CPU or faster
RAM	Min. 2 GB
	Recommended: 4 GB
	Note: RAM must also meet OS minimum requirements.
Hard drive	500 MB free disk space

3.2.2. macOS devices

macOS D-Client requirements

Operating system	 macOS Ventura (version 13)
	 macOS Monterey (version 12)
	 macOS Big Sure (version 11)
CPU	Dual-core CPU or faster



RAM	Min. 2 GB
	Recommended: 4 GB
	Note: RAM must also meet OS minimum requirements.
Hard Drive	500 MB free disk space

3.2.3. Linux devices

Linux D-Client requirements

Operating system	 AWS Linux 2 kernel 4.14.x
	 Oracle Linux 7.9
	 CentOS 7.9
	 RHEL Server* 7.6, 7.7, 7.8, 7.9, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5
	 Ubuntu 20.04 - including GNOME** desktop environments
	 Added support in LVM framework
	*Operating system must be registered, and available subscrip- tions attached.
	**Ubuntu devices with GNOME require a restart after the D-Cli- ent installation is completed.
CPU	Dual-core CPU or faster
RAM	Min. 2 GB
	Recommended: 4 GN
	Note: RAM must also meet OS minimum requirements
Hard drive	500 MB free disk space

3.2.3.1. Required prerequisite installation packages

Following is the list of prerequisite installation packages required for installing the Linux Client. Depending on the implemented option, these will either be pulled by the installer or need to be pre-installed <u>before</u> installing the Linux Client.

RHEL 7 & RHEL 8



System	Package Name	Package Filename	Source Repo- sitory
RHEL 7	libtomcrypt	libtomcrypt-1.17-25.el7.x86_64	EPEL
	libtommath	libtommath-0.42.0-5.el7.x86_64	EPEL
	libb2	libb2-0.98.1-2.el7.x86_64	EPEL
	mimetic	mimetic-0.9.8-6.el7.x86_64	EPEL
	libarchive	libarchive- 3.1.2-10.el7_2.x86_64	Default RHEL 7 repo
RHEL 8	libtomcrypt	libtomcrypt-1.18.2-5.el8.x86_64	EPEL
	libtommath	libtommath-1.1.0-1.el8.x86_64	EPEL
	libb2	libb2-0.98.1-6.el8.x86_64	EPEL
	mimetic	mimetic-0.9.8-14.el8.x86_64	EPEL
	libarchive	libarchive- 3.3.3-4.el8.x86_64	Default RHEL 8 repo



NOTE

The required versions of the libraries listed for the RHEL 7 & RHEL 8 packages above are subject to change in future Linux Client (agent) releases.

Ubuntu 20.04 packages



NOTE

All packages should be available through the package manager.

Table 1. List of Ubuntu 20.04 packages

System	Package Name	Source Repo- sitory
Ubuntu 20.04	rpm	Default Ubun-
	libtomcrypt1	tu 20.04 repo
	libtommath1	



System	Package Name	Source Repo- sitory
	curl	
	libmimetic0v5	
	minizip	
	libpython2.7	
Ubuntu 20.04 systems	python3	Default
with GUI(python3-pip	Default
(Required in addition to	python3-tk	Default
for Ubuntu 20.04 sys-	python3-pil	Default
tems))	python3-pil.imagetk	Default
	gir1.2-appindicator3-0.1	Default
	idle-python3.8	Default
	flatbuffers	Default
	(From pip package manager)	
	PyGObject	Default
	(From pip package manager)	
	pystray	Default
	(From pip package manager)	

3.2.4. iOS and iPadOS devices

Operating system	iOS 12.1 and higher
Storage	80 MB storage space

3.2.5. Android devices

Operating system	Android 9.0 or higher
Storage	70 MB storage space

3.2.6. Chrome OS devices

Operating system	Chrome 87.0 or higher
Storage	70 MB storage space

3.3. Application Security

Docker host	 Docker installed
	 Network connectivity — 1 Gbps Ethernet port or faster
	 IP forwarding enabled

Docker container (per container)	Operating system	 Red Hat Enterprise Linux (RHEL) Server 7.9 CentOS 7.9
	For RHEL	Operating system must be registered, and available subscriptions attached.
	CPU	 4-Cores, 2.0 GHz or higher Requirements may change depending on the total number of files that re- quire scanning Each CPU core can handle approxi- mately 20 MB/second peak capacity for file scans
	RAM	16 GB pr higher Requirements may change depending on the total number of files that require scanning
	Hard drive	60 GB or higher



4. Deployment and installation

Deep Instinct[™] integrates with many systems to simplify the deployment process. Depending on your organization's system and clients, the deployment flow varies. You can deploy Deep Instinct[™] on the following device types:

- Windows D-Client Installation
- macOS D-Client Installation
- Linux D-Client Installation
- Mobile D-Client Installations
- Application Security Deployment

4.1. Before you deploy

Deep Instinct's solution works independently from other IT and security assets. The D-Appliance and D-Clients add an additional, critical layer of security to the organization. They can be deployed in augmentation to any software solution (including other security solutions) implemented in the customer's environment and do not require any significant modifications to the existing infrastructure.

4.1.1. Required network ports

Specific network ports are used by Deep Instinct and must be opened to enable communication between the Management Console, management server (D-Appliance), Syslog and Active Directory servers, D-Clients, and the Application Security container.

) IMPORTANT

Verify that all firewalls have been configured appropriately to allow communication on the ports specified in the following table.

The following table lists the network ports required by Deep Instinct for communication. There are configurable and non-configurable ports, where:

• **Configurable** — ports that are allocated by your organization and can be configured through the Console Settings page.



• **Non-configurable** — specified port is used by Deep Instinct and blocking this port will result in the product's inability to function as intended.

Communication De- scription	Source	Destination	Port(s)
Deep Instinct Manage- ment Server/SMTP Serv- er	Management Serv- er (D-Appliance)	SMTP Server	Configurable
Deep Instinct Manage- ment Server/Active Di- rectory (AD) Server	Management Serv- er (D-Appliance)	AD Server	Configurable
Administrators' connec- tion to the Management Console	Management Con- sole	Management Server	443
Reputation Services (D- Cloud) D-Cloud ad- dress: cloud-api.deepin- stinctweb.com	Management Serv- er (D-Appliance) D-Client	Reputation Services En- gine (D-Cloud)	443



Communication De- scription	Source	Destination	Port(s)
Communication Description D-Client/Management Server (D-Appliance) Connection required for downloading configura- tion files and policy to the D-Clients as well as sending event notifi- cations to the Manage- ment Server.	Source D-Client	Destination Management Server (D-Ap- pliance) FQDN exam- ples for the Management Server: • mycompa- ny.custom- ers.deepin- stinct- web.com • apiv2-my- compa- ny.custom- ers.deepin- stinct- web.com ("apiv2- <fqdn>")</fqdn>	 Port(s) 443 Note the following: When installed, the D-Clients set the port to 443. If this port is not available, the port is set to 4339. When port 443 is used, the connectivity needs to open to both the D-Appliance FQDN, and to "apiv2- FQDN>". When port 443 is used with maccos D- Clients, the connectivity also needs to
			 the connectivity also needs to open to "api- <fqdn>".</fqdn> Once the port is set during instal- lation, the D-Cli- ents continue to use this port in-
			cluding up- grades.



Communication De- scription	Source	Destination	Port(s)
Communication De- scription Application Security / Management Server (D- Appliance) Connection required for registering with the Management Server, status reporting, and event notifications as well as downloading configuration files and policy updates.	Source Application Securi- ty	Management Server (D-Ap- pliance) *Depending on the API ver- sion, requests are directed using one of the following DNS names (both return the same IP address): • For API v1: mycompa- ny.custom- ers.deepin- stinct- web.com	Port(s) 443
		 For API v2 ("apiv2- <fqdn>".):</fqdn> apiv2-my- compa- ny.custom- ers.deepin- stinct- web.com 	
REST API file scan re- quests	Custom app		Configurable
Communication with Sy- slog Server Note: The port defined for this communication is allocated by your organi- zation.	Management Serv- er (D-Appliance)	Syslog Server	Configurable
ICAP file scan requests	Custom app		Configurable



Communication De- scription	Source	Destination	Port(s)
Android D-Client/Man- agement Server (D-Ap- pliance) communication during deployment	Android D-Client	Management Server (D-Ap- pliance)	4331
Android D-Client/Deep Instinct POC Server Connection required for D-Client access to the application database on the Deep Instinct POC Servers.	Android D-Client	Management Server (D-Ap- pliance)	7443
Management Console and Server screen-re- fresh functionality.	Management Con- sole	Management Server	8084

4.1.2. Plan the deployment in stages

It is recommended to deploy the D-Clients gradually. Start the initial deployment with a small number of devices, and then increase the number of deployed endpoints in stages, by order of magnitudes.

The initial stage allows your organization to get familiar with the features, functions, and options available with Deep Instinct. It provides you with a way to determine the level of support you may need during and after the full deployment process.

The initial stage also provides your organization with a means to refine the deployment process without impacting your organization. During this stage, we recommend that the 'Prevention' action is disabled in the policies, and to analyze the 'Detection' events. Some of the detected files may not be malicious and can be added to the Allow List.

4.1.2.1. Define the initial stage

In the initial stage, select devices that best represent your actual environment. Try to include variations in the operating systems and software that exist in your actual environment. To group devices, you may want to use Device Groups and Device Tags, described in the Administrator Guide.

4.1.2.2. Initial deployment

Review all deployment methods provided to you and determine which methods will be used in the full deployment. The initial stage should include all methods that will be implemented in the full deployment.



4.1.3. Exclusions on antivirus software

If your Windows or macOS devices have antivirus software installed, it is recommended to include several files, folders and processes to the exclusion list of the antivirus software. This eliminates the possibility of conflicts and performance issues with your antivirus. Add the following objects to your antivirus's exception list:

Platform	Folder Exclusions	File and Process Exclusions
Windows	 C:\Program Files\DeepInstinct\ C:\ProgramDa- ta\DeepInstinct\ 	 DeepMgmtService.exe DeepNetworkService.exe DeepTHService.exe DeepStaticService.exe DeepUI.exe DeepUninstaller.exe DeepCIService.exe DeepETPService.exe
macOS	N/A	/Library/DeepInstinct

The following table contains information and links to assist you with adding objects to the exception lists for several enterprise antivirus software:

McAfee	Files may be added to the process exception list via the Pro- cesses Policies to eliminate any possible conflict with Deep Instinct processes. For more information, see https://kc.mca- fee.com/corporate/index?page=content&id=KB58692
Symantec Endpoint Protection	Objects may be added to Symantec's exception list by creating a Centralized Exception policy. For more information, see https://support.symantec.com/en_US/arti- cle.TECH183201.html.
Trend Micro	Files may be added to the Behavior Monitor- ing exception list to eliminate any possible con- flict with Deep Instinct processes. For more in- formation, see https://docs.trendmicro.com/en-us/enter- prise/officescan-110-sp1-server/using-behavior-monit/behav- ior-monitoring/behavior-monitoring-12345.aspx



4.2. Windows D-Client installation

Before deploying, refer to the "Prerequisites" and make sure you have all the requirements in place for your deployment.

You can deploy D-Clients on Windows devices by using one of the following deployment methods:

- Remote deployment:
 - Remote deployment using SCCM
 - Remote deployment using GPO
- Local deployment (directly from the device):
 - Local deployment using the Installation CLI command
 - Local deployment using the Installation screen
- Deploying in a VDI environment refer to D-Client Installation for Windows VDI for details.

4.2.1. Prerequisites

Verify that you have completed the following before you deploy the Windows D-Client.

- Active Directory for organizations using Active Directory, an Active Directory user with read-only privileges must exist before running the Startup wizard to acquire the organization's list of managed Windows devices. If not, configure the Active Directory (AD) Credentials from the General Configuration screen. For more information, see the Administrator Guide.
- Remote deployment tools you can deploy Windows D-Clients using the SCCM (System Center Configuration Manager) or GPO (Group Policy Object) tools. Click on the corresponding links for instructions on how to deploy using these tools.
- Access to registry values D-Clients need access to add registry values in order to be installed.
- **General configuration and policies** configure Deep Instinct's General Configuration settings and relevant policies. For more information, see the the Administrator Guide.
- Add Deep Instinct to Exclusion list If your Windows devices have an antivirus software installed, add Deep Instinct's objects to your antivirus's exclusion list.





D-Client installation package — download the Windows D-Client installation package from the Management Consoles' Windows Deployment Resources screen.

4.2.1.1. Windows Deployment Resources

The Windows Deployment Resources screen provides the resources for you to deploy and install Windows D-Client on your devices. It provides you the ability to download the Windows D-Client and preview the required CLI command to install Windows D-Client on your devices.

To download the Windows D-Client file:

- 1. Log on to Deep Instinct.
- 2. From the Navigation pane, click Settings \rightarrow Deployment \rightarrow Windows.

Image: Section of Sectin of Sectin of Sectin of Section of Section of Section of Section o	image:	Southbaard Windows macOS Linux ChromeOS Mobile Image: SouthBaard South Comparison of SouthBaard	So Deshboard Windows mac03 Linux Chome 03 Mobile Image: Solution of Common and Common	Image: Section of the control of th	d≋p instinct	Q	Settings > Deployment		
Monitor , Download installation File 3.42.35	Monitor , Download installation File 3.42.35 , Policy , Select the version and download Select Tenant Tenants Selectings CLI Pericer Le network proxy Delient disabled after installation	• Monitor • Download installation File 3.42.35 • • Policy • Select the version and download • Tenant. • • Asacto • Select Tenant • Tenant. • Tenant. • • • Revoke and Regenerate Token • <t< td=""><td> Monitor Monitor Policy Select the version and download Assets Select Ternant Ternants Installation Tole Ternants Installation Tole Revoke and Regenerate Token Installation for Vol Installation for Vol Installation for Vol Derive Tag Derive Tag Monitor for Unitallation Derive Tag Monitor for Vol Installation for Vol Installation for Vol Installation for Vol Installation for Vol Derive Tag Monitor for Installation Derive Tag Monitor for Molece Tag Monitor for Vol Installation for Vol Installation for Vol Revoke and Regenerate Token Derive Tag Monitor for Vol No Installation for Vol Derive Tag Monitor for Molece Tag Monitor for Select Tablebion Derive Tag Monitor for Vol Select Tablebion Derive Tag Monitor for Vol Derive Tag Monitor for Vol Classification Derive Tag Monitor for Vol Derive Tag Monitor for Vol Classification Derive Tag Monitor for Vol Derive Tag <</td><td>Monitor Policy Policy Select the version and download Select the version and download Tenant: Select Tenant Tenant: Tenant:<th>B Dashboard</th><td></td><td>Windows macOS Linux Chrome OS Mobile</td><td></td><td></td></td></t<>	 Monitor Monitor Policy Select the version and download Assets Select Ternant Ternants Installation Tole Ternants Installation Tole Revoke and Regenerate Token Installation for Vol Installation for Vol Installation for Vol Derive Tag Derive Tag Monitor for Unitallation Derive Tag Monitor for Vol Installation for Vol Installation for Vol Installation for Vol Installation for Vol Derive Tag Monitor for Installation Derive Tag Monitor for Molece Tag Monitor for Vol Installation for Vol Installation for Vol Revoke and Regenerate Token Derive Tag Monitor for Vol No Installation for Vol Derive Tag Monitor for Molece Tag Monitor for Select Tablebion Derive Tag Monitor for Vol Select Tablebion Derive Tag Monitor for Vol Derive Tag Monitor for Vol Classification Derive Tag Monitor for Vol Derive Tag Monitor for Vol Classification Derive Tag Monitor for Vol Derive Tag <	Monitor Policy Policy Select the version and download Select the version and download Tenant: Select Tenant Tenant: <th>B Dashboard</th> <td></td> <td>Windows macOS Linux Chrome OS Mobile</td> <td></td> <td></td>	B Dashboard		Windows macOS Linux Chrome OS Mobile		
Policy Select the version and download In Assets Select Trant Tenants Tenants In Reports Installation Token Revoke and Regenerate Token Revoke and Regenerate Token Select the options to display and copy the installation Revoke and Regenerate Token Installation Token CLI Preview Select the options to display and copy the installation Installation Installation for VDI Installation Installation for VDI Installation Installation device Tag Add top Installet/Anaged_deep.exe diproduct customers deepinstinctweb com /token ab218669-1066-48a7-988c-42848d2a1806 Copy CLI Command Copy CLI Command	Policy Setting Set	Policy · Select the version and download Select Travet: Tra	Policy Select the version and download In Assets Select Treamt Intelliction Will influence the installation token Intelliction Token Installation Installation Installation Installation Installation Installation Token ab218d69 Incid-48a7 988c 42848d2a1806	Policy Policy Select the version and download Tenants Tena	Monitor		Download Installation File 34.2	35 -	
A Asets , Select Trant Internal, I Int	Assets Sectorant Totant selection will influence the installation token In Report Installation Token Settings CLI Proview Settings Settings Installation for VDI Settings CLI Bereiew of Installation Settings No initial set and invisibilition Settings CLI Proview Settings Settings Settings Settings Settings Settings Settings Settings <p< td=""><td>Asset Sectorant Tennets Tennets In Reports Tennets/sectoralisation token Sectors Tennets/sectoralisation token In Reports Tennets/sectoralisation token Sectors Tennets/sectoralisation token In Reports CUPrevier Sectors of the sector of the sectoralisation to the installation Cul command (for D-Client version 2.4 and later) In Installation for V01 Installation for V01 In No Initial full can after installation In Orient disease of the installation In Previer Sectors of the sectoralisation Installation for V01 In No Initial full can after installation In Previer III Content disease of the installation In Previer IIII Content disease of the installation Installation for V01 In Sector regions Installation for V01 In Stallation for V01 In Previer IIII Content disease of the installation In Sector regions InstallerManaged_deep nere diproduct.cuutomers deepinstitute/bcom /token ab218669-lace.48a7 988: 42848d2a1806 Copy CLI Command</td><td>In Ased Select Team In Reports Teamint selection will influence the installation token In Reports Installation Token IIII Theorem Select 428.43243 1806 Is Settings CL Preview Select the options to display and copy the installation CL command (for D-Client version 2.4 and later) In No Initial for You In No Initial for an administration on the installation Image: Client Teaming Client Tea</td><td>Image: Sector Terrant Image: Sector Terrant Image: Sector Terrant Terrant Sector will influence the installation token Image: Sector Terrant Image: Sector Terrant Image: Sector Terrant Terrant Sector Terrant Image: Sector Terrant Sector Terrant Terrant Sector Terrant Image: Terrant Sector Terrant Terrant Sector Terrant Image: Terrant Sector Terrant Terrant Sector Terrant Image: Terrant Sector Terrant Terrant Secto</td><th>Policy</th><td></td><td>Select the version and download</td><td></td><td></td></p<>	Asset Sectorant Tennets Tennets In Reports Tennets/sectoralisation token Sectors Tennets/sectoralisation token In Reports Tennets/sectoralisation token Sectors Tennets/sectoralisation token In Reports CUPrevier Sectors of the sector of the sectoralisation to the installation Cul command (for D-Client version 2.4 and later) In Installation for V01 Installation for V01 In No Initial full can after installation In Orient disease of the installation In Previer Sectors of the sectoralisation Installation for V01 In No Initial full can after installation In Previer III Content disease of the installation In Previer IIII Content disease of the installation Installation for V01 In Sector regions Installation for V01 In Stallation for V01 In Previer IIII Content disease of the installation In Sector regions InstallerManaged_deep nere diproduct.cuutomers deepinstitute/bcom /token ab218669-lace.48a7 988: 42848d2a1806 Copy CLI Command	In Ased Select Team In Reports Teamint selection will influence the installation token In Reports Installation Token IIII Theorem Select 428.43243 1806 Is Settings CL Preview Select the options to display and copy the installation CL command (for D-Client version 2.4 and later) In No Initial for You In No Initial for an administration on the installation Image: Client Teaming Client Tea	Image: Sector Terrant Image: Sector Terrant Image: Sector Terrant Terrant Sector will influence the installation token Image: Sector Terrant Image: Sector Terrant Image: Sector Terrant Terrant Sector Terrant Image: Sector Terrant Sector Terrant Terrant Sector Terrant Image: Terrant Sector Terrant Terrant Sector Terrant Image: Terrant Sector Terrant Terrant Sector Terrant Image: Terrant Sector Terrant Terrant Secto	Policy		Select the version and download		
At Tenants Installation Token Revoke and Regenerate Token In Reports ab21866 hote 486 / 988c 42848d2a 1806 Settings • CLI Preview Settings • CLI Preview Settings • CLI Preview On Initial for CVD Initialization for VVI Initialization for VVI Initialization for VVI Initialization for VVI Initialization Initialization for VVI Initialization Initialization Initialization for VVI Initialization for VVI Initialization Initialization for VVI Initialization Initialization Initialization for VVI Initialininitialinininitialization Initialization	A: Tenants Installation Token Revoke and Regenerate Token ink Reports ab218dob Toke 483/988-42848d23 806 Revoke and Regenerate Token is Settings CLI Preview Setect the options to display and copy the installation CLI command (for D-Client version 2.4 and later) is settings CLI Preview Setect the options to display and copy the installation CLI command (for D-Client version 2.4 and later) is network proxy InstallerManaged.deep.ere diproduct customers deepinstinctweb.com /token ab218d69 1cde 48a7 988c 42848d2a1806 is network proxy InstallerManaged.deep.ere diproduct.customers deepinstinctweb.com /token ab218d69 1cde 48a7 988c 42848d2a1806 installerManaged.deep.ere diproduct.customers deepinstinctweb.com /token ab218d69 1cde 48a7 988c 42848d2a1806	A: Tenards Installation Token Revoke and Regenerate Token iki Reports ab21866-106-8837-9886-42848231806 Revoke and Regenerate Token (i) Reports CLI Preview Select the options to display and copy the installation CLI command (for D-Client version 2.4 and later) Image: Client version 2.4 and later) (ii) Use network provy Image: Im	A: Transis Installation Token Installation Token 	x. Tennits installation token Revoke and Regenerate Token ing Reports bitstallation Token Revoke and Regenerate Token is Settings CLI Preview Setect the options to display and copy the installation CLI command (for D Client version 2.4 and later) is settings CLI Preview Setect the options to display and copy the installation CLI command (for D Client version 2.4 and later) is the installation for VDI Is the installation for VDI Display and for installation is the installation for VDI No installer installation Display and for installation is before Tag Add log Installer Managed, deep exe diproduct, customers deepinstinctweb com /token ab218d69-1cdc-48a7-988c-42848d2a1806 Copy CLI Command Copy CLI Command Copy CLI Command	_□ Assets		Select Tenant	् Tenant_1	
In Reports instatutory (Notif) revolut and regulation (Notif) is Settings instatutory (Notif) CLI Proview Settings instatutory (Notif) CLI Proview Settings CLI Proview Setect the options to display and copy the instatlation CLI command (for D Client version 2.4 and later) Instatlantion for VDI Instatlation for VDI Instatlation Device Tag Add later Instatler/Managed_deep.exe diproduct customers deepinstinctweb com /token ab218669 1066-48a7 4986-42848d2a1806 Copy CLI Command	In Reports Installandon (Notif) Installandon (Notif) Installandon (Notif) Image: Settings Image: Setings Image: Settings Ima	In Reports ab214669-1006-483474886-42848d231806 Image: Settings CLI Preview Settings CLI Preview Settings CLI Preview Settings Image: Settings Image: Ima	In Reports microal and any Agenetical 10.04m (i) Reports CLI Preview Select the options to display and copy the installation CLI command (for D-Client version 2.4 and later) Iiii I adaption for YOI Iiii No No Initial adaption of a resultation Iiiii D-Client version Iiiii D-Client version Iiiiii D-Client version Iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii	In Reports ab218669-10d-48a7986-428482a1806 Settings CLI Preview Select the options to display and copy the installation CLI command (for D Client version 2.4 and later) Use network prov installation for VDI installation Device Tag Add tog InstallerManaged_deep exe diproduct customers deepinstinctweb com /token ab218609-10do-48a7988c-42848d2a1806 Copy CLI Command	음. Tenants		Tenant selection will influence the installation token	Development 7	
Settings CLI Proview Settings Settings CLI Proview Settings Settings Client designed and copy the installation CLI command (for D Client version 2.4 and later) Installation for VDI Installation for VDI Colient disabled after installation Deriver Tag InstallerManaged. deep exe diproduct customers deepinstinctweb com /token ab218669 1066-4837-9886-42848d2a1806 Copy CLI Command	Settings CLI Proview Settings Settings CLI Proview Settings Settings Cliptic disability Collect disability Collect disability Collect disability Collect disability Copy CLI Command Copy CLI Command	Settings CUPreview Settings Settings Settings Cupreview Settings	Settings CLI Preview Settings Setting	Settings CLI Preview Setet the options to display and copy the installation CLI command (for D Client version 2.4 and later) I dise network prov I is stallation for VDI D Client disabled after installation I notable disabled after installation D client disabled after installat	II Reports		ab218d69-1cdc-48a7-988c-42848d2a1806	Revoke and Regenerate TC	sen
Copy CLI Command	Copy CLI Command	Copy CLI Command	Copy CLI Command	Copy CLI Command	(2) Settings		CLI Preview Select the options to display and copy the installation CLI command (for D-Client version 2.4 and later) Use network proxy CLI ataliation for VDI CLI ataliation for VDI CLI ataliation after installation CLI command (for D-Client version 2.4 and later) CLI ataliation CLI ataliati	1842a1806	
Copy CLI Command	Copy CLI Command	Copy CLI Command	Copy CLI Command	Copy CLI Command					
								Copy CLI Comm	and

- 3. Select the version of the Windows D-Client you want to download from the Download Installation File dropdown box.
- 4. Click 🛃 and the installation file is downloaded.

4.2.1.2. Windows D-Client CLI Command

To install the D-Client on a Windows device the installation CLI command must be used. This command has several options and these options must be defined. This section describes the installation CLI command and the available options.

Refer to the following table for the list of installation CLI commands.



What do you want to do?	Command
Install the D-Client on a Windows device	<pre><exe path=""><installation file=""> <server address=""> /token <installation token=""> [/tag <tag>] [/disabled] [/nfs] [/np / manualproxy <proxy url="">:<proxy port="">]</proxy></proxy></tag></installation></server></installation></exe></pre>
Install the D-Client on a VDI ma- chine	<pre><exe path=""><installation file=""> <serv- address="" er=""> /token <installation ken="" to-=""> /vdi [tag <tag>] [/disabled] [/nfs] [/np /manualproxy <proxy url="">:<proxy port="">]</proxy></proxy></tag></installation></serv-></installation></exe></pre>
Install the D-Client on a Windows server with the Cluster Shared Volume (CSV) feature enabled	<pre><exe path=""><installation file=""> <serv- address="" er=""> /token <installation ken="" to-=""> /ignorecsv [/tag <tag>] [/disa- bled] [/nfs] [/np /manualproxy <proxy url="">:<proxy port="">]</proxy></proxy></tag></installation></serv-></installation></exe></pre>

Where:

Command Pa- rameter	Description	Comments
<exe path=""></exe>	Path for the appropriate installation file, where all the Windows devices have access	N/C
<installa- tion file></installa- 	file name for the appropriate installa- tion file	N/C
<server ad-<br="">dress></server>	FQDN for the D-Appliance	N/C
<installa- tion token></installa- 	ID of the installation token, as dis- played in the Windows Deployment Resources screen	N/C

Command Pa-	Description	Comments		
<tag></tag>	Adds a tag associated with the deployed devices. Use quotation marks to enter values with spaces or special characters.	 Optional The Device Tag must comply to the following: Maximum length is 256 characters Device Tags are case sensitive Valid characters: Letters (a-z, A-Z) Numbers (0-9) Spaces representable in UTF-8 Special characters: +-=:/@ Device tags can be used with rules to automatically add devices to a Device Group. It can also be used for selecting and filtering devices in the Management Console. For more information, see the Administrator Guide. 		
/disabled	When /disabled is included, the D- Client is disabled during the installa- tion. This allows the administrator to select when to initially enable the D- Client.	Optional		
/nfs	Starts the D-Client without performing the initial full scan	Optional		
/np	Enables the use of a network proxy server using the default proxy set- tings.	 Optional Cannot be used with / manualproxy 		

Command Pa- rameter	Description	Comments
/manual- proxy	Enables the use of a network proxy server, using the specified settings of the proxy server URL and port number.	 Optional Only available for D-Client v2.5.1 or higher Do not use with /np
<proxy url=""></proxy>	URL for the proxy server, including the scheme	N/C
<proxy port></proxy 	Port number to access the proxy serv- er	N/C
/vdi	Required when installing the D-Client on a VDI machine. For more informa- tion, see D-Client Installation for Win- dows VDI	N/C
/ignorecsv	Required when installing the D-Client on a Windows server with the Cluster Shared Volume (CSV) feature enabled.	Files accessed from the Clus- ter Shared Volume are not scanned. However, all files copied to the local drive are scanned.
<abortifno- ServerCon- nection></abortifno- 	Enables the D-Client installer to run a connectivity check with the manage- ment server before deployment. When included, if the D-Client fails to estab- lish connectivity, the installation proc- ess is aborted.	 Optional See "Connectivity check flag" for details on the use of this flag

Windows CLI command

For the following values:

- exe path = c:\users\administrator\downloads\
- installation file = Installer.exe
- server address = customer.deepinstinctweb.com
- installation token = 12345678
- System without MSP support

The CLI command would be:

```
c:\users\administrator\downloads\Installer.exe customer.deepinstinct-
web.com /token 12345678
```

Connectivity check flag

By default, during the D-Client installation, the installer attempts to establish connectivity during the initial installation phase with the Management Server for registration and policy updates. If there is no connectivity, the D-Client will continuously retry to establish a connection for registration unless the process is aborted.

The **Connectivity Check** feature enables the D-Client installer to run a connectivity check with the management server before deployment, preventing scenarios where the installation is only partially performed.

When the feature flag is included in the installation, if the D-Client fails to establish connectivity, the installation process is aborted and the following error message is prompted: *"Aborting installation due to inability to establish connectivity with the Management Console, please check Internet connectivity or D-Console URL/Address"*.

This feature is especially beneficial in the following use cases:

- Deployments using remote software distribution in cases where the installation has only been partially performed (without registration,) due to lack of connectivity, the client software will be indicated as installed on the MDM side, however, there will be no indication that the client has not been activated or registered and the devices will not appear in the Device List in the Management Console.
- Deployments including air gap devices or devices that are not connected to the internet for security reasons — if the installation process is not aborted, these types of devices, for example, will be stuck continuously trying to establish connectivity and the complete installation process would need to be repeated (uninstall and then re-install of the client).



The "Connectivity Check' feature is enabled as a Windows D-Client CLI command which you include in the installer CLI before deployment:

<Installer.exe MY_SERVER.com /token MyToken /abortIfNoServerConnection /nfs>

Where:

- My_SERVER server address (D-Appliance FQDN)
- My Token ID of the installation token (shown in the Windows Deployment Resources page in the Management Console)



This CLI Command cannot be copied from the CLI Preview area of the Management Console Devices → Deployment → Windows screen.

4.2.2. Remote deployment of Windows D-Client

4.2.2.1. D-Client deployment with SCCM

System Center Configuration Manager (SCCM) is a Microsoft management tool that can deploy D-Clients on all your organization's Windows devices. The following procedure is based on using SCCM 2012.

The D-Client deployment process using SCCM requires the following:

- Deep Instinct Windows EXE installation file. The file may be downloaded from the Windows Deployment Resources screen.
- Determine the installation CLI command to run with SCCM.
- Create a package for D-Client deployment.
- Deploy the D-Client installation package.

Creating a Package for D-Client Deployment

To create a package for deployment:

1. Download the installation file from the Windows Deployment Resources screen.



- 2. Save the installation file to a location where all the organization's Windows devices have access.
- 3. Start Microsoft System Center Configuration Manager.
- 4. In the Configuration Manager console, click Software Library.
- 5. In the Software Library workspace, expand Application Management.

Software Library	<
A Overview	*
A Gapplication Management	
Applications	
💽 Packages	
Approval Requests	
[]‡] Global Conditions	
🗮 App-V Virtual Environments	-
豫 Windows Sideloading Keys	
Application Management Policies	
 Software Updates 	
🟹 All Software Updates	
🔊 Software Update Groups	
💽 Deployment Packages	
Automatic Deplovment Rules	-
Assets and Compliance	
Software Library	
Monitoring	
Administration	
	-

6. Right-click Packages and click Create Package. The Create Package and Program Wizard opens. Perform the following:

deep instinct

<u>a</u>	Create Package and Program Wizard
Package	
Package Program Type Standard Program Requirements Summary Progress	Specify information about this package Enter a name and other details for the new package. To take full advantage of new features that include the Application Catalog, use an application instead. Name: Deep Instinct 3.0
Completion	Description: ^ Manufacturgr:
	Language: en Version: 3.0 ✓ This package contains source files Sourge folder: \\servername\sharename\path Brgwse
	< Previous Next > Summary Cancel

- a. Enter the name of the package.
- b. As an option, enter the description, manufacturer, language, and/or version of the package. It is recommended to enter the version number for version control.
- c. Select This package contains source files.
- d. Click Browse. Go to the folder where the installation file is located and select the folder.
- e. Click Next.





7. Select Standard program. Click Next and perform the following:





1	Crea	ate Package and Program Wizard	×
Standard Progr	ram		
Package Program Type Standard Program Requirements	Specify informati	Deep Instinct 3.0	
Summary Progress	<u>C</u> ommand line: S <u>t</u> artup folder:	Installer.exe customer.deepinstinctweb.com/token 12345678	
Completion	<u>R</u> un:	Normal	~
	Program can run:	Only when a user is logged on	~
	Run mod <u>e</u> :	Run with administrative rights	~
	Allow users to view	and interact with the program installation	
	<u>D</u> rive mode:	Runs with UNC name V	
	Reconnect to distri	bution pgint at log on	
		< Previous Next > Summary Can	:el

- a. Enter the name of the D-Client installation file.
- b. Type the CLI command with all required options and values in the Command line. For details on how to define the CLI command, see Windows D-Client CLI Command.
- c. Change Run Mode to Run with administrative rights and click Next.



1	Create Package and Program Wizard	X
Requirements		
Package Program Type Standard Program	Specify the requirements for this standard program	
Requirements Summary Progress Completion	Bun another program first Package: Program: Always run this program first Platform requirements This program can run on any platform This program gan run only on specified platforms All Windows RT All Windows RT 8.1 All Windows 10 Professional/Enterprise and higher (32-bit) All Windows 10 Professional/Enterprise and higher (64-bit) All Windows 8.1 (64-bit) All Windows 8.1 (64-bit) All Windows 8.1 (64-bit) Windows Embedded 8 Industry (64-bit) Windows Embedded 8.1 Industry (64-bit)	
	Maximum allowed run time (minutes): (<u>Previous</u>) <u>Next ></u> <u>Summary</u> Cance	:1

8. Click **Next** and a summary of the package settings are displayed.





3	Create Package and Program Wizard	x
Summary		
Package Program Type Standard Program	Confirm the settings	
Requirements	Details:	
Summary Progress Completion	General: • Name: DeepInstinct3.0 • Description: • Version: 3.0 • Publisher: • Language: en • Source files: Vservername\sharename\path • Always obtain files from the source folder Program Type: Standard Program Program: • Name: DeepInstinct3.0 • Command line: Installer.exe customer.deepInstinctweb.com/token 12345678 • Start in: • Run: Normal • Run: Normal • Run mode: Run with administrative rights • Program can run: Only when a user is logged on • Drive mode: Runs with UNC name Requirements: • Platforms supported: Any • Maximum allowed runtime(minutes): 120	
	To change these settings, click Previous. To apply the settings, click Next.	
	< Previous Next > Summary Cancel	

9. Click **Next**. A progress bar and then a message appears to indicate that the wizard completed successfully.



1	Create Package and Program Wizard	x
Completion		
Package Program Type Standard Program Requirements Summary	The Create Package and Program Wizard completed successfully	
Progress Completion	 Success: General: Name: Deepinstinct3.0 Description: Yersion: 3.0 Publisher: Language: en Source files: Wervername\sharename\path Always obtain files from the source folder Success: Program Type: Standard Program Success: Program: Name: Deepinstinct3.0 Command line: Installer.exe mycompany.customers.deepinstinctweb.com Start in: Run mode: Run with administrative rights Program can run: Only when a user is logged on Drive mode: Runs with UNC name Success: Requirements: Platforms supported: Any Maximum allowed runtime(minutes): 120 To exit the wizard, click Close. 	× *
	< Previous Next > Summary	Close

10. Click **Close** and the Deep Instinct deployment package appears in the list of packages.

Folder Tools System Center Configuration Man	ager (Connecte	d to DIP - De	eepinstinct)							- 8 ×
Home Folder										^ 🔞
Create Package Import Package Trom Definition Create Searches - Searches -	ounts ontent File Program Package	➢ Export	Deploy Distribute Content Deploy	Update Distribution Point ment	ts Move	Set Security Scopes Classify	Properties Properties			
← → ▼ 🔄 \ → Software Library → Overview → Application	Management 🔸	Packages								- 2
Software Library <	Packages 5 items									
4 🗇 Overview	Search								🗙 🔎 Search	Add Criteria 🔻
🖌 🚞 Application Management	Icon Name			Programs	Manu	facturer	Version	Language	Package ID	
Applications	🛐 Configu	ration Manager	Client Package	0	Micro	soft Corpo			DIP00002	
Packages	🛐 User Sta	te Migration To	ol for Windows 8.1	0	Micro	soft Corpo	6.3.9600.17237		DIP00001	
Approval Requests	DLP			1	Force	Point		en	DIP00050	
[4] Global Conditions	DeepIns	tinct23		1			2.0	en	DIP00052	
App-V Virtual Environments Windows Sidebading Keys E Application Management Policies Gottware Updates Operating Systems	2.0.5.22	Create Pro Create Pro Export Refresh Delete	estaged Content File	F5 Delete	Deep	Instinct	2.0.5.22	en	DIP00051	
		Distribute	Content							
E Accets and Compliance	DeepInstinct2	👔 Update Di	istribution Points							*
	Package Propert	🔁 Move		5	tent Status			!	Related Objects	
Software Library	Package ID:	💩 Set Securi	ity Scopes				Success:	0	🐻 Content Status	E
Monitoring	Manufacturer: Version:	Propertie	5				Failed: 0	s: U		
Administration	Language:	e	n				Unknown:	0		
•	Summary Progra	ams Deployme	nts		0 Targeted	I (Last Update:	3/8/2017 2:43 AN	1)		*
Ready										
\Xi 占 🛛 🚔 🔍 🥥 🗈									- Ra 12 (2:44 AM 3/8/2017



Deploying the D-Client Installation Package

To deploy the package using SCCM:

- 1. Start Microsoft System Center Configuration Manager.
- 2. In the Configuration Manager console, click Software Library → Application Management → Packages. The list of packages appears.

Folder Tools System Center Configuration Man	ager (Connected	i to DIP - De	eepinstinct)							- 8 ×
Home Folder										^ 🔞
Create Package Import Package from Definition Saved Searches - Create Package Import Saved Searches - Searches -	ounts ontent File Program Package	 Export Refresh Delete 	Deploy Distribute Content Distribute Deploymen	Update ibution Points	Move Move	Set Securit Scopes Classify	Properties Properties			
← → ▼ 🔄 \ → Software Library → Overview → Application	Management 🕨 F	ackages								- 2
Software Library <	Packages 5 items									
4 😴 Overview	Search								🗙 👂 Search	Add Criteria 🔻
🔺 🚞 Application Management	Icon Name			Programs	Manu	facturer	Version	Language	Package ID	
Applications	Configura	ation Manager	Client Package	0	Micro	osoft Corpo			DIP00002	
Packages	🛐 User Stat	e Migration To	ol for Windows 8.1	0	Micro	osoft Corpo	6.3.9600.17237		DIP00001	
📝 Approval Requests	DLP			1	Force	Point		en	DIP00050	
Global Conditions	DeepInsti	net23		1			2.0	en	DIP00052	
App-V Virtual Environments Windows Sideloading Keys Application Management Policies Goftware Updates Goftware Updates	2.0.5.22	Create Pre Create Pre Create Pre Export Refresh Delete	acces Accounts estaged Content File ogram	F5 Delete	Deep	Instinct	2.0.5.22	en	DIP00051	
		Deploy								
ssets and Compliance	DeepInstinct2	Distribute Update Di	Content istribution Points							*
Cotheren Library	Package Propert	Move		nt.	ent Status				Related Objects	
Monitoring	Package ID: Manufacturer: Version: Language:	Set Securi Propertie	ity Scopes 15				Success: 0 In Progres Failed: 0 Unknown:) s: 0 0	🐻 Content Status	H.
	-	1-			0 Targeted	l (Last Update	: 3/8/2017 2:43 AN	1)		*
Ready	Summary Program	ns Deployme	nts							
									- Ra 12 (2:44 AM 3/8/2017

3. Right-click the Deep Instinct deployment package and click Deploy. The Deploy Software Wizard opens.



•		Deploy Software Wizard	×
General			
General	Specify general	information for this deployment	
Deployment Settings			
Scheduling			
User Experience	Software:	DeepInstinct3.0 (DeepInstinct3.0)	
Distribution Points	Collection:	Browse.	
Summary	Us <u>e</u> default distrib	ution point groups associated to this collection	
Progress			
Completion	 Automatically distr 	ibute content for dependencies	
	Comments (optional):		
	I		^
			~
		< <u>Previous</u> <u>Next</u> > <u>Summary</u> Can	ncel

4. Click **Browse**, select the Device Collection for deployment and click **OK**.



Device Collections	✓ Filter	Filter					
Root	Name All Desktop and Server Clients All Mobile Devices All Systems All Unknown Computers Deep_Full Deep_hase 1 Deployment Phase 1	Member Count 71 0 183 2 48 5 0					
	 Deployment_phase 1 Deployment_phase 1b DI_Uninstall Salesforce Test_uninstall Uninstall_1.5.30.0 Uninstall1.6.A20 	0 0 5 0 0 2					
	Stand Conning_Agent	U					

5. Click **Next**. Click **Add** + **Distribution Point** and select the distribution points for the content destination. This is typically the SCCM server.


٠		Deploy Software W	izard		x
Content					
General Content	Specify the cont	ent destination			
Deployment Settings					
Scheduling	Distribution points or di	stribution point groups that the	e content has been distributed to:		
User Experience					
Distribution Points	Name	Туре			
Summary		There are no	items to show in this view.		
Progress					
Completion					
	Additional distribution p	oints, distribution point groups	, and the distribution point groups that a	are currently associated	
	with collections to distr	ibute content to:			
	Filter			Add	•
	Name	Description	Associations		_
	SCCM.DEEP	Distribution point	1000000000	<u>R</u> emove	
		< <u>P</u> r	evious <u>N</u> ext > <u>S</u> um	mary Cancel	I

6. Click **Next** and make this a required installation, by selecting Required in the Purpose box.



•	Deploy Software Wizard	x
Deployment Set	ttings	
General Content Deployment Settings Scheduling	Specify settings to control how this software is deployed	
User Experience Distribution Points	Action: Install V Purpose: Required V	
Summary Progress Completion	Pre-deploy software to the user's primary device Sgnd wake-up packets Allow clients on a metered Internet connection to download content after the installation deadline, which might incur additional costs	
	< <u>P</u> revious <u>N</u> ext > <u>Summary</u>	Cancel

7. Click **Next** and the Scheduling dialog box opens.



+	Deploy Software Wizard
Scheduling	
General Content Deployment Settings Scheduling User Experience Distribution Points Summary Progress Completion	Specify the schedule for this deployment This program will be available as soon as it has been distributed to the content servers unless it is scheduled for a later time below. For required applications, specify the assignment schedule. Schedule when this deployment will become available: 2/15/2017 2/15/2017 4:43 AM 2/15/2017 4:43 AM UTC Assignment schedule: Oracle There are no items to show in this view.
	Rerun behavior: Always rerun program v
	< <u>P</u> revious <u>N</u> ext > <u>Summary</u> Cancel

- 8. Select Schedule when this deployment will become available.
- 9. Click **New** and the Assignment Schedule dialog box opens.

Assignment Schedule	x
O Assign to the following <u>s</u> chedule: Occurs on 2/15/2017 4:44 AM	
 Assign immediately after this <u>e</u>vent: 	Schedule
As soon as possible V	
ОК	Cancel

10. Select Assign immediately after this event and select As soon as possible from the dropdown box.



11. Click **OK** and 'As soon as possible' is added to the assignment schedule.

٠	Deploy Software Wizard	x
Scheduling		
General Content Deployment Settings Scheduling User Experience	Specify the schedule for this deployment This program will be available as soon as it has been distributed to the content servers unless it is scheduled for a later time below. For required applications, specify the assignment schedule.	
Distribution Points Summary Progress	 ✓ Schedule when this deployment will become available: 2/16/2017 □▼ 3:38 AM UTC 	
Completion	Schedule when this deployment will expire: 2/16/2017 3:38 AM Assignment schedule: New Edit	
	As soon as possible	
	Rerun behavior: Rerun if failed previous attempt v	
	< <u>P</u> revious <u>N</u> ext > <u>S</u> ummary Cancel	

12. Click **Next** and the **User Experience** dialog box opens.



*	Deploy Software Wizard	x
User Experience		
General Content Deployment Settings Scheduling <u>User Experience</u> Distribution Points Summary Progress Completion	Specify the user experience for the installation of this software on the selected devices Notification settings: Allow users to run the program independently of assignments When the scheduled assignment time is reached, allow the following activities to be performed outside the maintenance window: Software installation System restart (if required to complete the installation) Write filter handling for Windows Embedded devices Commit changes at deadline or during a maintenance winglow (requires restarts) If this option is not selected, content will be applied on the overlay and committed later.	
	< <u>P</u> revious <u>N</u> ext > <u>S</u> ummary Cancel	

13. Click **Next** and the **Distribution Points** dialog box opens.



•	Deploy Software Wizard X
Distribution Po	pints
General Content Deployment Settings Scheduling User Experience Distribution Points Summary Progress Completion	Specify how to run the content for this program according to the type of boundary the client is connected to Select the deployment option to use when a client is connected within a fast (LAN) network boundary. Deployment options: Download content from distribution point and run locally v Select the deployment option to use when a client is within a slow or unreliable network boundary, or when the client uses a fallback source location for content.
	Deployment options: Download content from distribution point and run locally ▼ Image: Allow clients to share content with other clients on the same subnet This option allows clients that use Windows BranchCache to download content from on-premises distribution points. Content downloads from cloud-based distribution points can always be shared by clients that use Windows BranchCache. Image: Allow clients to use a fallback source location for content
	< <u>P</u> revious <u>N</u> ext > <u>S</u> ummary Cancel

- 14. In both Deployment options lists, select Download content from distribution point and run locally .
- 15. Click **Next** and a summary of the deployment settings are displayed.



•	Deploy Software Wizard	x
Summary		
General Content Deployment Settings Scheduling	Confirm the settings for this new deployment	
User Experience Distribution Points Summary Progress Completion	General 9. Software: DeepInstinct3.0 (DeepInstinct3.0) 0. Collection: Deep_Full (Member count: 48) 1. Use default distribution point groups associated to this collection: Disabled 4. Automatically distribute content for dependencies: Disabled Deployment Settings 9. Action: Install 9. Purpose: Required 9. Pre-deploy software to the user's primary device: Disabled 9. Pre-deploy software to the user's primary device: Disabled 9. Allow clients to use a metered Internet connection to download content: Disabled Schedule when this deployment will become available: 3/8/2020 2:51 AM 9. Schedule when this deployment will expire: Disabled 9. Software installation: Disabled 9. System restart (if required to complete the installation): Disabled 9. System restart (if required to complete the installation): Disabled 9. Software installation: Disabled 9. System settings, click Previous. To apply the settings, click Next. Image: New Summary <	E T

16. Click **Next**. A progress bar and then a message appears to indicate that the wizard completed successfully.





17. Click Close .

4.2.2.2. D-Client Deployment with GPO

Group Policy Management Console (GPMC) is a Microsoft management tool that can create a Group Policy Object (GPO) to deploy D-Clients on all your organization's Windows devices.

The D-Client deployment process using GPO requires the following:

- Deep Instinct Windows EXE installation file. The file may be downloaded from the Windows Deployment Resources screen.
- Determine the installation CLI command to run with GPO.
- Installation batch file for GPO
- Deployment using GPO



Create an installation Batch File

Before you can deploy the D-Client with GPO, you need to create an installation batch file. You can create the batch file with a text editor (such as Notepad).

To create the installation batch file:

- 1. Download the installation file from the Windows Deployment Resources screen.
- 2. Save the installation file to a location where all the Windows devices have access.
- 3. Open the text editor.
- 4. Type the CLI command with all required options and values in the Command line. For details on how to define the CLI command, see Windows D-Client CLI Command.
- 5. Save the file with the name installer.bat.

Example 1. Example:		
For the following values		
installer.bat - Notepad		×
File Edit Format View Help <pre>\\tgdc1\company\Installer.exe customer.deepinstinctweb.com /token</pre>	123456	78
<		>
Where:		
<pre>exe path = \\tgc1\company\</pre>		
installation file = Installer.exe		
<pre>server address = customer.deepinstinctweb.com</pre>		
 installation token = 12345678 		

6. Copy the batch file to the same location the installation file was saved and to the location where the Windows deployment tool has access.

Deploying D-Clients using GPO

To deploy D-Clients using GPO:

1. Download the installation file from the Windows Deployment Resources.

deep instinct

- 2. Create the installation batch file.
- 3. Save the installation batch file to the Startup Script folder.
- 4. Save the EXE and batch files to a location where all the organization's Windows devices have access.
- 5. Log on to the Domain Controller (DC) and start the Microsoft Group Policy Management Console (GPMC).
- 6. In the GPMC tree, right-click the Organization Unit (OU) to which you want to deploy the D-Client and click Create a GPO in this domain, and Link it here to create a new GPO. The New GPO dialog box opens.

New GPO			×
Name:			
New Group Policy Object			
Source Starter GPO:	R		
(none)			•
		ОК	Cancel

- 7. Type the name of the new GPO and click **OK**. The new GPO is now added to the list of Linked Group Policy Objects.
- 8. Right-click on the new GPO and click Edit.
- 9. In the GPMC tree, expand Policies+Windows Settings.
- 10. Click Scripts (Startup/Shutdown) and double-click Startup. The **Startup Properties** dialog box opens.





Sta	artup Properties	? X
Scripts PowerShell Scripts		
Startup Scripts for	or DI deploy	
Name	Parameters	
		Up
		Down
		Add
		Edit
		Remove
To view the script files stored the button below.	f in this Group Policy Object, p	ress
	OK Cancel	Apply

- 11. Click **Add** and the **Add a Script** dialog box opens.
- 12. Click **Browse** and select the installation batch file.

Add a Script	X
Script Name:	
installer.bat	Browse
Script Parameters:	
ОК	Cancel

- 13. Click **OK** to add the script.
- 14. Click **OK** and exit the Microsoft Group Policy Management Console. The D-Client is deployed on each device when the device restarts.



To install the D-Client immediately from a device, perform the procedure described in Apply GPO to Deploy D-Client Manually.

Apply GPO to Deploy D-Client Manually

After a GPO has been created to deploy the D-Client, the D-Client is deployed on each device when the device restarts. If you want the D-Client to be deployed immediately on a device, perform the following procedure on the device.

To manually apply the GPO to deploy D-Client:

- 1. Open the Command Prompt window.
- 2. At the command prompt, type <code>gpupdate /force</code>. The Command Prompt window indicates that the policy updated successfully.



3. Type Y to restart the device and complete the D-Client deployment on this device.

4.2.3. Local Deployment of Windows D-Client

4.2.3.1. Local deployment using the installation CLI command

The D-Client can also be installed on each Windows device using a CLI command. This may be practical when only a few devices need to be installed or for devices that are not managed by the Active Directory.

To install D-Client on a Windows device:

- 1. Download the installation file from the Windows Deployment Resources screen.
- 2. Save the installation file to a location where the Windows device has access.
- 3. Open the Command Prompt window as an administrator.



4. At the command prompt, type the CLI command with all required options and values in the Command line. For details on how to define the CLI command, see Windows D-Client CLI Command.

Example 2. Example

For the following values:

- exe path = c:\users\administrator\downloads\
- installation file = Installer.exe
- server address = customer.deepinstinctweb.com
- Installation token = 12345678

The CLI command appears like this:

```
C:\Windows\system32> c:\users\administrator\downloads\Installer.exe
customer.deepinstinctweb.com /token 12345678
```

4.2.3.2. Local deployment using the Installation screen

The D-Client can also be installed on each Windows device using the Installation screen and then monitored using the D-Client Console. This may be practical when only a few devices need to be installed or for devices that are not managed by the Active Directory.

To install D-Client on a Windows device:

- 1. Download the installation file from the Windows Deployment Resources screen.
- 2. Save the installation file to a location where the Windows device has access.
- 3. Run the installation file. A message appears to confirm.





4. Click Yes to open the D-Client Installation screen.

deep Instinct	Installation		×
Management server address		Management server address	
Installation token		Installation token	
Device tag (optional)		Device tag	
		Install	

- 5. Enter the FQDN for the management server.
- 6. Enter the ID of the installation token, as displayed in the Windows Deployment Resources screen.
- 7. As an option, enter a tag associated with the deployed device. The Device Tag must comply to the following:
 - Maximum length is 256 characters



- Device Tags are case sensitive
- Allowable characters:
 - Letters (a-z, A-Z)
 - Numbers (0-9)
 - Spaces representable in UTF-8
 - Special characters: + = . _ : / @

Device tags can be used with rules to automatically add devices to a Device Group. It can also be used for selecting and filtering devices in the Management Console. For more information, see the Administrator Guide.

- 8. Click **Install** to install the D-Client.
- 9. To determine whether the D-Client installation is in process, look at the D-Client icon in the notification area, at the far right of the taskbar. If the icon appears with a gray indicator \mathbb{N} , the installation is in process.
- 10. To monitor the progress of the installation , you can open the D-Client Console by rightclicking the icon and selecting Show Console.





4.2.4. D-Client installation for Windows VDI

The Windows D-Client can operate in VDI environments.

4.2.4.1. Operating in VM based VDI environments

In VM based VDI environments the Windows D-Client is installed on the Master-template which is used to launch the actual VDI machines (VMs). The launched VMs include a pre-configured DI-Client that fully protects the VM using the assigned policy.



NOTE

Deep Instinct conducts regular testing of the Windows D-Client on VMWare Horizon's Virtual Desktop Infrastructure.

The Windows D-Client can operate in both Persistent and Non-Persistent VDI environments, keeping in mind that once the VDI is up and running it performs a re-registration against the Management Console and a new Device is created in the system. You can manage and monitor the new device as you would any other device.



Using the /vdi flag from VM based VDI

The /vdi flag ensures that the D-Client properly operates on any new VM that is launched by performing the following:

- 1. The D-Client is installed on the Master-template with the /vdi flag (refer to "D-Client installation in a VDI environment" for additional details).
- 2. The installation on the Master-template performs a full installation and activation of the D- Client, including:
 - a. Registration of the D-Client.
 - b. Download the policy.
 - c. Perform a full scan.
 - d. Unregister the D-Client at the end of the process.

The Windows D-Client is now ready to re-register at the next restart. Once the VDI orchestration launches a new VDI from the Master-template, it re-registers upon the restart of the VM. Then, it downloads the policy and is activated.



NOTE

Instant-clone technology does not utilize a restart process, which can cause a disruption to the operation of the D-Client.

4.2.4.2. Operating in an SBC/Multi-session based VDI environment

In installations in an SBC/Multi-session based VDI environment, the Windows D-Client is installed on the Windows server — protecting the server itself. However, the virtual desktop machines, running as part of the SBC implementation, are transparent to the D-Client and therefore may not fully benefit from its protection capabilities (e.g., prevention and end-user notifications). This should be considered when installing in this type of environment. deep instinct



4.2.4.3. D-Client installation in a VDI environment

To install D-Client on a VDI machine:

- 1. Install Windows on the master image. You can use any of the supported Windows operating systems listed in the Client System Requirements.
- 2. Install the Windows updates you want. Deep Instinct recommends that you install all security updates by Microsoft. However, the security updates from KB2813430 are required.
- 3. Reboot to ensure all updates are properly installed and initialized.
- 4. Install all other applications, and application updates you want on the image and then reboot. Installing the D-Client should be one of the last actions you do prior to finalizing the master image.
- 5. Install the D-Client using the CLI command on the master image, as follows:
 - a. Download the installation file from the Windows Deployment Resources screen.
 - b. Save the installation file to a location where the Windows virtual machine has access.
 - c. Open the Command Prompt window as an administrator from the virtual machine.
 - d. At the command prompt for installing the D-Client, type the following command:<exe
 path><installation file><server address>/token <installation token>/vdi [/tag <tag>] [/disabled] [/nfs] [/np | /manualproxy <proxy
 url>:<proxy port>]

Where:

• exe path – Path for the appropriate installation file



- installation file file name for the appropriate installation file. To enter the file name, click **Browse** and select the file from the folder.
- server address FQDN for the D-Appliance.installation token This is the ID of the installation token, as displayed in the Windows Deployment Resources screen. When installing in a system with MSP support, each tenant has a different installation token ID. Therefore, each tenant requires a different master image.
- tag This is optional. Adds a tag associated with the deployed devices. Use quotation marks to enter values with spaces or special characters. The Device Tag must comply to the following:
 - Maximum length is 256 characters.
 - Device Tags are case sensitive.
 - Allowable characters:
 - Letters (a-z, A-Z)
 - Numbers (0-9)
 - Spaces representable in UTF-8
 - Special characters: + = . _ : / @

Device tags can be used with rules to automatically add devices to a Device Group. It can also be used for selecting and filtering devices in the Management Console. For more information, see the Administrator Guide.

- /disabled This is optional. When /disabled is included, the D-Client is disabled during the installation. This allows the administrator to select when to initially enable the D-Client.
- /nfs This is optional. Starts the D-Client without performing the initial full scan.
- /np This is optional and cannot be used with /manualproxy. Enables the use of a network proxy server using the default proxy settings.
- /manualproxy- This is optional and only available for D-Client version 2.5.1 or later. Enables the use of a network proxy server, using the specified settings of the proxy server URL and port number. Do not use with /np.
- proxy url URL for the proxy server, including the scheme
- proxy port port number to access the proxy server
- e. The following is an example of the command, where:



- exe path = c:\users\administrator\downloads\
- installation file = Installer.exe
- server address = customer.deepinstinctweb.com
- installation token = 12345678

The CLI command is as follows:

```
C:\users\administrator\downloads\Installer.exe
```

```
customer.deepinstinctweb.com /token 12345678 /vdi
```

- f. This installation performs specific action that also include unique actions for VDI installations, as follows:
 - Uses a random registration code that is unique for each registration (clones of this machine will receive a new Device ID)
 - Download the configuration file
 - Performs a full scan (unless the /nfs option was used)
 - Once the above is completed:
 - Device ID is removed (this allows regeneration when the clone machines are spun up)
 - Network service is disabled (this prevents re-registration)
 - Network queues are emptied
- 6. After the full scan is completed and all that you want is included in the master image, run Sysprep as follows:
 - a. Open the Command Prompt window, as an administrator from the virtual machine.
 - b. Run Sysprep. At the command prompt, type the following command:

C:\Windows\System32\Sysprep\sysprep

c. The System Preparation Tool window opens.



System Preparation Tool 3.14		
System Preparation Tool (Sysprep) prepares the machine for hardware independence and cleanup.		
System Cleanup Action		
Enter System Out-of-Box Experience (OOBE) 🛛 🗸		
Generalize		
Shutdown Options	-17	
Shutdown 🗸		
OK Cancel		

- d. Select Enter System Out-Of-Box Experience (OOBE) from the dropdown box for the system cleanup action and then select Generalize.
- e. Select Shutdown from the dropdown box.
- f. Click **OK** to generalize the machine and shut everything down to make the master image.



Once completed, do not use the master image. Clone the machine to prevent the services for Deep Instinct do not start again and communicate to the server. This ensures that a new SID (System ID) is generated each time a machine is cloned from the template, and no duplicates appear in the Management Console.

4.2.5. Installation error codes

Once the installation process is completed, the D-Client for each device provides an Installation Error Code (Exit Code) that can be read by the Windows deployment tool. The codes are as follows:

Code	Description	Comments	Agent enum
0	Success	N/C	Success_OperationDone = 0
1	No connection to management server	Could be incor- rect server URL or network issue	Failed_ManagementServerDoes- NotExist = 1



Code	Description	Comments	Agent enum
2	Invalid command line token	CLI token not accepted by the management server	Failed_InstallationTokenIsInvalid = 2
3	Unknown error	Usually some ex- ception	Failed_UnknownReason = 3
4	Bad parameters in command line	N/C	Failed_UnexpectedParameters = 4
5	Not In use	N/C	Failed_NotEnoughParameters = 5
6	Empty token in com- mand line	N/C	Failed_InstallationTokenIsEmpty = 6
7	Missing external API GUID	N/C	Failed_ExternalApiGuidIsEmpty = 7
8	Invalid external API GUID	N/C	Failed_ExternalApiGuidIsInvalid = 8

4.3. Deployment to macOS Devices

To deploy on macOS devices, perform the following steps:

- 1. Configure Deep Instinct's General Configuration and macOS policies. For more information, see the Administrator Guide.
- 2. If your macOS devices have antivirus software installed, add Deep Instinct's objects to your antivirus's Exclusion list.
- 3. Download the relevant D-Client installation DMG file from the macOS Deployment Resources screen.
- 4. Install the macOS D-Client by using the downloaded installation DMG file. Installation can be performed remotely using a macOS deployment tool or directly from the devices. For more information, see macOS D-Client Installation.

4.3.1. macOS D-Client deployment

The deployment of D-Clients on macOS devices can be performed remotely using a macOS deployment tool or directly from the devices. Deep Instinct supports the following deployment methods:

Remote deployment using a macOS Deployment Tool

Remote deployment using Jamf

Local deployment using the Installation CLI command

Local deployment using the Installation Wizard

4.3.1.1. Remote deployment with a macOS deployment tool

A macOS deployment tool can be used to deploy D-Clients on all your organization's macOS devices. To deploy using a macOS deployment tool, the following is required:

- Deep Instinct installation DMG file. The file may be downloaded from the macOS Deployment Resources screen.
- Deploy the D-Client with the macOS deployment tool using the downloaded macOS installation file.
- To protect your device, the D-Client on your device needs specific permissions to monitor, protect and notify you against threats. Three main types of permissions are required:
 - 1. System Extension Installation Permissions:
 - Endpoint Security Extension (DeepInstinctUtility)
 - Network Extension (DeepInstinctUtility)
 - 2. Full Disk Access Permission for the following processes:
 - DeepInstinctExtension
 - DeepInstinctClassifier
 - DeepInstinctRansomSVC
 - 3. Network Content Filtering Permission:
 - DeepInstinctUtility

4.3.1.2. D-Client deployment with Jamf

Jamf is a management tool that can deploy D-Clients on all your organization's macOS devices. The following procedure is based on using Jamf Pro 10.34.2.

The D-Client deployment process using Jamf requires the following:

- Enroll all computers into Jamf to which you want to deploy macOS D-Client
- Acquire the Deep Instinct DMG installation file, which can be downloaded from the macOS Deployment Resources screen.
- Create a Configuration Profile to enable the required macOS permissions

deep instinct

- Create a Jamf script to define the action that is performed during deployment
- Create a Jamf package
- Create a Jamf Policy for D-Client Deployment

Creating a Jamf configuration profile

The Jamf Configuration Profile is used to define and enable the required macOS permissions.

Jamf Configuration Profile prerequsites

- Create a Jamf Profile
- Add Full Disk Access Permission
- Add System Extension Permission
- Allow the removal of Extension Permission
- Add Content Filter Permission
- Define the scope to which computers the profile is deployed

To create a Jamf Configuration Profile:

1. Start Jamf Pro.





2. In the left pane, click Computers \rightarrow Configuration Profiles.



••• • • < >	I dimacdev.jamfcloud.com	c 🖞 + 🖽
🗖 jamf PRO		요 \$ 尊
Computers Devices Users	Computers Configuration Profiles	
	✓ Q. Filter Pr. 0 - 0 of 0	+ New DUpload
Search Inventory	NAME LOGS COMPLET	PENDING FAILED SCOPE
Licensed Software	No data available in table	
CONTENT MANAGEMENT		
Policies		
ಂfiguration Profiles (양) Configuration Profiles		
Restricted Software		
\Lambda Mac Apps		
🔂 Patch Management		
eBooks		
GROUPS		
Smart Computer Groups		
Collapse Menu		

3. Click **New**, and type **DeepInstinct** as the name of the profile.



••• • • < >	D 🔒 dimacdev	.jamfcloud.com C 🖞 + 🔡	
🗖 jamf PRO		ይ 4 🕸	
Computers Devices Users	Computers : Configuration Profile: ← New macOS Configu	iration Profile	
INVENTORY	Options Scope		
Search Inventory Search Volume Content Licensed Software	@ General	General Name Display name of the profile	
CONTENT MANAGEMENT	Passcode Not configured	DeepInstinct Description Brief explanation of the content or purpose of the profile	
Configuration Profiles	Retwork Not configured		
Mac Apps Patch Management	VPN Not configured	Category Category to add the profile to	
GROUPS	DNS Settings Not configured	Level Level at which to apply the profile	
Collapse Menu	DNS Proxy Not configured	Computer Lever V S Cancel Sav	

- 4. Configure the first Full Disk Access Permission, as follows:
 - a. From the left of the New macOS Configuration Profile panel, scroll down and click Privacy Preferences Policy Control.





b. Click **Configure**.





- c. Enter the identifier. Type or copy the following: /Library/DeepInstinct/Executables/DeepInstinctClassifier
- d. Set the identifier type to Path.
- e. Enter the code requirement. Type or copy the following:

```
identifier DeepInstinctClassifier and anchor apple generic and cer-
tificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certif-
icate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and cer-
tificate leaf[subject.OU] = MV9BR98H24
```

- f. Click **Add** to add an Apple service.
- g. Select the SystemPolicyAllFiles service and set the access to Allow.
- h. Click **Save** to save the Apple service and then click **Save** to save the Configuration Profile.
- 5. Configure the second Full Disk Access Permission, as follows:
 - a. Click **Edit**, and then click ⁺ for App Access.
 - b. Scroll down to the new App Access entry.





- c. Enter the identifier. Type or copy the following: /Library/DeepInstinct/Executables/DeepInstinctRansomSvc
- d. Set the identifier type to Path.
- e. Enter the code requirement. Type or copy the following: identifier Deep-InstinctRansomSvc and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = MV9BR98H24
- f. Click **Add** to add an Apple service.
- g. Select the **SystemPolicyAllFiles** service and set the access to **Allow**.
- h. **Save** the Apple service and then **Save** the Configuration Profile.
- 6. Configure the third Full Disk Access Permission, as follows:
 - a. Click **Edit**, and then click ⁺ for App Access.
 - b. Scroll down to the new App Access entry.



- c. Enter the identifier. Type or copy the following: com.deepinstinct.DeepInstinctUtility.Extension
- d. Set the identifier type to **Bundle ID**.
- e. Enter the code requirement. Type or copy the following: identifier "com.deepinstinct.DeepInstinctUtility.Extension" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = MV9BR98H24
- f. Click **Add** to add an Apple service.
- g. Select the **SystemPolicyAllFiles** service and set the access to **Allow**.
- h. **Save** the Apple service and then **Save** the Configuration Profile.
- 7. Configure the System Extension Permission, as follows:
 - a. Scroll down and click System Extensions.





b. Click **Configure**.





- c. Type "DeepInstinct" as the Display Name.
- d. Select Allowed System Extensions for the System Extension Types.
- e. Enter the Team Identifier. Type or copy the following: MV9BR98H24
- f. Click Add and enter the first System Extension. Type or copy the following: com.deepinstinct.DeepInstinctUtility.Extension
- g. Save the System Extension. Then click Add to add another System Extension.
- h. Enter the second System Extension. Type or copy the following: com.deepinstinct.DeepInstinctUtility.NetworkExtension
- 8. Continue to configure the System Extension Permission to allow the removal of system extensions during upgrades, as follows:
 - a. Click ^t for Allowed Teams IDs and System Extensions.
 - b. Scroll down to the new Allowed Teams IDs and System Extensions entry.





- c. Type **DeepInstinct Extensions Removal** as the Display Name.
- d. Select Removable System Extensions for the System Extension Types.
- e. Enter the Team Identifier. Type or copy the following: MV9BR98H24.
- f. Click Add and enter the first System Extension. Type or copy the following: com.deepinstinct.DeepInstinctUtility.Extension
- g. Save the System Extension. Then click Add to add another System Extension.
- h. Enter the second System Extension. Type or copy the following: com.deepinstinct.DeepInstinctUtility.NetworkExtension
- i. **Save** the System Extensions.
- 9. Configure the Content Filter Permission, as follows:
 - a. Click Content Filter.





- b. Type **Deep Instinct** as the Filter Name.
- c. Enter the Identifier. Type or copy the following: com.deepinstinct.DeepInstinctUtility
- d. Scroll down to Filter Order.





- e. Select Firewall for the Filter Order. Verify that Filter Order is enabled by the blue toggle.
- f. Enter the Socket Filter Bundle Identifier. Type or copy the following: com.deepinstinct.DeepInstinctUtility.NetworkExtension
- g. Enter the Socket Filter Designated Requirement. Type or copy the following: identifier "com.deepinstinct.DeepInstinctUtility.NetworkExtension" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = MV9BR98H24

```
Enter the Socket Filter Designated Requirement. Type or copy
the following: identifier "com.deepinstinct.DeepInstinctUtility.Net-
workExtension" and anchor apple generic and certificate
1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate
leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate
leaf[subject.OU] = MV9BR98H24
```

h. Click Save


Deployment and installation



10. Set the scope to define to which computers this profile is deployed, as follows:

- a. Click Edit + Scope.
- b. Click **Edit** to edit the scope.



••• • • < >	C 🔒 dimacdev.ja	amfcloud.com	① + 器
🗖 jamf 🛛 PRO			<u>ᡗ</u> 4 ‡
Computers Devices Users	Computers : Configuration Profiles ← DeepInstinct		
INVENTORY	Options Scope		
Search Volume Content	Targets	Limitations	Exclusions
CONTENT MANAGEMENT	Target Computers Computers to assign the profile to	Target Users Users to distribute the profile to	
Configuration Profiles	All Computers 🔹	All Users 🔹	
Mac Apps			
 Patch Management eBooks 			
GROUPS			
Collapse Menu			Cancel Save

- c. To deploy this profile to all macOS devices managed by Jamf, set Target Computers to All Computers and set Target Users to All Users.
- d. Click Save.

Create a Jamf script

The Jamf Package requires a script to define the action that is performed during deployment of the macOS D-Client. Before you create a Jamf Package, we recommend preparing a Jamf Script since it needs to be included in the Jamf Package.

To create the Jamf Script:

- 1. Open a text editor.
- 2. For the first three lines, type the following:

```
#!/bin/sh
## postinstall
hdiutil attach -nobrowse /private/tmp/DeepInstinct.dmg
```

3. The forth line is the CLI Installation command. Type the following: sudo sh /Volumes/Deep\ Instinct/installer.sh <server address>-token <installation token> [-tag <tag>] [-disabled] [-nfs]

Where:

Command El- ement	Description	Comment
<server address></server 	FQDN for the Manage- ment Server (D-Appli- ance)	N/C
<installa- tion to- ken></installa- 	ID of the installation token as displayed in the macOS De- ployment Resources screen	N/C
<tag></tag>	Adds a tag associated with the deployed de- vices	 Optional Use quotation marks to enter values with spaces or special characters The Device Tag must comply to the following: Maximum length is 256 characters Case sensitive Valid characters: Letters (a-z, A-Z) Numbers (0-9) Spaces representable in UTF-8 Special characters: + - = : / @ Device tags can be used with rules to automatically add devices to a Device Group. It can also be used for selecting and filtering devices in the Management Console. For more information, see the Administrator Guide.



Command El- ement	Description	Comment
-disabled	D-Client is disabled during the installation when this is included in the command. This al- lows the administrator to select when to ini- tially enable the D-Cli- ent.	Optional
-nfs	Starts the D-Client without performing the initial full scan.	Optional

4. For the last four lines, type the following:

hdiutil unmount /Volumes/Deep\ Instinct/

#delete file

rm -rf /private/tmp/DeepInstinct.dmg

exit 0 ## Success

Example of a Jamf script

For the following values:

<server address> = customer.deepinstinctweb.com

<installation token> = 12345678

The Jamf script would be:





5. Save this file, as the content of this file can be copied to the Jamf Package when you create the package, as detailed in Creating a Jamf Package for D-Client Deployment.

Creating a Jamf package for D-Client deployment

The Jamf Package with the Jamf Script defines the actions that are performed on a macOS device during deployment.

To create a Jamf package for deployment:

- 1. Download the installation file from the macOS Deployment Resources screen.
- 2. Save the installation DMG file to the folder /private/tmp.
- 3. Create the Jamf Script, as described in Create a Jamf Script.



Monitoring Installation	0		
Snapshot	-10		0
🛓 Operating System	Nous 9 Modified	Monitor File	Normal Chanabat
Build OS Package	Snapshot	System Changes	Normai Snapshot
🍄 Package Manifests		.,	
> Pre-Installed Software User Environment			
	Take a sn will be ta snapshot	apshot that watches f ken before and after th s will be compared.	or any new files on the boot drive. A since installation process, and then the tw

- 4. Start Jamf Composer to create a new package.
- 5. Select Normal Snapshot and click **Next**.



Choose a name f	or your package:		
Choose a name f	or your package:	Previous Next	

6. Type **DeepInstinct** as the name of the package, and click **Next**. A progress bar is displayed to indicate the progress of the Before Snapshot.



Deployment and installation

	7.2	New	Build as DMG	Build as PKG	Search
OURCES eepInstinct					
ACKAGES					
		Pe	rform you	r Installati	on
		Whe	II and configure n you are done,	your software. click Create Paci	kage Source below.
	Cancel				Create Package Source

7. Click **Next**, and a progress bar is displayed to indicate the progress of the After Snapshot. Once completed, an icon to the left of DeepInstinct Source in Composer is displayed.



• • • Composer 10.34.2	New	Build as DMG	Build as PKG	Q Search	Search
SOURCES					
PACKAGES					
		_			
				0	
N					•••

8. Drag the installation DMG file from folder /private/tmp to Composer.





🗧 🗧 🗧 Comp	oser 10.34.2	New	Ruild as DMG	Ruild as PKG	Q Search	Search	
SOURCES	> private		build us billo	build up rive			
	priva	té	Owner: Group: Everyone:	root (0) wheel (0)	0	R W X ✓ ✓ ✓ ✓ ■ ✓ Mode: 755	Θ

- 9. Apply the Directory Permissions to the installation DMG file. Click on the bottom-right of the screen and select Apply Permissions to private and All Enclosed Items.
- 10. Add a Shell Script :
 - a. From the Navigation Panel, expand DeepInstinct and right-click Scripts.
 - b. Select Add Shell Script → Postinstall.
 - c. Select DeepInstinct \rightarrow Scripts \rightarrow Postinstall.
 - d. Delete the script content and enter the script as defined in Create a Jamf Script.



- 11. Save the Jamf package:
 - a. Click **DeepInstinct** from the Navigation Panel.
 - b. Click the Build as PKG icon ጆ on the top of the screen.
 - c. Select **Desktop** as the location and click **Save**.

Creating a Jamf policy for D-Client deployment

The Jamf Policy is used to define the triggering method to deploy the D-Client and to which computers. To create a Jamf Policy, you need to perform the following:

- **Configure Jamf Console**
- Upload Jamf Package
- Create a new Jamf Policy
- Configure the policy
- Define the scope for deployment

To create a Jamf policy for deployment:



1. Start Jamf Pro.



- 2. Click an the top-right of the screen.
- 3. Click Server Infrastructure \rightarrow Cloud Distribution Point.
- 4. From the Cloud Distribution Point panel, set the Content Delivery Network to **Jamf Cloud**.



Deployment and installation

••• • • <	>	0	a dimacdev.jamfcloud	.com d		ŵ + 8
🗖 jamf 🛛 PRO						ይ 4 ф
Computers Devices	لک) Users	Settings : Server Infra ← Cloud Distri	structure bution Point			
VERSION 10.39.1-t1656084637 MANAGED Computers: 0 Mobile Devices: 0		Content Delivery Network Jamf Cloud Use as prind Use as the au	Content delivery netwo The second s	rk to use for the distribution	on point	
UNMANAGED Computers: 0		USAGE PERIOD	FILES UPLOADED	DATA UPLOADED	FILES DOWNLOADED	DATA DOWNLOADEI
Mobile Devices: 1		Last 30 Days	4	151.7 MB	0	0 B
		Last 12 Months	4	151.7 MB	0	0 B
		Usage updated h	ourly. Last update: 202	2-06-27 10:37:43 UTC		
		Pac	kages	In-House Apps		eBooks
🕒 Collapse Menu					Histo) 🥥 🗹 Dry Test Edit

- 5. Upload the DeepInstinct Package, as follows:
 - a. Click 🔯 on the top-right of the screen.
 - b. Click Computer Management \rightarrow Packages.
 - c. From the New Packages panel, click **New**.





- d. Click **Choose File** for the Filename.
- e. Select **DeepInstinct.pkg** from the Desktop, and click **Upload**. The Display Name changes to **DeepInstinct.pkg**.





- f. Click Save .
- 6. Once the package is uploaded, create a new policy:
 - a. In the left pane, click Computers \rightarrow Policies. The Policies panel opens.



Deployment and installation

••• • • < >		① + 器
🗖 jamf 🛛 PRO		<u>}</u> 4 ‡
Computers Devices Users	Computers Policies	
INVENTORY	C Filter Pc 1-1 of 1	+ New 🗄 🔠
 Search Inventory Search Volume Content 	NAME ^ FREQUENCY	TRIGGER SCOPE
Licensed Software CONTENT MANAGEMENT	 No category assigned 	
Policies	Update Inventory Once every week	Check-in All computers
Restricted Software		
 Patch Management eBooks 		
GROUPS		
Collapse Menu	▲ 1 ▼ ▶ Show: 100 ▼	

b. From the Policies panel, click New.





- c. Type **DeepInstinct** as the Display Name of the policy.
- d. Set the Trigger to define the events that will initiate the policy. Suggested triggers:
 - Enrollment Complete Policy is initiated immediately after the enrollment process.
 - **Custom** Define the Custom Event as **di**. Policy can be manually initiated using **di**.
- e. Set Execution Frequency to **Ongoing**.
- 7. Add the DeepInstinct Package to the policy, as follows:
 - a. Click Packages and then click Configure. The Packages panel opens.





- b. Click **Add**, to add the Deepinstinct.pkg to the policy.
- 8. Set the scope to define to which computers this policy is deployed, as follows:
 - a. Click Scope.



••• • • < >	C dimacdev.ja	amfcloud.com	① + 器
🗖 jamf 🛛 PRO			L 4 @
Computers Devices Users	Computers : Policies ← New Policy		
	Options Scope Self Servi	ce User Interaction	
Search Volume Content	Targets	Limitations	Exclusions
CONTENT MANAGEMENT	Target Computers Computers to deploy the policy to	Target Users Users to deploy the policy to	
 Configuration Profiles Restricted Software 	All Computers 👻	All Users 👻	
A Mac Apps			
eBooks groups			
Collapse Menu			Cancel Save

- b. To deploy the D-Client to all macOS devices managed by Jamf, set Target Computers to All Computers and set Target Users to All Users.
- c. Click Save.

4.3.1.3. D-Client local installation with the CLI

The D-Client can also be installed on each macOS device using a CLI command. To install macOS D-Client, you need to sign in as an administrator user.

To install D-Client on a macOS device:

- 1. Download the installation file from the macOS Deployment Resources screen.
- 2. Save the installation DMG file to a location where the macOS devices has access.
- 3. Open a Terminal window.
- 4. Mount the DMG installation file. At the command prompt, type the following command:

open <path><DMG installation file>

Where:

• <path> — path for the installation file



- <DMG installation file> file name for the downloaded installation DMG file
- 5. Run the installation file. At the command prompt, type the following command for installing the D-Client on a macOS device:

sudo "/Volumes/Deep Instinct/installer.sh" <server address>-token <installation token> [-tag <tag>] [-disabled] [-nfs]

For installing the D-Client on a VDI machine:

sudo "/Volumes/Deep Instinct/installer.sh" <server address>

-token <installation token> -vdi [-tag <tag>] [-disabled]

Where:



Command El- ement	Description	Comments
<server address></server 	FQDN for the Management Server (D-Appliance)	N/C
<installa- tion to- ken></installa- 	ID of the installation token, as displayed in the macOS Deploy- ment Resources screen	N/C
<tag></tag>	Adds a tag associated with the deployed devices	 Optional Use quotation marks to enter values with spaces or special characters Maximum length is 256 characters Case sensitive Valid characters: Letters (a-z, A-Z) Numbers (0-9) Spaces representable in UTF-8 Special characters: + - = : / @ Device tags can be used with rules to automatically add devices to a Device Group. It can also be used for selecting and filtering devices in the Management Console. For more information, see the Administrator Guide.
-disabled	When included in the command the D-Client is disabled during the installation. This allows the administrator to select when to initially enable the D-Client.	Optional

Command El- ement	Description	Comments
-nfs	Starts the D-Client without per- forming the initial full scan	Optional
-vdi	Required when installing the D- Client on a VDI machine	N/C

Example 3. Installation on VDI command

For the following values:

- path = /Users/user/Downloads/
- installation file = 2.4.0.1_DeepInstinct_installer.dmg
- server address = customer.deepinstinctweb.com
- installation token = 12345678

The commands will look like this:

- Macbook-Pro:Desktop user\$ open /Users/user/Downloads/2.4.0.1_DeepInstinct_installer.dmg
- Macbook-Pro:Desktop user\$ sudo "/Volumes/Deep Instinct/installer.sh"customer.deepinstinctweb.com -token 12345678
- Password: Macbook-Pro:Desktop user\$

During the installation of the D-Client, specific permissions must be enabled to protect your device. The required permissions vary based on the operating system on your device.

The Deep Instinct extensions must be allowed to load. If permissions are required, the System Extension Blocked message opens and perform the following:





Click Open Security Preferences and the Security & Privacy screen opens.



• • < > IIII Security & Privacy	Search
General FileVault Firewall Privacy	
A login password has been set for this user Change Password	
🗹 Require password 5 minutes 📀 after sleep or screen saver l	begins
Show a message when the screen is locked Set Lock Message	
 Disable automatic login 	
Allow apps downloaded from:	
App Store	
App Store and identified developers	
Some system software requires your attention before it can be used	Details
Click the lock to make changes	Advanced 2
	Auvanceu

Click the Lock icon at the bottom left corner of the screen. A dialog box opens for you to enter your administrator credentials.

System Preferences is trying to unlock Security & Privacy preferences. Enter your password to allow this.	
User Name:	
Cancel Unlock	

Enter the administrator's username and password.

Click Unlock to unlock the Security & Privacy screen.

Click Details to continue.



System software from the following developers was updated and the system needs to be restarted before it can be used.	
✓ DeepInstinctUtility	
✓ DeepInstinctUtility	
Canad	

Select all instances of "DeepInstinctUtility" and click OK to permit Deep Instinct to load the required system extensions.

Deep Instinct may need to perform network filtering. If permission is required, the Filter Network Content message opens and click Allow.

"DeepInstinctUt	ility" Would Like
to Filter Netw	work Content
All network activity	on this Mac may be
filtered or	monitored.
Allow	Don't Allow

For Full Disk Access Permission, perform the following:



	Security & Privacy	Q Search
	General FileVault Firewall	Privacy
Speech Recogni	tion Allow the apps belo	ow to access data like Mail,
Accessibility	Messages, Safari, H certain administrat Mac.	Home, Time Machine backups, and ive settings for all users on this
Input Monitoring	I	
Full Disk Access	Deeplr	nstinctClassifier
Files and Folders	s 🔽 🔀 Deeplr	nstinctRansomSvc
Screen Recordin	ig 🔽 🔀 Deeplr	nstinctExtension
Media & Apple N	<i>A</i> usic	
HomeKit	+	
Bluetooth		
Automation		
Click the lock to prev	ent further changes.	Advanced

Click the Privacy tab and select Full Disk Access from the left panel.

Select DeepInstinctClassifier, DeepInstinctRansomSvc and DeepInstinctExtension.

Full Disk Access Permission needs to be enabled.

Close the Security & Privacy screen.

If permissions are removed in the future, they can be re-enabled using the D-Client Console. For more information, see Enable Permissions from D-Client Console.

4.3.1.4. D-Client local installation with the Wizard

The D-Client can also be installed on each macOS device using the Installation wizard. This method may be useful in cases where you only have a few devices to install.

To install the D-Client on a macOS device using the Installation wizard:

1. Download the installation file from the macOS Deployment Resources screen and save it to a location where the macOS device has access.



2. Double-click the installation DMG file to mount it.



3. Double-click the Deep Instinct icon and click Allow in the confirmation dialog to open the wizard.

The **Deep Instinct Installer** appears.





4. Click **Continue** to start the installation. The **Configuration** dialog box opens.





•••	蔁 Install Deep Instinct	A
	Configuration	
Introduction	Management server address	DNS name
ConfigurationDestination Select	Installation token	Installation token
Installation Type	Device tag (optional)	Device tag
 Installation System Extension Permission 		
 Full Disk Access Permission 		
Summary		
deep Instinct		
		Go Back Continue

- 5. Enter the Management Server address (FQDN).
- 6. Enter the ID of the installation token, as displayed in the macOS Deployment Resources screen.
- 7. (Optional) Enter a tag associated with the deployed device. The Device Tag must comply to the following:
 - Maximum length is 256 characters
 - Case sensitive
 - Valid characters:
 - Letters (a-z, A-Z)
 - Numbers (0-9)
 - Spaces representable in UTF-8
 - Special characters: + = . _ : / @

Device tags can be used with rules to automatically add devices to a Device Group. It can also be used for selecting and filtering devices in the Management Console. For more information, see the Administrator Guide.



8. Click **Continue** and the Installation Type screen appears.



- 9. Click Install. A confirmation dialog appears.
- 10. Enter your administrator credentials and click Install Software.



11. The Deep Instinct extensions must be allowed to load. If permissions are required, the **System Extension Blocked** message appears.





12. Click **OK**. The System Extension Permission screen appears.

	蔁 Install Deep Instinct	A
	System Extension Permission	
IntroductionConfigurationDestination Select	To complete the installation, allow System Extensions to load. 1. <u>Click here</u> to open Security & Privacy Preferences.	
Installation TypeInstallation	 Click Details and select "DeepInstinctUtility" instances. 	
System Extension Permission Full Disk Access		
PermissionSummary		
dəep instinct	Go Back Continue	2

Perform the following:



a. Click Click here and the **Security & Privac**y screen opens.

- b. Click i at the bottom left corner of the screen. A confirmation dialog requesting your credentials appears.
- c. Enter the administrator's username and password.
- d. Click **Unlock** and then Details to continue.





- e. Select all instances of **DeepInstinctUtility** and click **OK** to permit Deep Instinct to load the required system extensions.
- 13. Deep Instinct may need to perform network filtering. If permission is required, the Filter Network Content message opens and click Allow.



14. Go back to the Installation Wizard to proceed with **Full Disk Access Permission**.



●● < > Ⅲ Secur	ity & Privacy	Q Search
Genera	I FileVault Firewall P	rivacy
yll Speech Recognition	Allow the apps below to	o access data like Mail,
Accessibility	Messages, Safari, Hom certain administrative s Mac.	e, Time Machine backups, and settings for all users on this
Input Monitoring		
Full Disk Access	🗹 🗎 DeepInstin	nctClassifier
Files and Folders	🖸 🍋 DeepInstin	nctRansomSvc
Screen Recording	🔽 🞅 DeepInstin	nctExtension
D Media & Apple Music		
HomeKit	+ -	
Bluetooth		
Automation		
Click the lock to prevent further	changes.	Advanced

a. Click the Click here link. The **Security & Privacy** screen appears.

- b. Select **DeepInstinctClassifier**, **DeepInstinctRansomSvc**, and **DeepInstinctExtension**.
- c. Enable Full Disk Access Permission for each user.
- d. Go back to the Installation Wizard.

ΝΟΤΕ
If permissions are removed in the future, they can be re-enabled using the D- Client Console. For more information, see <u>Enable Permissions from D-Client</u> Console.

15. A message appears after the installation completes successfully.



	蔁 Install Deep Instinct	8
	The installation was completed successfully.	
 Introduction Configuration Destination Select Installation Type Installation System Extension Permission Full Disk Access Permission 	Installation completed successfully.	
Summary		
deep instinct	Go Back Close	

16. Click **Close** to exit the Installation wizard.

4.3.2. Enabling permissions from the D-Client console

Required permissions

To protect your device, the D-Client on your device needs specific permissions to monitor, protect and notify you against threats. The OS requires various permissions to be enabled. The following permissions are required:

- System Extension Installation Permission
 - Endpoint Security Extension (DeepInstinctUtility)
 - Network Extension (DeepInstinctUtility)
- Full Disk Access Permission for the following processes:
 - DeepInstinctExtension
 - DeepInstinctClassifier
 - DeepInstinctRansomSVC



Network Content Filtering Permission

DeepInstinctUtility

Regardless of the method of installation (deployment tool/Installation Wizard/CLI Command), these permissions should be enabled during the installation. However, if permissions were removed or never granted, you can enable them through the D-Client Console.

To enable permissions from the D-Client Console:

Once the D-Client has been installed, the D-Client icon in the menu bar indicates whether macOS requires permissions. When permissions are missing, the Deployment status for the device changes to **Deployed with Warnings**, a Missing Permission screen appears on the macOS device and the icon is displayed with a yellow indicator, 💐.





In the **Missing Permissions** screen, click on the **click here** link. Depending on the number of missing permissions, one or more messages may appear. Refer to the following sections for details on enabling each type of system permission:
- "Enabling Missing System Extension Permissions"
- "Enabling Missing Full Disk Access Permission"
- "Enabling Missing Network Content Filtering Permission"

4.3.2.1. Enabling Missing System Extension Permissions

To enable missing permissions



1. In the **Missing Permissions** screen, click on the **click here** link.



2. If you are missing the **System Extension Permissions**, a message requesting to enable them is displayed (there may be additional messages for other missing permissions as well).



dəep instinct			
< 1/3 >	System Extens For Deep Instinct Extension permis Open <u>Security Pro</u> 'DeepInstinctUtili	ion Permission is to be fully operation ision must be allowe <u>eferences</u> and selec ity" instances.	Missing nal, System ed. t all
Remind me again	tomorrow	•	Close

3. Click the **Security Preferences** link. The **Security & Privacy** screen appears.





Security & Privacy	Q Search
General FileVault Firewall Privacy	
A login password has been set for this user Change Password.	
✓ Require password 5 minutes 0 after sleep or screer	n saver begins
Show a message when the screen is locked Set Lock M	essage
Disable automatic login	
Allow apps downloaded from:	
 App Store App Store and identified developers 	
App Store and Identified developers	
Some system software requires your attention before it can be us	ed. Details
Click the lock to make changes.	Advanced ?

4. Click the Lock icon at the bottom left corner of the screen and enter your administrator credentials in the dialog.

r	\bigcirc	System Prefe Privacy prefe	rences is trying rences.	to unlock Se	ecurity &
		Enter your pas	ssword to allow t	his.	
		User Name:			
		Password:			
				Cancel	Unlock

5. Click **Unlock** \rightarrow Details to continue.



System software from the following developers was updated and the system needs to be restarted before it can be used.	
 DeepInstinctUtility DeepInstinctUtility 	System software from the following developers was updated and the system needs to be restarted before it can be used.
Cancel OK	✓ DeepInstinctUtility
Cancel	DeepInstinctUtility
Cancel	
Cancel	
Cancel	
Cancel	
Cancel OK	
Cancer	
	Cancel

6. Select all **DeepInstinctUtility** instances and click **OK** to permit Deep Instinct to load the required system extensions.

4.3.2.2. Enabling Missing Full Disk Access Permission

To enable missing permission



1. In the **Missing Permissions** screen, click on the **click here** link.





2. If you are missing the **Full Disk Access Permission**, a message requesting to enable them is displayed (there may be additional messages for other missing permissions as well).





3. Click Security Preferences.





- 4. Click Security Preferences. The Security & Privacy screen appears.
- 5. Select **DeepInstinctClassifier**, **DeepInstinctRansomSvc**, and **DeepInstinctExtension**. Full Disk Access Permission needs to be enabled.
- 6. Close the **Security & Privacy** screen.

4.3.2.3. Enabling Missing Network Content Filtering Permission

To enable missing permission



1. In the **Missing Permissions** screen, click on the **click here** link.



2. If you are missing the **Network Content Filtering Permission**, a message requesting to enable them is displayed (there may be additional messages for other missing permissions as well).





3. Click the **Click here** link. The **Filter Content** screen appears.



4. Click **Allow**. After a few minutes the permissions are enabled and the D-Client icon changes to a normal state Ea.



4.3.3. macOS deployment resources

You can download the macOS D-Client installation package from the Management Console and preview the CLI command required to install the macOS D-Client on your devices.

To download the macOS D-Client file:

- 1. Log in to the Deep Instinct Management Console.
- 2. In the Navigation pane, click Settings \rightarrow Deployment \rightarrow MacOS.

deep instinct	Ø	Settings > Deployment	
답 Dashboard		Windows macOS Linux Chrome OS Mobile	
Monitor		Download Installation File	ى * *
Policy		Select the version and download	
□ Assets		Select Tenant	্ Tenant_1 🔹
武 Tenants		Installation Token	Revoke and Regenerate Token
II Reports		ab218d69-1cdc-48a7-988c-42848d2a1806	
ĝ Settings		CLI Preview Salect the ontione to display and convitte installation CLI command (for D	-Cliant version 2.4 and later)
		Use network proxy	
		Installation for VDI	
		No initial full scan after installation	
		D-Client disabled after installation	
		Device Tag O Add Lag	
		sudo DeepInstinct.dmg diproduct.customers.deepinstinctweb.com -toke	n ab218d69-1cdc-48a7-988c-42848d2a1806
			Copy CLI Command

- 3. Select the version of the macOS D-Client you want to download from the Download Installation File dropdown box.
- 4. Click 🛃 to download the installation file



Regenerating the installation token, deletes the previous token. All devices using a previously sent email to install the D-Client will fail. All devices will require the new installation token to install the D-Client.



4.4. Linux D-Client installation

The deployment of D-Clients on Linux devices can be performed remotely using a Linux deployment tool or directly from the devices.

Remote deployment using a Linux Deployment Tool

Local deployment using the Installation CLI command

4.4.1. Linux deployment resources

The Linux D-Client installation package is available for download in the Management Console's Settings \rightarrow Deployment \rightarrow Linux screen. In addition, in this screen you can also view the CLI command required to install the Linux D-Client on your devices.

To download the Linux D-Client file:

- 1. Log in to the Deep Instinct Management Console.
- 2. In the Navigation pane select Settings \rightarrow Deployment \rightarrow Linux.

dəsp instinct	¢	Settings > Deployment			MSP_1	MSP_1 (2)	мѕ₽_1 ⊘ Д
28 Dashboard		Windows macOS Linux Chrome OS Mobile					
Monitor		Linux Distribution - DHFL versions 7.6.7.7.7.8.7.9	PHEI 7				
Policy			ACTEL /				
_□ Assets		Select the version and download					
		Select Tenant	् Tenant_1 👻				
		Tenant selection will influence the installation token					
II Reports		Installation Token 💿	Revoke and Regenerate Token				
Settings		ab218d69-1cdc-48a7-988c-42848d2a1806					
		CLI Preview Salact the ontione to dienlay and conv the installation OI Loommand (for D-Client varian 2	and later)				
		No initial full scan after installation					
		bevice rag () Add day					
		deepinstinct_installer-3.4.2.305-0.sh diproduct.customers.deepinstinctweb.com -token	b218d69-1cdc-48a7-988c-42848d2a1806				
			Copy CLI Command				

3. Select the Linux distribution applicable to your device from the Linux Distribution dropdown box.



For CentOS devices, you will need to select the RHEL 7.9 distribution option and perform a few additional steps before running the installer file. These are specified in the relevant step of the "Linux D-Client installation" procedure.

- 4. Select the Linux D-Client version for download from the Download Installation File dropdown box.
- 5. Click 🛃 to download the installation file.

4.4.2. Remote deployment with a Linux deployment tool

In order to deploy the D-Client on your Linux devices using your Linux deployment tool, you need to first download the Deep Instinct Linux D-Client installation file from the Management Console Settings \rightarrow Deployment \rightarrow Linux screen. Refer to Linux Deployment Resources for details.



When installing on CentOS devices only — before running the installer package:

- 1. On the CentOS device, save a copy of the /etc/os-release file.
- 2. Open and edit the /etc/os-release file. The **/etc/os-release** file includes an entry with the field **<"NAME=CentOS Linux">**. The **NAME** string identifies the operating system without a version component.
- Rename the <"NAME=CentOS Linux"> to "NAME=Red Hat Enterprise Linux Server">.
- 4. Run and execute the Installer file.
- 5. Once the installation on the CentOS device is complete, restore and revert back to the original /etc/os-release file.



4.4.3. D-Client local installation with the CLI

To install D-Client on a Linux device:

- 1. Sign in to the device as a sudo or root user.
- 2. Verify that the device meets all of the requirements listed in Client System Requirements.
- 3. Download the relevant installation file from the Linux Deployment Resources screen.
- 4. Save the installation file to a location where the Linux devices has access.
- 5. For installations on CentOS devices only before running the installer package:
 - a. On the CentOS device, save a copy of the */etc/os-release* file.
 - b. Open and edit the */etc/os-release* file. The */etc/os-release* file includes an entry with the field <"NAME=CentOS Linux">. The NAME string identifies the operating system without a version component.
 - c. Rename the <"NAME=CentOS Linux"> to <"NAME=Red Hat Enterprise Linux Server">.
 - d. Once you have modified the file, you can run and execute the Installer file.
- 6. Open a Terminal window.
- 7. Provide executable permission for the installation file. At the command prompt, type the following command:

sudo chmod u+x <path><installation file>

Where:

Command Element	Description
<path></path>	Installation file path
<installation file=""></installation>	Installation file name

8. Run the installation file and at the command prompt, type the following command:

```
sudo <path><installation file> <server address> --token <installation
token> [--tag <tag>] [--nfs] [--mp <proxy url>:<proxy port>] [--on-
ly_validate_deps]
```

Where:



Command Ele- ment	Description	Comments
<path></path>	Installation file path	N/C
<installation file<="" td=""><td>Installation file name</td><td>N/C</td></installation>	Installation file name	N/C
<server ad-<br="">dress></server>	FQDN for the Management Server (D-Appliance)	N/C
<installation token></installation 	ID of the installation to- ken as displayed in the Linux Deployment Resour- ces screen.	N/C
<tag></tag>	Adds a tag associated with the deployed devices. Use quotation marks to enter values with spaces or spe- cial characters.	 Optional The Device Tag must comply to the following: Maximum length is 256 characters Device Tags are case sensitive Valid characters: Letters (a-z, A-Z) Numbers (0-9) Spaces representable in UTF-8 Special characters: + - = : / @ Device tags can be used with rules to automatically add devices to a Device Group. It can also be used for selecting and filtering devices in the Management Console. For more information, see the Administrator Guide.



Command Ele- ment	Description	Comments
nfs	Starts the D-Client without performing the initial full scan.	Optional
mp	Enables the use of a net- work proxy server, using the specified settings of the proxy server URL and port number.	Optional
<proxy url=""></proxy>	URL for the proxy server, in- cluding the scheme	N/C
<proxy port=""></proxy>	Port number to access the proxy server.	N/C
only_vali- date_deps	Disables the automatic in- stallation of the required packages. It validates whether the required pack- ages have been installed. If a required package is miss- ing, the installation of D-Cli- ent is aborted and an error message is provided.	Optional



```
Example 4. CLI command
For the following values:
 path = /home/user/Downloads/
installation file = deepinstinct_installer.sh
server address = customer.deepinstinctweb.com
  installation token = 12345678
  System without MSP
The commands appear as:
[user@localhost ~] # sudo chmod u+x /home/user/Downloads/deepin-
stinct installer.sh
[sudo] password for user:
[user@localhost ~] # sudo /home/user/Downloads/deepinstinct instal-
ler.sh customer.deepinstinctweb.com --token 12345678
Extracting installation files...
Redirecting to /bin/systemctl start DeepNetworkService.service Redi-
recting to /bin/systemctl start DeepSAService.service
[user@localhost ~]#
```

9. For CentOS devices only — on the CentOS device, restore and revert back to the original /etc/os-release file.

4.5. Mobile D-Client installations

The deployment of D-Clients on mobile devices can be performed either remotely using a mobile deployment tool or directly from the devices.

- Remote deployment on Android devices using SOTI
- Local deployment for Mobile D-Clients

Before deploying:

Make sure you have configured your **SMTP server account** required for the deployment on mobile devices and event notifications, The deployment of the D-Client uses a link sent



by email from the Management Server. The SMTP Server may have been configured while running the Startup wizard. If not, configure the SMTP Server from the General Configuration screen. For more information, see the Administrator Guide.

4.5.1. D-Client deployment with SOTI MobiControl

SOTI MobiControl is a management tool that can deploy D-Clients on all your organization's Android devices. The D-Client deployment process using SOTI MobiControl requires the following:

- Create and place a unique identification file on each mobile device
- Managed Google Play Account
- Approve the Deep instinct application using SOTI
- FQDN for the Deep Instinct Management Server
- Identification number of the installation token
- Create an App Policy
- Assign the policy to the devices

4.5.1.1. Creating a mobile identification file

Prior to deploying the D-Client with SOTI, a unique identification file must first be created and placed on each mobile device. The identification file and location must comply with the following:

- The installation file must be a JSON file.
- It must contain a serial key, also known as the **Mobile ID**.

Example: "serial":"21103522509568"

- Filename must be **devInfo.json**
- The file must be placed at the following location on the mobile device: /sdcard/UPRR/

4.5.1.2. Creating an app policy and assigning devices for D-Client deployment

To create an App Policy and assign devices for deployment:

1. Create and place a unique identification file on each mobile device to be deployed.

- 2. Verify that you have a managed Google Play Account and that you know the name of the account.
- 3. Verify that the Deep instinct application is approved by SOTI.

- 4. From the SOTI MobiControl console, open the **App Policies** list by selecting Policies+Apps.
- 5. Click NEW APP POLICY . The **CREATE APP POLICY** dialog appears.

CREATE APP POLICY			
Use an App policy to insta families have additional f	all Apps on your device ypes.	s. App policies can only be created for a s	ingle family at a time. Some
Please Choose *			
	ć		
Android ~	Apple >	Windows	
Android Enterprise			

6. Click Android+Android Enterprise to create an App Policy for your Android device. The **CREATE APP POLICY** screen appears (**GENERAL** tab).



CREATE APP POLICY		0
GENERAL	APPS	
App Policy Name *	Policy Name	
Description	Policy Description	
Policy Status	n/a	
Family	n Android Plus	
Туре	Android Enterprise	
Apps	0	
	CANCEL SAVE AND A	SSIGN SAVE

- 7. Enter the name of the new App Policy and click the APPS tab.
- 8. Click \bigoplus (top right corner of the screen) to add an application.



Apps				
App Source		Managed	Google Play	~
Bindings				
Select		DI		~
Apps	, P s	earch apps	MANAGED GOOGL	E PLAY
	NAME	VERSION	TYPE	
	Deep Instinct	3.3.1.500	Mandatory	Î
				Ŭ

- 9. Select MANAGED GOOGLE PLAY from the App Source dropdown box.
- 10. Select your Managed Google Play Account from the Select dropdown box.



11. Select the checkbox for Deep Instinct from the list and click 🙆. The Advanced Configuration screen opens.



ADVANCED CONFIGURATIONS		0
Configuration Options	Specify the configuration options for the application you are adding o	orediting
App Details Installation Options Managed App Config	Enable Managed App Config Advanced options available for the application Management server address Installation token	
		CANCEL SAVE

- 12. Click Managed App Config and perform the following:
 - a. Enable the Managed App Config by clicking the toggle. The available parameters are displayed.
 - b. Enter the FQDN for the Management Server.
 - c. Enter the ID of the installation token, as displayed in the Mobile Deployment Resources screen in the Management Console.
 - d. Click **SAVE** and then click **ADD**. The Deep instinct app is now displayed in the Apps list.
- 13. Click **SAVE AND ASSIGN** to assign this policy to devices. The Assign screen opens.



DEVICES	USERS		FILTERS
evice Groups	,O	Devices (1)	$\leftarrow \texttt{lof1} \rightarrow $
/ 🔽 My Company 😐		DEVICE	NAME
 Management bevices Sales Devices Warehouse Devices 			Zebra test device unavailable

- 14. Select the checkboxes for all the Device Groups and Devices that you want to assign the new App Policy.
- 15. Click **ASSIGN** to deploy D-Client to all the selected devices. Once the D-Client is installed on a device, you can see the device in the Device List from the Management Console.

4.5.2. Local deployment for mobile D-Clients

The local deployment of D-Clients on Android, Chrome OS, iOS and iPadOS devices consists of two phases:

- 1. Running the Deployment wizard to send an email to each user of Android, Chrome OS, iOS or iPadOS devices
- 2. Install the D-Client using the received email.



IMPORTANT

Before you can deploy:

Make sure you have configured your **SMTP server account** required for the deployment on mobile devices and event notifications, The deployment of the D-Client uses a link sent by email from the Management Server. The SMTP Server may have been configured while running the Startup wizard. If not, configure the SMTP Server from the General Configuration screen. For more information, see the Administrator Guide.

4.5.2.1. Deployment Wizard

The Deployment Wizard generates a deployment email to the mobile devices which is then used to install the D-Client.

To run the Deployment wizard:

- 1. Log in to the Deep Instinct Management Console.
- 2. Select Settings \rightarrow Deployment \rightarrow Chrome OS \rightarrow Mobile (Android, iOS, and iPadOS devices).

dəep instinct		Setti	ngs > Deployment		
문문 Dashboard	1		Windows macOS Linux Chrome	DS Mobile	
Monitor		Play	Store (Android)		Copy Link
Policy		http:	://play.google.com/store/apps/details?id=com.deepin:	tinct.android&hl=en	
C Assets		App	Store (iOS)		Copy Link
음. Tenants		Sele	ct Tenant		্ Tenant_1
II Reports		Tena	nt selection will influence the installation token		
ĝ: Settings		Insta	Ilation Token 💿		Revoke and Regenerate Token
				Deployment Emails Send deployment emails to your employees	Start

- 3. For deployments with MSP support click the Select Tenant dropdown box and select the tenant associated with the deployment.
- 4. Click **Start** to start the Deployment wizard. The Settings page of the Deployment Emails screen appears.



B bahbcard B bahbcard <th>Bethour Image: Control of the contr</th> <th>dəep instinct</th> <th>Settings > Deployment</th> <th></th> <th>MSP_1 ⑦</th>	Bethour Image: Control of the contr	dəep instinct	Settings > Deployment		MSP_1 ⑦
o homor o, memor o homor Tanat o homor Tanat o homor Administrator Contact Details Administrator Contact Details x remark Name poor Name Poor number Poor number Email address ure, Email address ure, Email address ure, Subject Subject Introduction Deer finploree, Ag part of our organization's security Solution Deep instinct ogo ony our defec. This is important to ensure the security	indication in holine in keys the	문 Dashboard	(C) 1 Settings		
Assets Administrator Contact Details A renards Name Tile Tile Phone number Phone number Phone number Inmal address URL URL Email address URL Sabjet New Mobile Security Solution Introduction Despringer Employees are required to install the peoployees are required to install the security solution	Assts Administrator Contact Details Name Name Teamsts Tile Poore number Pione number Pione number Email address UR UR	Monitor Policy	Tenant	C. Tenant, 1 -	
Name Name Name Name Tile Tile Phone number Phone number Brail address Email address URL URL Skylet New Mobile Security Solution Introduction Description or our desce. This is important to ensure the security solution Ar part of our organization's security solution Performance from prove are required to install the performant to ensure the security solution	Name Name Tile Phone number Phone number </th <th>_ Assets →</th> <th>Administrator Contact Details</th> <th></th> <th></th>	_ Assets →	Administrator Contact Details		
in Reports Tile Tile Phone number Phone number Enail address Enail address URL URL Enail Message Subject Subject New Mobile Security Solution Introduction Deer fundorers As part of our organization's security polycyou are required to install the Deep instanct op on your defect. This is important to ensure the security of our organization and its employees from malicious activities.	n Peorta Tile Tile Phone number Phone number Enail address Enail address URL URL Enail Message Enail Message Enail	앒. Tenants	Name		
Phose number Phose number Phose number Phose number Enail address Enail address UBL URL Subject New Mobile Security Solution Introduction Deer Employees As part of our organization's security policy you are required to install the Deep instanct on your defect. This is important to ensure the security of our organization and its employees from malicious activities.	Phone number Phone number Phone number Enail address Link Enail address URL URL Enail Messago Sobject Subject New Mobile Sacurity Solution Introduction Dear Englayers Subject New Mobile Sacurity Solution	II Reports	Title		
Enall address Enall address URL URL Email Message Subject New Mobile Security Solution Introduction Deer Employees As part of our organization's security policy, you are required to install the Deep instanct app on your derice. This is important to ensure the security of our organization and its employees from malicious activities.	Enail address Enail address URL URL Enail Message Subject New Mobile Security Solution Introduction Dear Engloyer. As part of our organization and its employers show are required to install the periphinter to provide dear this is important to ensure the security of our organization and its employers from malicious activities.	tĝt Settings →	Phone number		
URL URL Email Message Subject Subject New Mobile Security Solution Introduction Deer Employee: Deep instanct app on your device. This is important to ensure the security of our organization and its employees from malicious activities.	URL URL Email Message Subject New Mobile Security Solution Introduction Dear Employee. As part of our organization's security policy you are required to install the perfunction gap our orderice. This is important to ensure the security of our organization and its employees from malidious activities.		Email address		
Email Message Subject New Mobile Security Solution Introduction Dear Employee. As part of our organization's security policy, you are required to install the Deep instinct upp on your dence. This is important to ensure the security of our organization and its employees from malicious activities.	Email Message Subject New Mobile Socurity Solution Introduction Dear Employee. A part of our cognization's security policy you are required to install the polymore that whether a security of our cognization and its employees from multiclous activities.		URL		
Subject New Mobile Socially Solution Introduction Dest Employee. As part of our organization's security policy, you are required to install the Desp instinct upp on your device. This is important to ensure the security of our organization and its employees from malicious activities.	Subject New Mobile Security Solution Introduction Descriptions: As part of our complication's security policy you are required to install the polymorphile security and its employees from maldious activities. 23/1024		Email Message		
Introduction Dest Employee. As part of our organization's security policy you are required to install the Deep instinct app on your device. This is important to ensure the security of our organization and its employees from malicious activities.	Introduction Dear Employee, Append or arroy point of arrow point o		Subject	New Mobile Security Solution	
	233 / 1834		Introduction	Dear Employee, As part of our organization's security policy, you are required to install the Deep Institut app on your device. This is important to ensure the security of our organization and its employees from malicious activities.	
				Cancel Next	

- 5. For deployments with MSP support click the Select Tenant dropdown box and select the tenant associated with the deployment.
- 6. Enter the administrator's contact information for the employees to contact, if they have any questions (e.g., name, title, phone number, email address and URL). Name and email address are mandatory.

You can add a subject and an introduction message as well.

7. Click **Next** and the **Create Address List** page opens.



dəep instinct	Settings > Deployment	MSP_1	0	۵	8
品 Dashboard	» 3				
Monitor +					
Lo Assets →					
<u>와</u> Tenants					
II Reports					
Settings >					
	Crasta s list of amail addresses				
	Cancel Back Send				

8. Click Add Email Addresses to create the list of email addresses for the deployment emails. The Add Emails dialog box opens.

dd Emails		
Manually add email addresses () Create a list of email addresses to deploy D-Client in your organizaiton		
Email Addresses		
Import a list of email addresses from a file (i)		
The results from the file and the manually added addresses will be displayed in the email addresses list	Browse	
	Cancel	

- 9. Enter email addresses:
 - Manually type the addresses in the Email Addresses field. Separate each address
 with a comma, semicolon or a new line.

- Import click Browse and select a CSV or TXT file that contains a list of addresses. The selected file must separate each address by a comma, semicolon or a new line.
- 10. Click Add . The manually entered addresses and the addresses in the file will be added to the Deployment Email list. The Deployment Email table is displayed.

The Deployment Email table includes the following information:

- **Source** Displays whether the email address was entered manually, or the name of the file from where the address was imported.
- Line Displays the line in the imported file from where the address was taken. If you want to edit the imported address, this will assist you in finding the address.
- **Email Addres**s Displays the the email address to where the deployment email will be sent.
- **Details** Displays whether the address was added or if there is a problem with the address. The system identifies duplicate and invalid email addresses. These problem addresses must be resolved to continue. You can edit or remove any address in the list by right-clicking the address entry and select the appropriate action.



- 11. Once you have finalized the email address list, click **Send**. A confirmation screen is displayed to indicate how many emails were sent.
- 12. Click Finish .

deep

4.5.2.2. D-Client installation from emails

When an organization deploys D-Client on Chrome OS, Android, iOS and iPadOS devices, an email is sent out to each user. After the Deployment wizard completes successfully, users receive this deployment email. Users should follow this email to install D-Client. For more information, see the following sections:

- Email Installation for Android Devices
- Alternative Installation for Android Devices
- Email Installation for Chrome OS Devices
- Installation Prerequisite using Chrome OS Built-In Email App
- Email Installation for iOS and iPadOS Devices



Alternative Installation for iOS and iPadOS Devices

Email installation for Android devices

The email installation is the recommended method to install Deep Instinct D-Client on your Android device. However, if your device cannot receive emails or has limitations that prevent the installation by email, use the alternative installation.

Once users have received an installation email on their Android device, they can proceed to install Deep Instinct as follows:

1. Open the installation email on the Android device and read the email.



2. Tap Get App in the email to download and install Deep Instinct D-Client from Google Play. The Deep Instinct Agent installation screen opens.





Deep Instinct™ Deployment and Installation Guide

3. Tap INSTALL to install D-Client. A screen opens to indicate that Deep Instinct was installed.



4. Tap CONTINUE to start D-Client. A screen opens to allow access to the privacy policy and to activate D-Client.



- 5. Tap Get Started. Deep Instinct D-Client is activated and scans your device.
- 6. In order to protect your device, specific permissions must be enabled. The order of the permission requests and some of the permissions, vary based on the operating system on your device.
- 7. Allow Usage Access to monitor malicious activities from other apps.



8. Tap Allow Usage Access and the Apps with usage access screen appears.



9. Tap Deep Instinct and the Usage access screen appears.



- 10. Tap the switch to permit usage access for Deep Instinct.
- 11. Enable Battery Optimizations permission to ensure continuous protection of your device.





12. To allow the Deep Instinct app to stay connected in the background, tap Allow Battery Optimization. A message appears.



- 13. Tap Yes to allow the Deep Instinct app to stay connected.
- 14. For Android 10 enable Appear on Top permission to display messages on top of apps when a malicious app is detected.



15. Tap Allow Appear on Top and the Appear on top appears.



< Appear on top	
Deep Instinct	
Allow permission	\bigcirc

- 16. Tap the switch to allow this permission.
- 17. Once your device is scanned and no malicious file is detected, Deep Instinct informs you that no threats were found.



Alternative installation for Android devices

When an email installation cannot be performed on an Android device, there is an alternative method to install the Deep Instinct using a QR Code. The email must first be sent to another device. Once received, the user can proceed to install Deep Instinct as follows:

1. Go to **Google Play** and open the **Deep Instinct** app.







2. Tap Install to install D-Client. A screen opens to indicate that Deep Instinct was installed.
| | | | 🗿 📶 100% 🖿 | 16 | :45 | |
|--|---------------------------------------|-------|---------------------------------------|----|---------------|--|
| \leftarrow Google Play | | | Q | | • | |
| Deep Instinct
Deep Instinct LTD
Business | | | | | | |
| UNINSTA | ALL | | CONTINUE | | | |
| Ads Related to this app | | | | | | |
| 0 | PO ^N | No to | 2019 | | | |
| Power
Security - A
6.9 MB | Virus Cleaner
2019: Scan
8.4 MB | : | Virus Cleaner
& Phone Cl
9.3 MB | : | | |
| You might also like MORE | | | | | | |
| | | 9 | | 15 | Bus | |
| Quarry: | Mirror: Real
Mirror | : | Multi
Clinometer | : | Busir
Card | |

3. Tap Open to start D-Client. A screen opens to allow access to the privacy policy and to activate D-Client.



4. Tap Get Started and the App permissions screen opens.





5. To use the QR Code to enter the information, tap the switch to permit camera usage. The QR Code Scanning screen opens and perform the following:



- a. Open the Installation email on another device.
- b. With the camera on your Android device, scan the QR Code in the email.
- 6. To activate D-Client using your activation credentials, tap Enter your activation credentials. The Activation screen opens and perform the following:



- a. Enter the Management server address and Installation token.
- b. Tap **Activate**.
- 7. In order to protect your device, specific permissions must be enabled. The order of the permission requests and some of the permissions, varies based on the operating system on your device.
- 8. Allow **Usage Access** to monitor malicious activities from other apps.



9. Tap **Allow Usage Access** and the Apps with usage access screen appears.



10. Tap **Deep Instinct** and the Usage access screen opens.



- 11. Tap the switch to permit usage access for Deep Instinct.
- 12. Enable Battery Optimizations permission to ensure continuous protection of your device.





13. To allow the Deep Instinct app to stay connected in the background, tap Allow Battery Optimization. A message appears.



- 14. Tap Yes to allow the Deep Instinct app to stay connected.
- 15. In Android 10, enable **Appear on Top permission** to display messages on top of apps when a malicious app is detected.



16. Tap **Allow Appear on Top** and the Appear on top appears.



< Appear on top	
Deep Instinct 2.3.2.0	
Allow permission	\bigcirc

17. Tap the switch to allow this permission.

Once your device is scanned and no malicious file is detected, Deep Instinct informs you that no threats were found.



Email installation for Chrome OS devices

The email installation is the preferred method to install Deep Instinct D-Client on your Chrome OS device. If an email app has been installed (such as Gmail) in addition to the built-in app, use the installed email app to open the installation email. If the built-in email app will be used, a setting must be changed in this app prior to opening the email, as described in "Installation prerequisite using Chrome OS built-in email app".

Once users have received an installation email on their device, they can proceed to install Deep Instinct as follows:

1. If an email app has been installed on the Chrome OS device, open the installation email on the device using the installed app. If the built-in email app will be used, follow the steps in



2. Click Click App in the email to download and install Deep Instinct D-Client from Google Play. The Deep Instinct Agent installation screen opens.



16:19 M 🖸 🗟	💐 🙃 🕼 .ıll 36% 🛔			
←	Q :			
Deep Ir Deep Instin	nstinct ct LTD			
5.0★ 17 reviews 14 MB	3 1K+ PEGI 3 🛈 Download			
Install				
	Image: Section of the section of t			
About this app	\rightarrow			
Deep Learning cybersecurity platform for zero-time mobile threat prevention				
Business				

 \triangleleft



3. Click INSTALL to install D-Client. A screen opens to indicate that Deep Instinct was installed.



4. Click CONTINUE to start D-Client. A screen opens to allow access to the privacy policy and to activate D-Client.





- 5. Click Get Started. Deep Instinct D-Client is activated and scans your device.
- 6. In order to protect your device, specific permissions must be enabled. The order of the permission requests and some of the permissions, vary based on the operating system on your device.
- 7. Allow Usage Access to monitor malicious activities from other apps.





8. Click Allow Usage Access and the Apps with usage access screen appears.





9. Click Deep Instinct and the Usage access screen appears.



- 10. Enable Permit usage access for Deep Instinct.
- 11. Click Allow Battery Optimization to ensure continuous protection of your device.
- 12. To allow the Deep Instinct app to stay connected in the background, tap Allow Battery Optimization. A message appears.



- 13. Click Yes to allow the Deep Instinct app to stay connected.
- 14. For Android 10 enable Appear on Top permission to display messages on top of apps when a malicious app is detected.





15. Click Allow Appear on Top and the Appear on top appears.

< Appear on top	
Deep Instinct	
Allow permission	\bigcirc



- 16. Enable the Allow Permission option.
- 17. Once your device is scanned and no malicious file is detected, Deep Instinct informs you that no threats were found.



Installation prerequisite using Chrome OS built-in email app

If the built-in email app will be used to install Deep Instinct D-Client on your Chrome OS device, a setting must be changed in this app prior to opening the installation email. Change the Chrome OS setting, as follows:

1. Go to Settings.

← <u>default</u>	×
GENERAL > APPS & NOTIFICATIONS	
Default apps	
GENERAL > LANGUAGE & INPUT > SPELLING CORRECTIO	N
Default spell checker	
GENERAL > RESTART & RESET	
Factory data reset	

Delete all data and restore default settings

G	defa	ult	d	efaul	ts	de	faulte	d 🌷
\mathbf{q}^{1}	W ²	e i	4	t s	y ็i	J ⁷	i [®] (o [°] p [°]
а	s	d	f	g	h	j	k	Ι
仑	z	x	с	v	b	n	m	$\langle \times \rangle$
?123	;;			Eng	glish			٩
	7	7		\bigcirc				

2. Search and go to "Default apps".

← Default apps					
Assist & voice input					
Browser app Chrome					
Home app Home					
Phone app Contacts					
Message app Messages					
App links					
DEFAULT FOR WORK					
Browser app Chrome					



3. Click App links.



4. Click Google Play services.







5. Click Open supported links.



6. Select Open in this app.

To continue installing Deep Instinct D-Client on your Chrome OS device, following the steps in Email Installation for Chrome OS Devices.

Email installation for iOS and iPadOS devices

Once users have received an installation email on their iOS or iPadOS device, they can proceed to install D-Client as follows:

1. Open the installation email on the iOS or iPadOS device and read the email.



device.



2. Tap Get App in the email to download and install Deep Instinct D-Client from App Store. The Deep Instinct Agent installation screen opens.





3. Tap GET to install D-Client. A screen opens to indicate that Deep Instinct was installed.



Tap OPEN to start D-Client. A notification message appears.





To allow the Deep Instinct app to display security notifications, tap Allow. A screen opens to allow access to the privacy policy and to activate D-Client.



Tap Get Started. Deep Instinct is activated and scans your device.

Once your device is scanned and no problems were detected, Deep Instinct informs you that your device is secure.





Alternative installation for iOS and iPadOS devices

When an email installation cannot be performed on an iOS and iPadOS device, there is an alternative method to install the Deep Instinct using a QR Code. The email must first be sent to another device. Once received, the user can proceed to install Deep Instinct as follows:

1. Go to App Store and open the Deep Instinct app.





2. Tap GET to install D-Client. A screen opens to indicate that Deep Instinct was installed.



3. Tap OPEN to start D-Client. A notification message appears.





4. To allow the Deep Instinct app to display security notifications, tap Allow. A screen opens to allow access to the privacy policy and to activate D-Client.





5. Tap Get Started and the App permissions screen opens.





6. To use the QR Code to enter the information, tap the switch to permit camera usage. The QR Code Scanning screen opens.



Perform the following:

- a. Open the Installation email on another device.
- b. Then with the camera on your iOS or iPad device, scan the QR Code in the email.
- 7. To activate D-Client using your activation credentials, tap Enter your activation credentials. The Activation screen opens and perform the following:





- 8. Enter the Management server address and Installation token.
- 9. Tap Activate. Deep Instinct is activated and scans your device.
- 10. Once your device is scanned and no problems were detected, Deep Instinct informs you that your device is secure.



4.6. Application Security deployment

Application Security runs as a containerized application where you are provided with a Docker image used for deploying the application. We support two options for deploying with a Docker image:

Application Security deployment with a standard OS image

Application Security deployment with your organization's OS image of CentOS 7.9 or RHEL 7.9

Before you deploy:

- 1. Define General Configuration settings and your Application Security policies. For more information, see the Administrator Guide.
- 2. Verify that your Docker Host and Docker containers comply with the requirements listed in "Application Security" requirements.
- 3. Acquire the relevant Application Security package file from Deep Instinct Support.



4.6.1. Application Security deployment using a predefined Docker image

This procedure describes the process of deploying Application Security using a predefined Docker image supplied by Deep Instinct. This image includes a standard OS image.

To deploy and run Application Security:

- 1. Verify that the Docker host and Docker containers meets all of the requirements listed in "Application Security" requirements.
- 2. Verify that the Firewall rules are set to meet the requirements described in Prepare Your Network.
- 3. Acquire the relevant package from Deep Instinct Support.
- 4. Open a Terminal window.
- 5. Change the current directory to the folder where the package is located.
- 6. Load the Docker image using the package. At the command prompt, type the following command:

docker load -i <package>

Where: <package> = File name of the package acquired from Deep Instinct Support.

- 7. After the image is loaded, display the list of images to verify that the image is in the docker. At the command prompt, type the following command: **docker images**
- 8. Using the image ID, assign the tag name "application security" to this image. At the command prompt, type the following command:

docker image tag <image id> agentless

Where: **<image id>** = Image ID for the newly loaded image

9. Verify that the image now has the name "agentless". The name should be displayed in the Repository column of the Image List. At the command prompt, type the following command to display the image list:

docker images

10. Run a Docker container from the image. At the command prompt, type the following command:

docker run -e APPLIANCE_URL=<server address> -e TOKEN=<token> [-e PROXY_URL=<proxy url>:<proxy port>] [-e NO_SSL=true] [-e CERT=<base64_cert>; -e PRIVATE_KEY=<base64_key>] -p <service port>:5000 agentless

Where:

Command Parameter	Description	Comments
<server address></server 	FQDN for the Management Server (D-Appliance)	N/C
<token></token>	ID of the installation to- ken, as displayed in the Linux Deployment Resour- ces screen.	N/C
PROXY _URL	Enables the use of a net- work proxy server, using the specified settings of the proxy server URL and port number.	Optional
<proxy url></proxy 	URL for the proxy server, in- cluding the scheme.	N/C
<proxy port></proxy 	Port number to access the proxy server.	 Optional — only relevant with REST API integration Do not use with CERT or PRI- VATE_KEY
NO_SSL	When set to "true", no SLL certificate is required and all REST API requests to the container must use HTTP protocol.	Optional — only relevant with REST API integration
CERT and PRI- VATE_KRY	Enables the use of your X.509 certificate, using the specified information of your certificate and private key.	Do not use with NO_SSL
<base64_ce rt></base64_ce 	Single line base64 encoded string of the certificate file.	N/C
<base64_ke y></base64_ke 	Single line base64 encoded string of the private key associated with the certifi- cate.	N/C

Command Parameter	Description	Comments
<service port></service 	Port number used for inte- gration using ICAP or REST API.	Typically, ICAP uses port number 1344 and REST API port number 443.
<exposed port></exposed 	Port number used for inte- gration using ICAP or REST API: <1344> OR <443>	Typically, ICAP uses port number 1344 and REST API port number 443.
NUM_THREAD S_PER_WORK ER:	Used for configuring the number of Gunicorn (Py- thon web server) threads for the worker processes handling the REST API re- quests: NUM_THREADS_PER_WORK- ER = 4*Number of CPUs	 Applies to REST integration only Optional — can be manually added to the command Default (without this parameter) = 4*number of CPUs Used for optimizing the use of system CPU resources Cannot be used with "DIS-ABLE_WORKER_THREADING" parameter.
DISA- BLE_WORK- ER_THREAD- ING	 Disables the worker threading: DISABLE_WORK- ER_THREADING = true when threading is disabled DISABLE_WORK- ER_THREADING = false when threading is enabled 	 Applies to REST integration only Optional — can be manually added to the command Cannot be used with "NUM_THREADS_PER_WORKER" parameter
Command Parameter	Description	Comments
----------------------	-------------------------	--
NUM_WORK-	Enables configuring the	 Applies to REST integration only Optional — can be manually added to the command Default (without this parameter)
ERS:	number of workers	= 4*number of cores

11. Display the list of containers to verify that the container is running. At the command prompt, type the following command:

docker ps

- 12. Verify that your container is displayed in the Device List of the Management Console. The container ID displayed in the Container List should be displayed in the Management Console. For more information, see the Administrator Guide.
- 13. Once your container is registered with the Management Server and the configurations files have been downloaded, you can proceed to send files for scanning.

🦻 ΝΟΤΕ

For information on integration using ICAP or REST API, see Application Security Integration.

4.6.2. Application Security deployment using a customized Docker image

This procedure describes the process of deploying Application Security by creating a customized Docker image with your organization's OS image of CentOS 7.9 or RHEL 7.9.

To deploy and run Application Security:

- 1. Verify that the Docker host and Docker containers meets all of the requirements listed in Client System Requirements.
- 2. Verify that the Firewall rules are set to meet the requirements described in Prepare Your Network.
- 3. Acquire the relevant package from Deep Instinct Support.
- 4. Open a Terminal window.



- 5. Change the current directory to the folder where the package is located.
- 6. Create a new directory to unpack the package. At the command prompt, type the following command:

mkdir dipa-pkg

7. Unpack the package. At the command prompt, type the following command:

```
tar -xzvf <package> --directory dipa-pkg
```

Where: <package> = File name of the package acquired from Deep Instinct Support.

8. Change the current directory to the folder where the package was unpacked. At the command prompt, type the following command:

cd dipa-pkg

- 9. Customize the Dockerfile, to use your organization's OS image of CentOS 7.9 or RHEL 7.9.
- 10. Build the customized Docker image. At the command prompt, type the following command:

docker build -t agentless --network=none

11. After the image is built, display the list of images to verify that the image is in the docker and it has the name "agentless". The name should be displayed in the Repository column of the Image List. At the command prompt, type the following command to display the image list:

docker images

12. Run a Docker container from the image. At the command prompt, type the following command:

```
docker run -e APPLIANCE_URL=<server address> -e TOKEN=<token>
[-e PROXY_URL=<proxy url>:<proxy port>;] [-e NO_SSL=true] [-e
CERT=<base64_cert> -e PRIVATE_KEY=<base64_key>] -p <service port>:5000
agentless
```

Where:

Command Parameter	Description	Comments
<server address></server 	FQDN for the Management Server (D-Appliance)	N/C

Command Parameter	Description	Comments
<token></token>	ID of the installation to- ken, as displayed in the Linux Deployment Resour- ces screen.	N/C
PROXY _URL	Enables the use of a net- work proxy server, using the specified settings of the proxy server URL and port number.	Optional
<proxy url></proxy 	URL for the proxy server, in- cluding the scheme.	N/C
<proxy port></proxy 	Port number to access the proxy server.	 Optional — only relevant with REST API integration Do not use with CERT or PRI- VATE_KEY
NO_SSL	When set to "true", no SLL certificate is required and all REST API requests to the container must use HTTP protocol.	Optional — only relevant with REST API integration
CERT and PRI- VATE_KRY	Enables the use of your X.509 certificate, using the specified information of your certificate and private key.	Do not use with NO_SSL
<base64_ce rt></base64_ce 	Single line base64 encoded string of the certificate file.	N/C
<base64_ke y></base64_ke 	Single line base64 encoded string of the private key associated with the certifi- cate.	N/C
<service port></service 	Port number used for inte- gration using ICAP or REST API.	Typically, ICAP uses port number 1344 and REST API port number 443.

Command Parameter	Description	Comments
<exposed port></exposed 	Port number used for inte- gration using ICAP or REST API:	Typically, ICAP uses port number 1344 and REST API port number 443.
	<1344>	
	OR	
	<443>	
NUM_THREAD S_PER_WORK ER:	Used for configuring the number of Gunicorn (Py- thon web server) threads for the worker processes handling the REST API re- quests: NUM_THREADS_PER_WORK- ER = 4*Number of CPUs	 Applies to REST integration only Optional — can be manually added to the command Default (without this parameter) = 4*number of CPUs Used for optimizing the use of system CPU resources Cannot be used with "DIS-ABLE_WORKER_THREADING" parameter.
DISA- BLE_WORK- ER_THREAD- ING	 Disables the worker threading: DISABLE_WORK- ER_THREADING = true when threading is disabled DISABLE_WORK- ER_THREADING = false when threading is enabled 	 Applies to REST integration only Optional — can be manually added to the command Cannot be used with "NUM_THREADS_PER_WORKER" parameter



Command Parameter	Description	Comments
NUM_WORK- ERS:	Enables configuring the number of workers	 Applies to REST integration only Optional — can be manually added to the command Default (without this parameter) = 4*number of cores

13. Display the list of containers to verify that the container is running. At the command prompt, type the following command:

docker ps

- 14. Verify that your container is displayed in the Device List of the Management Console. The container ID displayed in the Container List should be displayed in the Management Console. For more information, see the Administrator Guide.
- 15. Once your container is registered with the D-Appliance and the configurations files have been downloaded, you can proceed to send files for scanning.



For information on integration using ICAP or REST API, see Application Security Integration.



5. Post-installation

Now that you have completed the deployment process, you may want to proceed with the following procedures:

- "Deployment monitoring"
- "Application Security integration" with REST/ICAP
- "Client deployment validation"

5.1. Deployment monitoring

The Device List can be used to monitor the deployment and installation progress in your organization. It displays the deployment status for each device and your total license usage. For more information, see the Administrator Guide.

5.2. Application Security integration

Deep Instinct[™] Prevention for Applications supports two main integration scenarios for configuring the Scan API:

"Integration using ICAP" — uses ICAP for gateway protection (prevention and detection)

"Integration using REST API" — uses REST API for application protection (detection)

5.2.1. Integration using ICAP

Access the Deep Instinct ICAP service using the following URL: ICAP://<Agentless IP>:1344/ classify

ICAP server supports the following requests:

• **Options** – This request specifies which ICAP services are supported.



Currently support is for RESPMOD only. Application Security returns a header called 'Methods', with a single value 'RESPMOD'.

• **RESPMOD** – Application Security receives the file buffer and analyses its content.



Response

- In case of a benign file no modifications will occur.
- In case of a malicious file the following fields are sent along with a 403 http status code:

Header Name	Description	Example
X-Blocked-Reason	Contains the blocking reason of the content	X-Blocked-Reason: Infected
X-Virus-ID	Contains a short description of the threat that was found in the content. If multiple threats were found, only the first one is returned.	X-Virus-ID: Mal- ware
X-Infection-Found	tion-Found Contains the description of the threat that was found in the content. If multiple threats were found, only the first one is returned.	
	The value is a semicolon separated list with three parameters.	X-Infection-Found: Type=2; Resolu- tion=0; Threat=En- crypted Archive;
	Туре:	
	0: Infection was found.	
	2: Container violation was found.	
	Resolution:	
	0: Suspicious content was not re- paired.	
	Threat: Threat name	
X-Violations-Count	Contains the number of the reported violations	0
X-Violation <num- ber>-FileName</num- 	Name of the file that was blocked	eicar.zip
X-Violation <num- ber>-ThreatName</num- 	A name describing the threat	Malware
X-Violation <num- ber>-ProblemID</num- 	Currently 0 returned for all threats	0



Header Name	Description	Example
X-Violation <num- ber>-ResolutionID</num- 	0: File was not repaired	
	2: Violating part was removed	

5.2.2. Integration using REST API

File scan requests are sent via REST API requests to Application Security application and the response consists of pulled data related to the verdict.

Post to the Scanner URL

The URL structure required for sending requests to the Scanner is based on the Application Security deployment and whether the content encoding of the files in the REST API is defined with or without base64 encoding.

Sending files in base64 mode:

When sending the file with base64 encoding, enter the file in the request body and use one of the following URLs:

• Application Security with enabled SSL option:

https://<Application Security Container IP>:443/scan/base64

Application Security with disabled SSL option (NO_SSL=true):

http://<Application Security Container IP>:443/scan/base64

Sending files in binary mode:

When sending the files in binary mode (without base64 encoding), enter the file in the request body of the API request and use one of the following URLs:

• Application Security with enabled SSL option:

```
https://<Agentless IP>:443/scan/binary
```

Application Security with disabled SSL option (NO_SSL=true):

http://<Agentless IP>:443/scan/binary

Headers

The Post request should include the following header:



Content-Type: application/octet-stream

Example:



Where:

Entry	Description
https://localhost/scan/binary	URL to which the request is sent
-H "Content-Type: applica- tion/octet-stream	Header for Content-Type
data-binary @eicar.exe	Sends the binary data (i.e., contents of the 'eicar.exe' file) in the request body

When the scan is completed, you will receive a JSON response with the scan verdict. See "REST API scan responses".

5.2.2.1. REST API scan responses

Field	Descrip- tion	Example Value	Comments
verdict	File scan verdict	Malicious	In case the ver- dict is a failure ver- dict (Unsupported, Timeout, Classifica- tion Failed) some fields, like severity, file_type, scan_du- ration, may not be available. Supported values: Malicious Benign Unsupported File Type Unsupported File Size
			Failed Timeout
<pre>sub- mit_time_in_milli- seconds</pre>	Local time on the Ap- plication Security Connector when the request was sub- mitted	1589284291800	N/C



Field	Descrip- tion	Example Value	Comments
severity	Threat se- verity This is not included in the re- sponse for benign files.	VERY_HIGH	 Possible values: VERY_LOW LOW MODERATE HIGH VERY_HIGH
scan_dura- tion_in_microsec- onds	Time in microsec- onds to complete the classi- fication	17159	
malware_family	Deep Clas- sification of the file. If multiple exist, the primary is returned. This is not included in the re- sponse for non-PE or benign files.	BACKDOOR	 Possible values: RANSOMWARE BACKDOOR DROPPER PUA SPYWARE VIRUS WORM





Field	Descrip- tion	Example Value	Comments
file_type	CionFile for- mat of the scanned filePE64FileType	 Possible values: Other Macho32File- Type Macho64File- Type 	
			 MachoFATFile- Type XarFileType TarFileType PDFFileType DMGFileType DMGFileType RTFFileType OTFFileType OfficeFileType ZipFileType SevenZipFile- Type EICARType EICARType PE32FileType PE64FileType SWFFileType SWFFileType TIFFileType TIFFFileType





Field	Descrip- tion	Example Value	Comments
			 JarFileType OOXMLFileType OLEInOOXMLFileType GzipFileType
file_size_in_bytes	Size of the scanned file	2465280	
file_hash	Sha256 hash of the mali- cious/ scanned file	11acded2db9cf70590 653684c085 1f8182f3eebcd5ba1db 41d531ca13cef5fe2	
scan_guid	Unique identifier for this scan	1589284291800.0352	
container_hash	If the scanned file is a container (like zip), hash of the con- tainer, and not the mali- cious file	1e0faca8e6847e1b0fe 7c2a7131254027cc38 e8489840bf9e5355ef3 b00c836b	
event_description	An explan- ation of the event	Office file identified as malicious	



Field	Descrip- tion	Example Value	Comments
additional_of- fice_data	List of val- ues for different compo- nents in the docu- ment. 1 means the docu- ment con- tains this compo- nent	{"vba": 1, "swf": 0, "load_external_object": 0, "dde": 0, "xl4_macros": 0, "activex": 0}	 When the value is 1, the document contains the fol- lowing: VBA: VBA mac- ro SWF: Adobe Flash object Reference to an external object (RELS) DDE object XL4 macros (old type of macros) Embedded Ac- tiveX object

Example 5. Example response for a malicious PE file: {"submit_time_in_milliseconds": 1658926425556, "scan_guid": "1658926425556.0800", "file_type": "PE32FileType", "file_size_in_bytes": 261120, "file_hash": "7127eb5e1bb1aa5ff98d4eb56380627aa81b5f6d3b6f854242d6f02d2cd636cc", "scan_duration_in_microseconds": 13564, "verdict": "Malicious", "severity": "VERY_HIGH", "malware_family": "BACKDOOR", "event_description": "File identified as backdoor"}



```
Example 6. Example response for a malicious non-PE file:
{"submit time in milliseconds": 1658926494264,
"scan guid": "1658926494264.0912",
"file type": "OFFICEFileType",
"file size in bytes": 30008687,
"file hash": "37d1dfad-
ba1b526cbe4a1bc57ba178f25f20e18eba438b6d96361b337a30ee7c",
"scan duration in microseconds": 38,
"additional office data": {
"vba": 1,
"swf": 0,
"load external object": 0,
"dde": 0,
"xl4 macros": 0,
"activex": 0},
"verdict": "Malicious",
"severity": "HIGH",
"event description": "Office file identified as malicious"}
```

5.3. Client deployment validation

Once D-Clients have been deployed in your organization, the Management Console **Device List** screen displays the progress of the deployments and installations on your devices. Once you have deployed to several devices, we recommend to go to the **Device List** to confirm deployment, by tracking device registrations.

The D-Client Console for Windows and macOS also displays the progress of the installation, as well as the status of the D-Client. The messages are as follows:

• Setup in progress — Configuration files have not been downloaded completely.

deep instinct

- **Full scan in progress** D-Client is installed and performing the initial full scan. After the initial full scan is completed, the message changes to Protection enabled.
- **Protection enabled** D-Client is installed and protecting the device, even when offline.
- **Protection disabled** D-Client is installed, and protection has been disabled.
- **Device isolated from network** D-Client is installed, but the device has been isolated from the network by the administrator.
- **Offline** Device is currently not connected with the D-Appliance.
- **Online** Device is connected with the D-Appliance.
- **Setup error** An error has occurred during the setup.

5.3.1. EICAR test

After installing the D-Client on a Windows or macOS device, it is recommended to test that the software was installed properly. A safe way to test the D-Client is by simulating a virus on the device. To simulate a virus, use the test file from the European Institute for Computer Antivirus Research (EICAR). This file is not malicious, but should be detected as a malware when the D-Client has been installed successfully.

There are two methods to acquire a test file:

- Download a test file from EICAR. A test file can be downloaded from the EICAR website at https://www.eicar.org.
- Create a test file, as follows:
 - 1. Using a simple text editor, open a new file, and type or copy the following:

X5O!P%@AP[4\PZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*

Note that the third character is the capital letter "O" and not the zero digit.

2. Save the file (with any name). The file name is not relevant.

Once this file has been downloaded or created, Deep Instinct will identify the test file as malicious and an event is created in the Management Console. This confirms that D-Client has been installed and is communicating with the D-Appliance.



6. Uninstalling D-Client

When a device is no longer relevant to your organization (e.g, deactivated) the D-Client may be uninstalled from the device. You can uninstall the D-Client from the Management Console or from the devices either using a deployment tool or manually:

- "Uninstalling D-Client from the Management Console"
- "Uninstalling D-Client from the device"

Once the D-Client has been uninstalled, the following occurs:

- As the default, uninstalled devices are not displayed in the Device List. However, the Device List can display these devices, by displaying devices with an Uninstalled status.
- On Windows and macOS devices, the D-Client is uninstalled.
- When the Android D-Client is remotely uninstalled using the Management Console, the D-Client returns to a pre-registration state.
- The license is released, and the number of used licenses decreases accordingly. This can be viewed from the License Usage screen.

6.1. Uninstalling D-Client from the Management Console

The Management Console includes an **Uninstall** feature that allows the removal of the D-Client remotely from any device with which it is currently communicating.

To uninstall the D-Client from a device, using a single entry:

- 1. Select Assets \rightarrow Device List Device List from the Management Console Navigation pane.
- 2. Right-click the device, on which the D-Client is installed and then select **Uninstall D-Client**. A confirmation dialog appears.dialog box opens to confirm your request.

deep instinct



3. Click Uninstall. The Deployment Status for the device changes to **Pending Uninstall** and the device is instructed to uninstall the D-Client. After the D-Client is uninstalled, the status changes to **Uninstalled**.

To uninstall the D-Client from several devices, using multiple entries:

1. Device List from the Management Console Navigation pane.Assets → Device ListSelect Select Devices > Device List from the left pane to open the Device List.

dəsp instinct	Assets	> Device List								dev 🤈 🛱 🕲
28 Dashboard	(2324	items)						Actions *	License Usage	
Monitor	-	Device Name	Deployment Status	Connectivity Status	License Status	Deployment Status Last Lin	Platform	D-Clier Edit tag	tress	Device Group
Policy			-			· · · · · · · · · · · · · · · · · · ·	-	Collect log	5	
⊥o Assets								Isolate dev	ices	
<u>의</u> , Tenants			Deployed Successfully	Online	Activated	12/07/2022 13:16:08	Windows	3.4.2.3 Disable D-0	Clients	
I Reports			Deployed Successfully	Online	Activated	12/07/2022 13:15:19	Windows	3.4.2.3 Uninstall D	Clients	
約: Settings			Deployed Successfully	Online	Activated	09/12/2022 09:57:14	Windows	3.4.2.29		
igs occurringo			Deployed Successfully	Online	Activated	12/18/2022 13:16:18	macOS	3.4.2.146		
			Deployed Successfully	Online	Activated	12/18/2022 13:53:05	macOS	3.4.2.146		
			Deployed Successfully	Online	Activated	12/18/2022 13:09:12	macOS	3.4.2.144		
			Deployed Successfully	Online	Activated	12/15/2022 09:53:18	Windows	3.4.2.35		
			Deployed Successfully	Online	Activated	12/06/2022 20:22:25	Windows	3.4.2.35		
			Deployed Successfully	Online	Activated	12/07/2022 15:45:04	Windows	3.4.2.35		
			Deployed Successfully	Online	Activated	12/07/2022 16:17:22	Windows	3.4.2.35		
			Deployed Successfully	Online	Activated	12/18/2022 13:23:03	macOS	3.4.2.144		
			Deployed Successfully	Online	Activated	12/18/2022 12:17:58	Application Security	3.4.2.205p		-
			Deployed Successfully	Online	Activated	12/12/2022 12:07:07	Windows	3.4.2.35		
			Pending Uninstall	Online	Activated	11/21/2022 14:18:20	Windows Servers	3.4.2.30		
			Deployed Successfully	Online	Activated	12/18/2022 13:53:02	macOS	3.4.2.144		
			Deployed Successfully	Online	Activated	12/07/2022 16:31:14	Windows	3.4.2.35		
			Deployed Successfully	Online	Activated	12/18/2022 13:22:10	macOS	3.4.2.146		
			Deployed Successfully	Online	Activated	11/24/2022 11:24:11	Windows	3.4.2.34		
			Deployed Successfully	Online	Activated	12/11/2022 11:00:44	Application Security	3.4.2.204p		
	25	50 100 150								

- 2. Select the devices for which you want to uninstall the D-Client. The Actions Icon Actions appears in the header of the table.
- 3. Click Actions (appears on the top-right above the table) and select Uninstall D-Client. A confirmation dialog appears.



Uninstall D-Clients	
Are you sure you want to uninstall the D-Client from 2 se	lected devices?
Cancel	Uninstall

4. Click **Uninstall** . The Deployment Status for each device changes to Pending Uninstall and each device is instructed to uninstall the D-Client. After the D-Client has been uninstalled, the status changes to Uninstalled for each device.

6.2. Uninstalling D-Client from the device

6.2.1. Uninstall Windows D-Client

The process to uninstall D-Client from Windows devices can be performed locally, or remotely using a Windows deployment tool. The options are as follows:

Remote uninstall from the Management Console

Remote uninstall using SCCM

Remote uninstall using GPO

Manual uninstall

6.2.1.1. Uninstall D-Clients with SCCM

System Center Configuration Manager (SCCM) is a Microsoft management tool that can be used to uninstall D-Clients on multiple Windows devices. The following procedure is based on using SCCM 2012.

The D-Client uninstall process using SCCM requires the following:

- Deep Instinct Windows EXE installation file. File may be downloaded from the Windows Deployment Resources screen.
- Create a package to uninstall D-Clients
- Deploy the D-Client uninstall package

Creating a Package to Uninstall D-Clients

To create a package to uninstall D-Clients:

deep instinct

- 1. Download the installation file from the Windows Deployment Resources screen.
- 2. Save the installation file to a location where all the organization's Windows devices have access.
- 3. Start Microsoft System Center Configuration Manager.
- 4. In the Configuration Manager console, click Software Library.
- 5. In the Software Library workspace, expand Application Management.
- 6. Right-click Packages and click Create Package. The Create Package and Program Wizard opens. Perform the following:

Software Library	<
 Øverview 	<u> </u>
 Application Management 	
Applications	
Packages	
📝 Approval Requests	
[]‡]] Global Conditions	
🗮 App-V Virtual Environments	E
🎨 Windows Sideloading Keys	
Plication Management Policies	
 Software Updates 	
🗟 All Software Updates	
🕣 Software Update Groups	
💽 Deployment Packages	
😭 Automatic Deplovment Rules	-
ssets and Compliance	
Software Library	
Monitoring	
Administration	



1	Create Package and Program Wizard	x
Package		
Package Program Type Standard Program Requirements Summary	Specify information about this package Enter a name and other details for the new package. To take full advantage of new features that include the Application Catalog, use an application instead.	
Progress Completion	Name: DeepInstinct3.0(Uninstall) Description:]]
	Language: en ⊻ersion: 3.0 ✓ Inis package contains source files Sourge folder: \\servemame\sharename\path]
	< Previous Next > Summary Cancel	

- a. Enter the name of the package.
- b. As an option, enter the description, manufacturer, language, and/or version of the package. It is recommended to enter the version number for version control.
- c. Select This package contains source files.
- d. Click **Browse**. Go to the folder where the installation file is located and select the folder.
- e. Click Next.





7. Select **Standard program** in the left pane. Click **Next** and perform the following:



1	Crea	Create Package and Program Wizard							
Standard Progra	m								
Package Program Type Standard Program	Specify informati	ion about this standard program							
Requirements Summary Progress Completion	Name: Command line: Startup folder: Run: Program can run: Run mode: Allow users to view Drive mode: Reconnect to distri	DeepInstinct3.0(Uninstall) Installer.exe /x PASSWORD1! Installer.exe /x PASSWORD1! Normal Normal Only when a user is logged on Run with administrative rights r and interact with the program installation Runs with UNC name bution pgint at log on							
		< Previous Next > Summary Cance	I						

- a. Enter the name of the D-Client installation file.
- b. Type the following command in the Command line:

<installation file> /x <password>

Where:

- <installation file> = File name for the appropriate installation file. To enter the path and file name, click Browse and select the file from the folder.
- <password> = Uninstall password, as defined in the relevant Windows Device policy. if the Windows devices were never in communications with the D-Appliance, the defined Uninstall password was not received and the initial Uninstall password must be used. For the initial password, please contact Deep Instinct Support.

For example: installer.exe /xPASSWORD!

c. Change Run Mode to **Run with administrative rights** and click **Next**.



0	Create Package and Program Wizard	x
Requirements		
Package Program Type Standard Program	Specify the requirements for this standard program	
Requirements	□ <u>R</u> un another program first	
Progress Completion	Package: Browse Program: ✓	
	<u>Always run this program first</u> Platform requirements	_
	This program can run on any platform This program can run only on specified platforms	
	All Windows RT All Windows RT 8.1 All Windows 10 Professional/Enterprise and higher (32-bit) All Windows 10 Professional/Enterprise and higher (64-bit) All Windows 7 (64-bit) All Windows 8 (64-bit) All Windows 8 (64-bit) All Windows 8 (64-bit) Windows 8 (64-bit) Windows 8.1 (64-bit) Windows Embedded 8 Industry (64-bit) Windows Embedded 8 Standard (64-bit) Windows Embedded 8.1 Industry (64-bit)	
	Estimated disk space:	•
	Maximum allowed run time (minutes):	
	< <u>P</u> revious <u>N</u> ext > <u>S</u> ummary Cance	I

8. Click **Next** and a summary of the package settings are displayed.



1	Create Package and Program Wizard
Summary	
Package Program Type Standard Program Requirements Summary	Confirm the settings Details: General:
Progress Completion	Central: Plan:: Name: Description: 9. Version: 3.0 Publisher: Deeplnstinct 1. Language: en Source files: \secondary en Source files: \secondary en Always obtain files from the source folder Program: Program: P. Name: DeepInstinct3.0(Uninstall) Command line: Installer.exe /x PASSWORD1! Start in: Bun mode: Run mode: Run with administrative rights Program can run: Only when a user is logged on Drive mode: Runs with UNC name Requirements: Platforms supported: Any Platforms supported: Any Naximum allowed runtime(minutes): 120 To change these settings, click Previous. To apply the settings, click Next.
	< <u>Previous</u> <u>Next</u> <u>Summary</u> Cancel

9. Click **Next**. A progress bar and then a message appears to indicate that the wizard completed successfully.





5	Create Package and Program Wizard	x
Completion		
Package Program Type Standard Program Requirements Summary	The Create Package and Program Wizard completed successfully Details:	
Progress Completion	 Success: General: Name: Deepinstinct3.0(Uninstall) Description: Version: 3.0 Publisher: DeepInstinct Language: en Source files: \Servername\sharename\path Always obtain files from the source folder Success: Program Type: Standard Program Success: Program: Name: DeepInstinct3.0(Uninstall) Command line: Installer.exe /x PASSWORD1! Start in: Run: Normal Run: Normal Run mode: Run with administrative rights Program can run: Only when a user is logged on Drive mode: Runs with UNC name Success: Requirements: Platforms supported: Any Maximum allowed runtime(minutes): 120 	×
	< Previous Next > Summary	Close

10. Click **Close** and the Deep Instinct package appears in the list of packages.

Folder Tools System Center Configuration Mar	nager (Connected to DIP - De	eepinstinct)								- 8 ×
Home Folder										^ 🔞
Create Create Package Import Package from Definition Create Create Ackage Search Search	ontent File Package	Deploy Distr Cor	ribute ntent Dis Deployme	Update tribution Points	Move Move	Set Securit Scopes Classify	Properties			
🗧 🔶 🕫 👔 🔪 > Software Library > Overview > Application Management > Packages										
Software Library 4	Packages 5 items									
4 @ Overview	Search								🗙 🔎 Search	Add Criteria 🔻
4 🦳 Application Management	Icon Name			Programs	Manuf	acturer	Version	Language	Package ID	
Applications	Configuration Manager	Client Package		0	Micro	soft Corpo		99-	DIP00002	
R Packages	User State Migration To	ol for Windows	8.1	0	Micro	soft Corpo	6.3.9600.17237		DIP00001	
Approval Requests	DLP DLP			1	Forcel	Point		en	DIP00050	
If Global Conditions	3.0.0.5un			1	Deepl	nstinct	3.0.0.5	en	DIP00051	
App-V Virtual Environments	DeepInstinct3.0(Uninst	all)		1	Deepl	nstinct	3.0	en	DIP00053	
 Windows Sideloading Keys Application Management Policies Software Updates Operating Systems 			 Man Crea Crea Crea Expc Refr Dele 	age Access Account: ate Prestaged Conter ate Program ort esh esh	s nt File	F5 Delete	_			
	DeepInstinct3.0(Uninstall)		🔶 Dep	loy						*
🕵 Assets and Compliance	Package Properties		Disti	ribute Content					alatad Objects	*
Software Library	Package Properties			ate Distribution Poin	its			'	Related Objects	
	Package ID: D Manufacturer: D	PO0053	Mov	re .			 Success: In Progress 	0 ss: 0	ontent Status	E
Monitoring	Version: 3	.0	lo Set 1	Security Scopes			Failed: 0	0		
Administration	Language: ei	n	🔄 Prop	perties						
•	Current Destaura	-*-		U	Targeteo	(Last Update	: 3/8/2017 3:00 AN	/1)		*
Ready	Summary Programs Deployme	111.5								
🗧 占 🛛 🚞 🔍 🖉 🗈									• 18 19 (3:01 AM 3/8/2017

deep Instinct

Deploying the D-Client Uninstall Package

To deploy the uninstall package using SCCM:

- 1. Start Microsoft System Center Configuration Manager.
- 2. In the Configuration Manager console, click Software Library.
- 3. In the Software Library workspace, expand Application Management.
- 4. Click Packages . The Packages list appears.

Folder Tools System Center Configuration Man	ager (Connected to DIP - D	eepinstinct)								- 8 ×
Home Folder										^ 🔞
Create Package Import Package from Definition Create Searches - Create Searches -	ounts ontent File Create Program Delete	Deploy Dist Cc	ribute ntent Distri Deployment	Update oution Points	Move Se Move	et Security Scopes Classify	Properties Properties			
← → ▼ 🛐 \ → Software Library → Overview → Application	Management > Packages									- 2
Software Library <	Packages 5 items									
4 @ Overview	Search								🗙 🔎 Search	Add Criteria 🔻
Application Management	Icon Name			Programs	Manufactu	irer	Version	Language	Package ID	
Applications	Configuration Manage	r Client Package		0	Microsoft	Corpo			DIP00002	
Packages	🛐 User State Migration Te	ool for Window	s 8.1	0	Microsoft	Corpo	6.3.9600.17237		DIP00001	
Approval Requests	DLP			1	ForcePoint	nt		en	DIP00050	
[4] Global Conditions	3.0.0.5un			1	DeepInstir	nct	3.0.0.5	en	DIP00051	
Rop-V Virtual Environments	DeepInstinct3.0(Unins	stall)	-	1	DeepInstir	nct	3.0	en	DIP00053	
 Windows Sideloading Keys Application Management Policies Software Updates Operating Systems 			Manag Create Create Export Refrest	e Access Account: Prestaged Conter Program	s nt File I	F5				
			A Delete			Delete				
	DeepInstinct3.0(Uninstall)		🔶 Deploy							*
Assets and Compliance			Distrib	ute Content						*
	Package Properties		1 Update	Distribution Poin	nts			F	elated Objects	
Software Library	Package ID:	DIP00053	🔒 Move				Success:) • 0	🐻 Content Status	Е
Monitoring	Version:	3.0	log Set Sec	curity Scopes			Failed: 0	0		
Z Administration	Language:	en	Prope	ties						
•	Summary Programs Deploym	ents		U	Targeted (Las	st update:	3/8/2017 3:00 AN	1)		Ŧ
Ready		e								
🗧 占 🛛 📋 🔍 🥥 🗈									- 18 12 (3:01 AM 3/8/2017

5. Right-click the Deep Instinct uninstall package and click Deploy. The Deploy Software Wizard opens.



•	C	Deploy Software Wizard
General		
General Content Deployment Settings	Specify general info	ormation for this deployment
User Experience	Software:	DeepInstinct3.0(Uninstall)
Distribution Points	Collection:	Browse
Summary Progress Completion	Use default distribution	n point groups associated to this collection
	Comments (optional):	
		< Previous Next > Summary Cancel

6. Click Browse. Select the Device Collection for uninstalling D-Clients and click OK.

deep instinct

	Select Collection	
Device Collections	✓ Filter	ç.
Root	Name	Member Count
	🗳 All Desktop and Server Clients	71
	Services 💞 All Mobile Devices	0
	🗳 All Systems	183
	🗳 All Unknown Computers	2
	💕 Deep_Full	48
	🗳 Deep_phase1	5
	🔮 Deployment_Phase1	0
	Seployment_phase1b	0
	💞 DI_Uninstall	0
	Salesforce	5
	💞 Test_uninstall	0
	🥩 Uninstall_1.5.30.0	0
	💞 Uninstall 1.6.A20	2
	💞 Uninstalling_Agent	0
		OK Cancel
		Calicer

7. Click **Next** and then click Add+Distribution Point and select the distribution points for the content destination. This is typically the SCCM server.



		Deploy Software Wi	zard			x
Content						
General	Specify the cont	ent destination				
Content						
Deployment Settings						
Scheduling	Distribution points or di	stribution point groups that the	content has been distributed to):		
User Experience						_
Distribution Points	Name	Туре				_
Summary		l here are no it	ems to show in this view.			
Progress						
Completion						
			•			
	Additional distribution p	oints, distribution point groups,	and the distribution point group	os that are cur	rently associated	
	With collections to distr	Ibute content to:				
	Filter			P	<u>A</u> dd	•
	Filter Name	Description	Associations	P	<u>A</u> dd	•
	Filter Name SCCM.DEEP	Description Distribution point	Associations	9	<u>A</u> dd	•
	Filter Name SCCM.DEEP	Description Distribution point	Associations	2	<u>A</u> dd <u>R</u> emove	
	Filter Name SCCM.DEEP	Description Distribution point	Associations	9	<u>A</u> dd <u>R</u> emove	•
	Filter Name SCCM.DEEP	Description Distribution point	Associations	9	Add Remove	
	Filter Name SCCM.DEEP	Description Distribution point	Associations	9	Add Remove	•
	Filter Name SCCM.DEEP	Description Distribution point	Associations	9	Add Remove	
	Filter Name SCCM.DEEP	Description Distribution point	Associations	9	<u>A</u> dd <u>R</u> emove	
	Filter Name SCCM.DEEP	Description Distribution point	Associations	2	<u>A</u> dd <u>R</u> emove	

8. Click **Next** and make this a required installation, by selecting Required in the Purpose box.





	Deploy Software Wizard	x
Deployment Set	ttings	
General Content Deployment Settings Scheduling User Experience Distribution Points Summary Progress Completion	Action: Install Purpose: Required Pre-deploy software to the user's primary device Send wake-up packets Allow clients on a metered Internet connection to download content after the installation deadline, which might incur additional costs	
	Care	

9. Click **Next** and the Scheduling dialog box opens.



<u>م</u>	Deploy Software Wizard
Scheduling	
General Content Deployment Settings	Specify the schedule for this deployment
Scheduling User Experience Distribution Points	This program will be available as soon as it has been distributed to the content servers unless it is scheduled for a later time below. For required applications, specify the assignment schedule.
Summary	✓ Schedule when this deployment will become available:
Progress	2/15/2017 🗐 ▼ 4:43 AM 💭 🗌 UTC
Completion	Schedule when this deployment will expire:
	2/15/2017 🗐 ▼ 4:43 AM 💭 🔲 UIC
	Assignment schedule: 🕖 New Edit Delete
	There are no items to show in this view.
	Berun behavior: Always rerun program v
	< Previous Next > Summary Cancel

- 10. Select Schedule when this deployment will become available.
- 11. Click New and the Assignment Schedule dialog box opens.

Assignment Schedule	x
O Assign to the following <u>s</u> chedule: Occurs on 2/15/2017 4:44 AM	
Schedule Assign immediately after this event:	
As soon as possible 🗸	
OK Cancel	

12. Select Assign immediately after this event and select As Soon As Possible from the dropdown box.



13. Click **OK** and As Soon As Possible is added to the assignment schedule.

>	Deploy Software Wizard	x
Scheduling		
General Content Deployment Settings	Specify the schedule for this deployment	
Scheduling User Experience Distribution Points	This program will be available as soon as it has been distributed to the content servers unless it is scheduled for a later time below. For required applications, specify the assignment schedule.	
Summary Progress Completion	✓ Schedule when this deployment will become available: 2/16/2017 ✓ 3:38 AM ✓ UTC ✓ Assignment schedule: New Edit Delete	
	< <u>P</u> revious <u>N</u> ext > <u>S</u> ummary Cance	

14. Click **Next** and the User Experience dialog box opens.



*	Deploy Software Wizard	x
User Experience		
General Content Deployment Settings Scheduling <u>User Experience</u> Distribution Points Summary Progress Completion	Specify the user experience for the installation of this software on the selected devices Notification settings: Allow users to run the program independently of assignments When the scheduled assignment time is reached, allow the following activities to be performed outside the maintenance window: Software installation System restart (if required to complete the installation) Write filter handling for Windows Embedded devices Commit changes at deadline or during a maintenance wingow (requires restarts) If this option is not selected, content will be applied on the overlay and committed later.	
	< <u>P</u> revious <u>N</u> ext > <u>S</u> ummary Cancel	

15. Click **Next** and the Distribution Points dialog box opens.



•	Deploy Software Wizard
Distribution Pc	pints
General Content Deployment Settings Scheduling User Experience Distribution Points Summary Progress Completion	Specify how to run the content for this program according to the type of boundary the client is connected to Select the deployment option to use when a client is connected within a fast (LAN) network boundary. Deployment options: Download content from distribution point and run locally Select the deployment option to use when a client is within a slow or unreliable network boundary, or when the client uses a fallback source location for content. Deployment options: Download content from distribution point and run locally Select the deployment option to use when a client is within a slow or unreliable network boundary, or when the client uses a fallback source location for content. Deployment options: Download content from distribution point and run locally Aligw clients to share content with other clients on the same subnet This option allows clients that use Windows BranchCache to download content from on-premises distribution points. Content downloads from cloud-based distribution points can always be shared by clients that use Windows BrenchCache
	Allow clients to use a fallback source location for content < Previous

- **16. In both Deployment options lists, select** Download Content From Distribution Point And Run Locally.
- 17. Click **Next** and a summary of the deployment settings are displayed.



\$	Deploy Software Wizard	x
Summary		
General Content Deployment Settings Scheduling User Experience Distribution Points Summary Progress Completion	Details: Deneral 9 Software: DeepInstinct3.0(Uninstall) 0.01 Election: Deep_Full (Member Count: 48) 0.02 Getail distribution point groups and 0.02 Getail distribution point groups and point and 0.02 Getail distribution point groups and point and point distribution point groups and distribution and and distribution point groups and distribution and and distribution point groups and distribution and distribution point groups and distribution and distribution point groups and distribution andistribution and distribution and distribution and distribution an	4
	< <u>P</u> revious <u>N</u> ext > <u>Summary</u> Ca	ncel

18. Click **Next**. A progress bar and then a message appears to indicate that the wizard completed successfully.




19. Click **Close** to exit the wizard.

6.2.1.2. Uninstall D-Client with GPO

Group Policy Management Console (GPMC) is a Microsoft management tool that can create a Group Policy Object (GPO) to uninstall D-Clients on your organization's Windows devices.

The D-Client uninstall process using GPO requires the following:

- Deep Instinct Windows EXE installation file. File may be downloaded from the from the Windows Deployment Resources screen.
- Uninstall batch file for GPO
- Uninstall using GPO

Create an Uninstall Batch File (for GPO only)

Prior to uninstalling the D-Client with a Windows deployment tools, an uninstall batch file must first be created. The batch file can be created with a text editor, such as Notepad. The following describes the procedure to create the uninstall batch file.

deep instinct

To create the uninstall batch file:

- 1. Save the installation file to a location where all the Windows devices have access.
- 2. Open the text editor.
- 3. Type the following command in the first line of the file:

<exe path><installation file> /x <password>

Where:

- <exe path> Path for the appropriate installation file, where all the Windows devices have access.
- **<installation file>** File name for the appropriate installation file.
- <password> Uninstall password, as defined in the relevant Windows Device policy. if the Windows devices were never in communications with the D-Appliance, the defined Uninstall password was not received and the initial Uninstall password must be used. For the initial password, please contact Deep Instinct Support.
- 4. Save the file with the name **uninstall.bat**.

Example 7. Co	mmand example	
	uninstall - Notepad	- • ×
<u>F</u> ile <u>E</u> dit F <u>o</u> rmat	t <u>V</u> iew <u>H</u> elp	
\\tgdc1\compa	ny\Installer.exe /x UninstallPas	sword1!
<		en e
 exe path = \\t, installation fi 	gc1\company\ ile = Installer.exe	
password = UninstallPassword1!		

5. Copy the batch file to the same location the installation file was saved and to the location where the Windows deployment tool has access.

Uninstall D-Clients using GPO

To uninstall D-Clients using GPO:

deep instinct

- 1. Create the uninstall batch file.
- 2. Save the uninstall batch file to the Startup Script folder.
- 3. Save the EXE and batch files to a location where all the organization's Windows devices have access.
- 4. Log on to the Domain Controller (DC) and start the Microsoft Group Policy Management Console (GPMC).
- In the GPMC tree, right-click the Organization Unit (OU) to which you want to deploy the D-Client and click Create a GPO in this domain, and Link it here to create a new GPO. The New GPO dialog box opens.

New GPO			×
Name:			
New Group Policy Object	N		
Source Starter GPO:	43		
(none)			•
		OK	Cancel

- 6. Type the name of the new GPO and click OK. The new GPO is now added to the list of Linked Group Policy Objects.
- 7. Right-click on the new GPO and click **Edit**.
- 8. In the GPMC tree, expand Policies and then expand Windows Settings.
- 9. Click Scripts (Startup/Shutdown) and double-click Startup. The Startup Properties dialog box opens.



St	artup Proper	ties	? X
Scripts PowerShell Scripts			
Startup Scripts f	or DI deploy		
Name	Parameters		
			Up
			Down
		[Add
		[Edit
			Remove
To view the script files stored the button below. Show Files	d in this Group Po	licy Object, pre	SS
	OK	Cancel	Apply

- 10. Click Add and the Add a Script dialog box opens.
- 11. Click **Browse** and select the uninstall batch file.

Add a Script	x
Script Name: uninstall.bat	Browse
Script Parameters:	
ОК	Cancel

- 12. Click **OK** to add the script.
- 13. Click **OK** and exit the Microsoft Group Policy Management Console. The D-Client is deployed on each device when the device restarts.



14. If you want to uninstall the D-Client immediately from a device, perform the procedure described in Apply GPO to Deploy D-Client Manually.

6.2.1.3. Manually Uninstall D-Client

The D-Client can also be uninstalled from each Windows device manually. This may be practical when only a few devices need D-Client to be uninstalled or for unmanaged devices.

To uninstall D-Client from a Windows device:

- 1. Save the installation file to a location where the Windows device has access.
- 2. Open the Command Prompt window as an administrator.
- 3. At the command prompt, type the following command:

<exe path><installation file> /x <password>;

Where:

- **exe path** Path for the appropriate installation file.
- **installation file** File name for the appropriate installation file.
- password Uninstall password, as defined in the relevant Windows Device policy. if the Windows device was never in communications with the D-Appliance, the defined Uninstall password was not received and the initial Uninstall password must be used. For the initial password, please contact Deep Instinct Support.

Example 8. Uninstall command

C:\Windows\system32> c:\users\administrator\downloads\Installer.exe /x 'UninstallPassword1!'

- exe path = c:\users\administrator\downloads\
- installation file = Installer.exe
- **password** = UninstallPassword1!



6.2.2. Manually Uninstall macOS D-Client

The D-Client can also be uninstalled from each macOS device manually. This may be practical when only a few devices need D-Client to be uninstalled.

To uninstall D-Client from a macOS device:

- 1. Open a Terminal window.
- 2. Type the following command in the command prompt:

sudo '/Volumes/Deep Instinct/installer.sh' -x '<password>'

Where: **password** = Uninstall password, as defined in the relevant macOS Policy.



7. D-Client upgrades

The process to upgrade the D-Client is an automatic process that applies the features available for each platform. When a new version of the D-Client becomes available, a notification is generated. For more information, see the following:

- Upgrading Windows, macOS and Linux D-Clients
- Upgrading D-Client for Windows VDI
- Upgrading Android, Chrome OS, iOS and iPadOS D-Clients

7.1. Upgrading Windows and macOS D-Clients

The upgrade process for Windows and macOS is automatically upgraded based on parameter Upgrade D-Client automatically in the device policies. It is recommended that you enable Upgrade D-Client automatically (in the applicable Policy) to take advantage of future enhancements, as they become available.

For macOS upgrades — additional permissions may be required. If required, the Deployment status for the device changes to Deployed with Warnings, a message also appears on the

macOS device and the Deep Instinct icon is displayed with a yellow indicator, 💐. To enable the missing permissions, follow the instructions in Enable Permissions from D-Client Console.



To upgrade macOS D-Clients prior to version 3.4.2, use on of the following methods:

- Upgrade the D-Client by performing a local installation using the CLI
- Upgrade the D-Client by performing a local installation using the Wizard
- Upgrade the D-Client by performing remote installations using Jamf

Using these methods, the installation process recognizes that an existing D-Client is installed and then performs the appropriate actions.

The list of available D-Client versions are displayed in the Management Console Release Notes screen. It displays the existing versions and the new version to which each version can be upgraded. For more information on the Release Notes screen, see the Administrator Guide.



7.2. Upgrading D-Client for Windows VDI

The upgrade process of the D-Client for VDI machines with Windows, requires the uninstall and installation of the D-Client from the Master image. The following procedure assumes the use of Microsoft Sysprep to assist with generalizing the virtual machine prior to saving the image.

To upgrade the D-Client on a VDI machine:

- 1. Boot up the latest master image.
- 2. Uninstall the D-Client, as follows:
 - a. Save the installation file to a location where the Windows virtual machine has access.
 - b. Open the Command Prompt window as an administrator from the virtual machine.
 - c. At the command prompt, type the following command:

```
<exe path><installation file> /x <password>
```

Where:

- exe path Path for the appropriate installation file
- installation file File name for the appropriate installation file. To enter the file name, click Browse and select the file from the folder.
- server address FQDN for the D-Appliance.
- password Uninstall password, as defined in the relevant Windows Device policy.

ΝΟΤΕ

If the Windows device was never in communications with the D-Appliance, the defined Uninstall password was not received and the initial Uninstall password must be used. For the initial password, please contact Deep Instinct Support.

Example 9. Uninstall command

```
c:\users\administrator\downloads\Installer.exe /xUninstallPass-
word1!
```

Where:

exe path = c:\users\administrator\downloads\



- installation file = Installer.exe
- password = UninstallPassword1!
- 3. Install the D-Client using the CLI command on the master image, as follows:
 - a. Download the new installation file from the Windows Deployment Resources screen.
 - b. Save the installation file to a location where the Windows virtual machine has access.
 - c. Open the Command Prompt window as an administrator from the virtual machine.
 - d. At the command prompt, type the following command:

<exe path><installation file> <server address> /token <installation
token> /vdi [/tag <tag>] [/disabled][/nfs] [/np]

Where:

Command Parameter	Description	Comments
<exe path=""></exe>	Path for the appropriate instal- lation file	N/C
<installa- tion file></installa- 	File name for the appropriate installation file.	To enter the file name, click Browse and select the file from the folder.
<installa- tion to- ken></installa- 	ID of the installation token, as displayed in the Windows De- ployment Resources screen	When installing in a system with MSP support, each tenant has a different installation to- ken ID. Therefore, each tenant requires a different master im- age.

Command Parameter	Description	Comments
<tag></tag>	Adds a tag associated with the deployed VDI machines	 Optional Device Tag must comply to the following: Maximum character length = 256 Case sensitive Valid characters: Letters (a-z, A-Z) Numbers (0-9) Spaces representable in UTF-8 Special characters: + -=: / @ Using rules — Device tags can be used with rules to automatically add machines to a Device Group. It can also be used for selecting and filtering devices in the Management Console. For more information, see the Administrator Guide.
/disabled	When /disabled is included, the D-Client is disabled during the installation. This allows the administrator to select when to initially enable the D-Client.	Optional
/nfs	Starts the D-Client without performing the initial full scan	Optional
/np	Enables the use of a network proxy server using the default proxy settings	Optional

Command Parameter	Description	Comments
/vdi	Required for installing the D- Client on a VDI machine	

Example 10. Install on VDI command

c:\users\administrator\downloads\Installer.exe

customer.deepinstinctweb.com /token 12345678 /vdi

Where:

- exe path = c:\users\administrator\downloads\
- installation file = Installer.exe
- server address = customer.deepinstinctweb.com
- installation token = 12345678

This installation performs specific action that also include unique actions for VDI installations, as follows:

- Uses a random registration code that is unique for each registration (clones of this machine will receive a new Device ID).
- Download the configuration file.
- Performs a full scan (unless the /nfs option was used)

Once the above is completed:

- Device ID is removed (this allows regeneration when the clone machines are spun up)
- Network service is disabled (this prevents re-registration)
- Network queues are emptied
- 4. After the full scan is completed and all that you want is included in the master image, run **sysprep** as follows:
 - a. Open the Command Prompt window, as an administrator from the virtual machine.
 - b. Run **sysprep**. At the command prompt, type the following command:



C:\Windows\System32\Sysprep\sysprep

The System Preparation Tool window opens.

System Preparation Tool 3.14		
System Preparation Tool (Sysprep) prepares the machine for hardware independence and cleanup.		
System Cleanup Action		
Enter System Out-of-Box Experience (OOBE) $\qquad \lor$		
Generalize		
Shutdown Options		
Shutdown 🗸		
OK Cancel		

- c. Select Enter System Out-Of-Box Experience (OOBE) from the dropdown box for the system cleanup action and then select Generalize.
- d. Select Shutdown from the dropdown box for the shutdown option.
- e. Click **OK** to generalize the machine and shut everything down to make the master image.



Once completed, do not use the master image. Clone the machine to prevent the services for Deep Instinct do not start again and communicate to the server. This ensures that a new SID (System ID) is generated each time a machine is cloned from the template, and no duplicates appear in the Management Console.



7.3. Migrating to a new Linux D-Client

To migrate to Linux D-Client version v4.0 from an older version:

- 1. Uninstall the old version (before running the installer) using one of the following methods:
 - "Uninstalling D-Client from the Management Console"
 - Manually Uninstall D-Client
- 2. Install the v4.0 Linux D-Client installer as described in Deployment to Linux Devices

During the migration process to the new version a new Device ID is created (previous one is not maintained).

7.4. Upgrading Android, Chrome OS, iOS and iPadOS D-Clients

All new Android and Chrome OS D-Client versions are placed in the Google Store, and all new iOS and iPadOS D-Client versions are placed in the App Store. All devices set to automatically update apps will be updated immediately when a new version is released. All others will need to update their D-Client from the Google Store or App Store.

To see the progress of the upgrades, display the D-Client Versions on the devices from the Device List or the Dashboard.

The list of available D-Client versions is displayed in the Release Notes Screen (see the Administrator Guide for more information).



8. Troubleshooting options

8.1. Debug log collection

The administrator has an option to collect and download D-Client Debug logs for Deep Instinct to assist in troubleshooting your devices. Once the Debug log has been downloaded, it can be viewed by the administrator or sent to Deep Instinct for debugging.

Downloading the debug file can be performed remotely from the Device List or locally from the device. For more information, see the Administrator Guide.

8.2. Disable/enable D-Client

After the D-Client has been installed, the D-Client may be disabled to eliminate its influence, while troubleshooting a problem on a Windows or macOS device. This can be performed remotely from the Device List or locally from the device. Once the problem is resolved, the D-Client can be enabled again. For more information, see the Administrator Guide.

8.3. Changing the Management Server address

The Management Server (D-Appliance) assigned to a D-Client is defined by the Management Server address. If needed for troubleshooting purposes (such as network connectivity issues) or server maintenance, you can locally change the assigned Management Server on your Windows, macOS, or Linux devices.

- "Changing the Management Server address on a Windows device"
- "Changing the Management Server address on a macOS device"
- "Changing the Management Server address on a Linux device"

8.3.1. Changing the Management Server address on a Windows device

To locally change the Management Server (D-Appliance) address on a Windows device

- 1. Save the installation file to a location where the Windows device has access.
- 2. Open the Command Prompt window as an administrator.





```
<exe path><installation file> /m <password> <server address> <instal-
lation token>
```

Where:

- exe path Path for the installation file
- installation file File name for the appropriate installation file
- password Uninstall password, as defined in the relevant Windows Device policy. If the Windows device was never in communications with the D-Appliance, the defined Uninstall password was not received and the initial Uninstall password must be used. For the initial password, please contact Deep Instinct Support.
- server address FQDN for the Management Server
- installation token ID of the installation token, as displayed in the Windows Deployment Resources screen

Example 11. Change Management Server address command

```
C:\Windows\system32>c:\users\administrator\downloads\Instal-
ler.exe /m UninstallPassword1! customer.deepinstinctweb.com
12345678
```

- exe path = c:\users\administrator\downloads\
- installation file = Installer.exe
- password = UninstallPassword1!
- server address = customer.deepinstinctweb.com
- installation token = 12345678

8.3.2. Changing the Management Server address on a macOS device

To locally change the D-Appliance address on a macOS device:

- 1. Download the installation file from the macOS Deployment Resources screen.
- 2. Save your configured installation DMG file to a location where the macOS devices has access.

deep instinct

- 3. Open a Terminal window.
- 4. Mount the DMG installation file. At the command prompt, type the following command.

open <path><DMG installation file>

Where:

- **<DMG installation file>** = downloaded DMG file name
- 5. Run the installation file. At the command prompt, type the following command.

sudo '/Volumes/Deep Instinct/installer.sh' -m '<password>'

<server address> <installation token>

Where:

- <password> = Uninstall password, as defined in the relevant macOS Device policy. If the macOS device was never in communications with the Management Server, the defined Uninstall password was not received and the initial Uninstall password must be used. For the initial password, please contact Deep Instinct Support.
- server address = FQDN of the Management Server
- installation token: ID of the installation token, as displayed in the macOS Deployment Resources screen
- server address = customer.deepinstinctweb.com
- installation token = 12345678



Example 12. Change Management Server address command

-m UninstallPassword1! customer.deepinstinctweb.com 12345678

Password:

Macbook-Pro:Desktop user\$

Where:

- path = /Users/user/Downloads/
- installation_file = 2.4.0.1_DeepInstinct_installer.dmg
- **password** = UninstallPassword1!
- server address = customer.deepinstinctweb.com
- installation token = 12345678
- System without MSP support

8.3.3. Changing the Management Server address on a Linux device

To locally change the D-Appliance address on a Linux device:

- 1. Open a Terminal window.
- 2. At the command prompt, type the following command:

sudo /opt/deepinstinct/bin/DeepCLI -m '<password>' <server address>

<installation token>

Where:

- password = Uninstall password, as defined in the relevant Linux Device policy. If the Linux device was never in communications with the D-Appliance, the defined Uninstall password was not received and the initial Uninstall password must be used. For the initial password, please contact Deep Instinct Support.
- server address; FQDN for the Management Server





 installation token: ID of the installation token, as displayed in the Linux Deployment Resources screen.

9. Glossary

Term	Description
ΑΡΤ	Advanced Persistent Threat – A sophisticated method of attack used to avoid detection that leverages the attack to new heights. This method of attack may also be split into several modules to further avoid detection. In some cases, it is a targeted attack to a specific entity.
ΑΤΑ	Advanced Threat Analysis – An additional threat analysis that can be initiated by the administrator on any PE file identified. It produces a report that displays a wide range of information to assist you in further analyzing malicious files. The analysis is performed on an isolated virtual machine and are performed on demand.
Benign	A benign software is harmless, which is the opposite of malware.
D-Appliance	Management and monitoring server, hosted in the cloud
D-Brain	The prediction model (D-Brain) is the result of the deep learning in the D-Lab, which detects the cyber threats on the devices.
D-Client	A lightweight client software installed on the device according to its platform (Windows, macOS, Linux, Android, Chrome OS, iOS or iPadOS).
Endpoint	Computerized equipment that is connecting to an organizational net- work and functions as part of this network, usually resides in the low end of the network tree (Smartphone, tablet, PC, laptop, etc.).
FQDN	Fully Qualified Domain Name – A complete and unique address for a specific host or computer. The FQDN usually consists of the hostname and the domain name (all domain levels).
GPO	Group Policy Object – A collection of settings for a defined group of users that is used with Microsoft's Group Policy feature. This feature pro- vides the centralized management and configuration for the Windows operating systems, applications, and users' settings in an Active Directo- ry environment.
Malware	An abbreviation for malicious software, which is any software/applica- tion used to disrupt a computer or a mobile device's operation, gather sensitive information, or gain access to private data.
MSP	Managed Service Provider – A service provider that delivers managed services. The MSP has direct oversight of the organization or system being managed.

Term	Description
SCCM	System Center Configuration Manager – A systems management soft- ware product developed by Microsoft for managing large groups of computers. It provides remote control, patch management, software distribution, operating system deployment, network access protection and hardware and software inventory.
UDID	Unique Device Identifier – A unique string assign to each mobile device that can be used to identify the device.
Zero-Day Threat	A threat that exploits an unknown computer security vulnerability. It is known as a "zero-day" because it is not publicly reported or announced before becoming active, leaving the software's author with zero days in which to create patches or advise workarounds to mitigate against its actions.

dəep Instinct

New York Global Headquarters

322 W 52nd Street Suite 2038 NYC, NY, 10101 USA

Phone: +1 212-981-2703

Tel Aviv

Tou-Towers 4 Yitzhak Sadeh Street Tel Aviv, 6777504 Israel

Phone: +972 3545-6600

United Kingdom

Highlands House Basingstoke Road Spencers Wood Reading RG7 1NT United Kingdom

Phone: +44 7810-553692

Japan

World Trade Center Building Level 17 World Trade Center Building South Wing, 2-4-1 Hamamtsu-cho, Minato-ku Tokyo, Japan 105-5117

Phone: +81-3-4567-2621



www.deepinstinct l contact@deepinstinct.com