



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	9
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
4.1.1. Required network ports	11
4.1.2. Plan the deployment in stages	15
4.1.3. Exclusions on antivirus software	16
4.2. Windows D-Client installation	17
4.2.1. Prerequisites	17
4.2.2. Remote deployment of Windows D-Client	23
4.2.3. Local Deployment of Windows D-Client	45
4.2.4. D-Client installation for Windows VDI	49
4.2.5. Installation error codes	54
4.3. Deployment to macOS Devices	55
4.3.1. macOS D-Client deployment	55
4.3.2. Enabling permissions from the D-Client console	104
4.3.3. macOS deployment resources	115
4.4. Linux D-Client installation	116
4.4.1. Linux deployment resources	116
4.4.2. Remote deployment with a Linux deployment tool	117
4.4.3. D-Client local installation with the CLI	118
4.5. Mobile D-Client installations	121
4.5.1. D-Client deployment with SOTI MobiControl	122
4.5.2. Local deployment for mobile D-Clients	127
4.6. Application Security deployment	174
4.6.1. Application Security deployment using a predefined Docker image	175
4.6.2. Application Security deployment using a customized Docker image	178
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 MERCHANTABILITY, 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 CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT 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 technical 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.

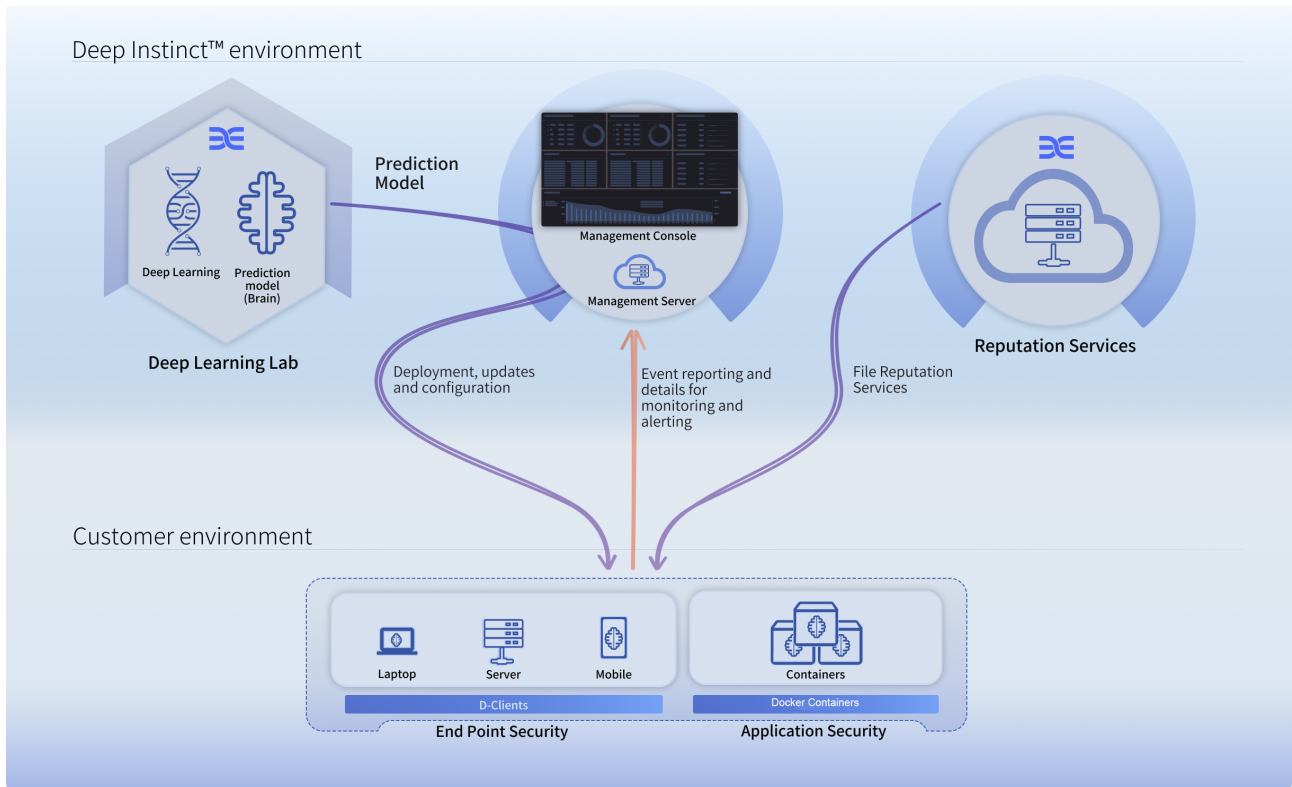
2. Introduction

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	<ul style="list-style-type: none"> ▪ 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 Framework	Version 3.5 or higher

Certificates	<p>When upgrading/installing the Windows D-Client without an internet connection you need to pre-install the following certificates:</p> <ul style="list-style-type: none"> ■ 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 <p><i>Note: All Microsoft-supported Windows versions typically contain these certificates, and D-Client installation automatically installs these certificates if they are missing (requires an internet connection).</i></p>
CPU	Dual-core CPU or faster
RAM	<p>Min. 2 GB</p> <p>Recommended: 4 GB</p> <p><i>Note: RAM must also meet OS minimum requirements.</i></p>
Hard drive	500 MB free disk space

3.2.2. macOS devices

macOS D-Client requirements

Operating system	<ul style="list-style-type: none"> ■ macOS Ventura (version 13) ■ macOS Monterey (version 12) ■ macOS Big Sure (version 11)
CPU	Dual-core CPU or faster

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

3.2.3. Linux devices

Linux D-Client requirements

Operating system	<ul style="list-style-type: none"> ■ 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 <p><i>*Operating system must be registered, and available subscriptions attached.</i></p> <p><i>**Ubuntu devices with GNOME require a restart after the D-Client installation is completed.</i></p>
CPU	Dual-core CPU or faster
RAM	<p>Min. 2 GB</p> <p>Recommended: 4 GN</p> <p><i>Note: RAM must also meet OS minimum requirements</i></p>
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 before installing the Linux Client.

RHEL 7 & RHEL 8

System	Package Name	Package Filename	Source Repository
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 Repository
Ubuntu 20.04	rpm	Default Ubuntu 20.04 repo
	libtomcrypt1	
	libtommath1	

System	Package Name	Source Repository
	curl	
	libmimetic0v5	
	minizip	
	libpython2.7	
Ubuntu 20.04 systems with GUI (Required in addition to the Ubuntu files listed for Ubuntu 20.04 systems)	python3	Default
	python3-pip	Default
	python3-tk	Default
	python3-pil	Default
	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	<ul style="list-style-type: none"> ■ Docker installed ■ Network connectivity — 1 Gbps Ethernet port or faster ■ IP forwarding enabled
--------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Docker container (per container)	Operating system	<ul style="list-style-type: none"> ■ 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 <ul style="list-style-type: none"> ■ Requirements may change depending on the total number of files that require scanning ■ Each CPU core can handle approximately 20 MB/second peak capacity for file scans
	RAM	16 GB or 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 Description	Source	Destination	Port(s)
Deep Instinct Management Server/SMTP Server	Management Server (D-Appliance)	SMTP Server	Configurable
Deep Instinct Management Server/Active Directory (AD) Server	Management Server (D-Appliance)	AD Server	Configurable
Administrators' connection to the Management Console	Management Console	Management Server	443
Reputation Services (D-Cloud) D-Cloud address: cloud-api.deepinstinctweb.com	Management Server (D-Appliance) D-Client	Reputation Services Engine (D-Cloud)	443

Communication Description	Source	Destination	Port(s)
<p>D-Client/Management Server (D-Appliance)</p> <p>Connection required for downloading configuration files and policy to the D-Clients as well as sending event notifications to the Management Server.</p>	<p>D-Client</p>	<p>Management Server (D-Appliance)</p> <p>FQDN examples for the Management Server:</p> <ul style="list-style-type: none"> ■ mycompany.customers.deepinstinct-web.com ■ apiv2-mycompany.customers.deepinstinct-web.com ("apiv2-<FQDN>") 	<p>443</p> <p><i>Note the following:</i></p> <ul style="list-style-type: none"> ■ <i>When installed, the D-Clients set the port to 443. If this port is not available, the port is set to 4339.</i> ■ <i>When port 443 is used, the connectivity needs to open to both the D-Appliance FQDN, and to "apiv2-<FQDN>".</i> ■ <i>When port 443 is used with macOS D-Clients, the connectivity also needs to open to "api-<FQDN>".</i> ■ <i>Once the port is set during installation, the D-Clients continue to use this port, including upgrades.</i>

Communication Description	Source	Destination	Port(s)
<p>Application Security / Management Server (D-Appliance)</p> <p>Connection required for registering with the Management Server, status reporting, and event notifications as well as downloading configuration files and policy updates.</p>	Application Security	<p>Management Server (D-Appliance)</p> <p>*Depending on the API version, requests are directed using one of the following DNS names (both return the same IP address):</p> <ul style="list-style-type: none"> ■ For API v1: mycompany.customers.deepinstinct-web.com ■ For API v2 ("apiv2-<FQDN>"): apiv2-mycompany.customers.deepinstinct-web.com 	443
REST API file scan requests	Custom app		Configurable
<p>Communication with Syslog Server</p> <p><i>Note: The port defined for this communication is allocated by your organization.</i></p>	Management Server (D-Appliance)	Syslog Server	Configurable
ICAP file scan requests	Custom app		Configurable

Communication Description	Source	Destination	Port(s)
Android D-Client/Management Server (D-Appliance) communication during deployment	Android D-Client	Management Server (D-Appliance)	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-Appliance)	7443
Management Console and Server screen-refresh functionality.	Management Console	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	<ul style="list-style-type: none"> ▪ C:\Program Files\DeepInstinct\ ▪ C:\ProgramData\DeepInstinct\ 	<ul style="list-style-type: none"> ▪ 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 Processes Policies to eliminate any possible conflict with Deep Instinct processes. For more information, see https://kc.mcafee.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/article.TECH183201.html .
Trend Micro	Files may be added to the Behavior Monitoring exception list to eliminate any possible conflict with Deep Instinct processes. For more information, see https://docs.trendmicro.com/en-us/enterprise/officescan-110-sp1-server/using-behavior-monit/behavior-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](#).

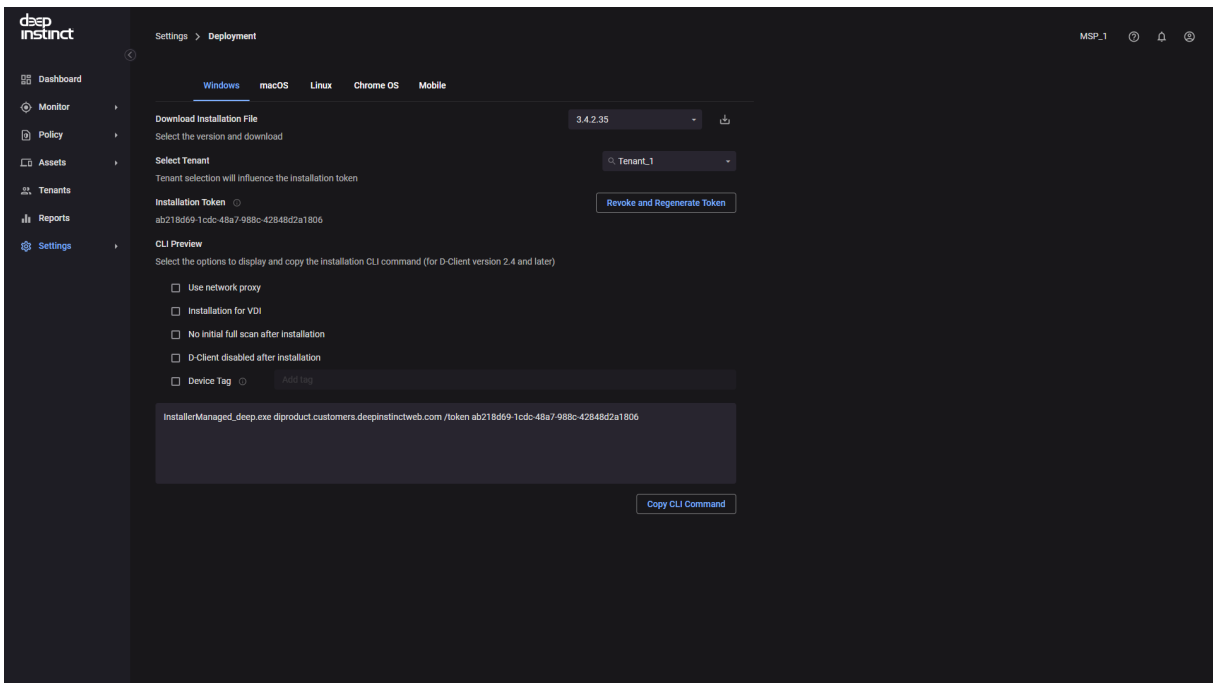
- **D-Client installation package** — download the Windows D-Client installation package from the Management Consoles' [Windows Deployment Resources](#) screen.


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](#) → [Deployment](#) → [Windows](#) .



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	<code><exe path><installation file> <server address> /token <installation token> [/tag <tag>] [/disabled] [/nfs] [/np /manualproxy <proxy url>:<proxy port>]</code>
Install the D-Client on a VDI machine	<code><exe path><installation file> <server address> /token <installation token> /vdi [tag <tag>] [/disabled] [/nfs] [/np /manualproxy <proxy url>:<proxy port>]</code>
Install the D-Client on a Windows server with the Cluster Shared Volume (CSV) feature enabled	<code><exe path><installation file> <server address> /token <installation token> /ignorecsv [/tag <tag>] [/disabled] [/nfs] [/np /manualproxy <proxy url>:<proxy port>]</code>

Where:

Command Parameter	Description	Comments
<code><exe path></code>	Path for the appropriate installation file, where all the Windows devices have access	N/C
<code><installation file></code>	file name for the appropriate installation file	N/C
<code><server address></code>	FQDN for the D-Appliance	N/C
<code><installation token></code>	ID of the installation token, as displayed in the Windows Deployment Resources screen	N/C

Command Parameter	Description	Comments
<code><tag></code>	Adds a tag associated with the deployed devices. Use quotation marks to enter values with spaces or special characters.	<ul style="list-style-type: none"> Optional The Device Tag must comply to the following: <ul style="list-style-type: none"> Maximum length is 256 characters Device Tags are case sensitive Valid characters: <ul style="list-style-type: none"> Letters (a-z, A-Z) Numbers (0-9) Spaces representable in UTF-8 Special characters: + - = . _ : / @ <p>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.</p>
<code>/disabled</code>	When <code>/disabled</code> is included, the D-Client is disabled during the installation. This allows the administrator to select when to initially enable the D-Client.	Optional
<code>/nfs</code>	Starts the D-Client without performing the initial full scan	Optional
<code>/np</code>	Enables the use of a network proxy server using the default proxy settings.	<ul style="list-style-type: none"> Optional Cannot be used with <code>/manualproxy</code>

Command Parameter	Description	Comments
/manual-proxy	Enables the use of a network proxy server, using the specified settings of the proxy server URL and port number.	<ul style="list-style-type: none"> Optional Only available for D-Client v2.5.1 or higher Do not use with /np
<proxy url>	URL for the proxy server, including the scheme	N/C
<proxy port>	Port number to access the proxy server	N/C
/vdi	Required when installing the D-Client on a VDI machine. For more information, see D-Client Installation for Windows 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 Cluster Shared Volume are not scanned. However, all files copied to the local drive are scanned.
<abortIfNo-ServerConnection>	Enables the D-Client installer to run a connectivity check with the management server before deployment. When included, if the D-Client fails to establish connectivity, the installation process is aborted.	<ul style="list-style-type: none"> 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)



NOTE

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:

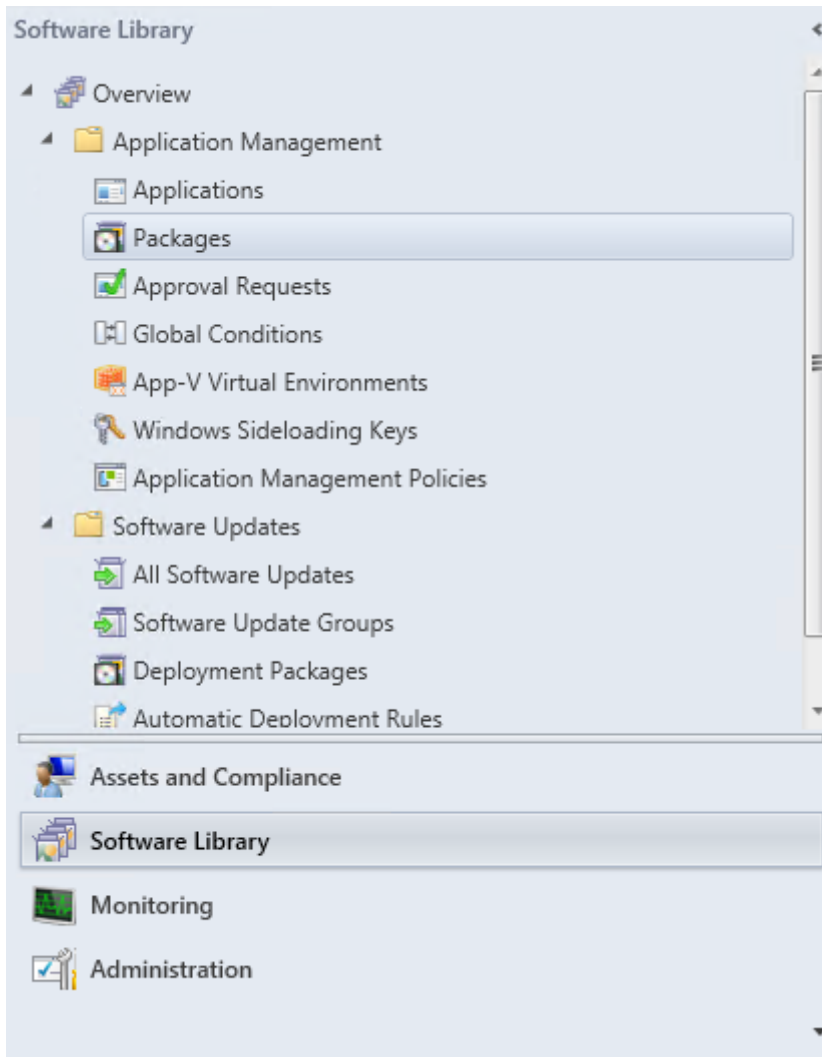
- Deep Instinct Windows EXE installation file. The file may be downloaded from the [Windows Deployment Resources](#) screen.
- [Determine the installation CLI command](#) to run with SCCM.
- [Create a package for D-Client deployment](#).
- [Deploy the D-Client installation package](#).

Creating a Package for D-Client Deployment

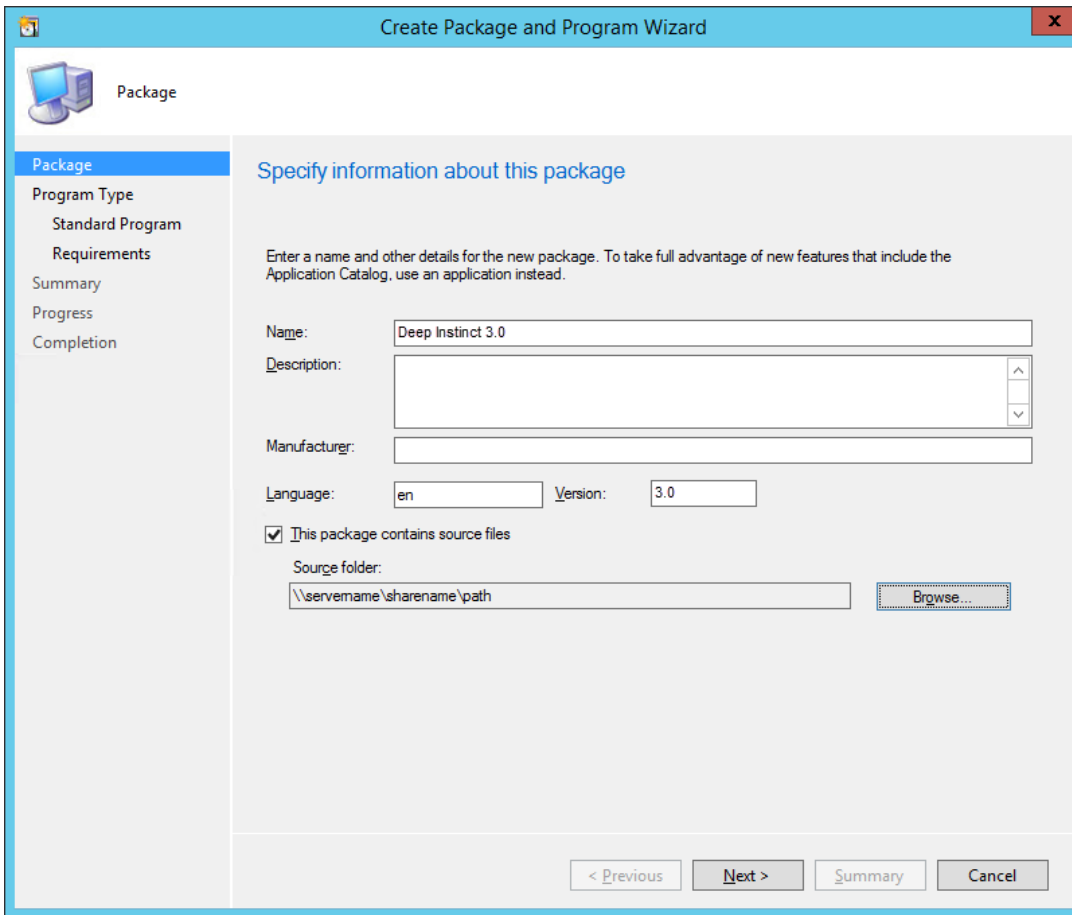
To create a package for deployment:

1. Download the installation file from the [Windows Deployment Resources](#) screen.

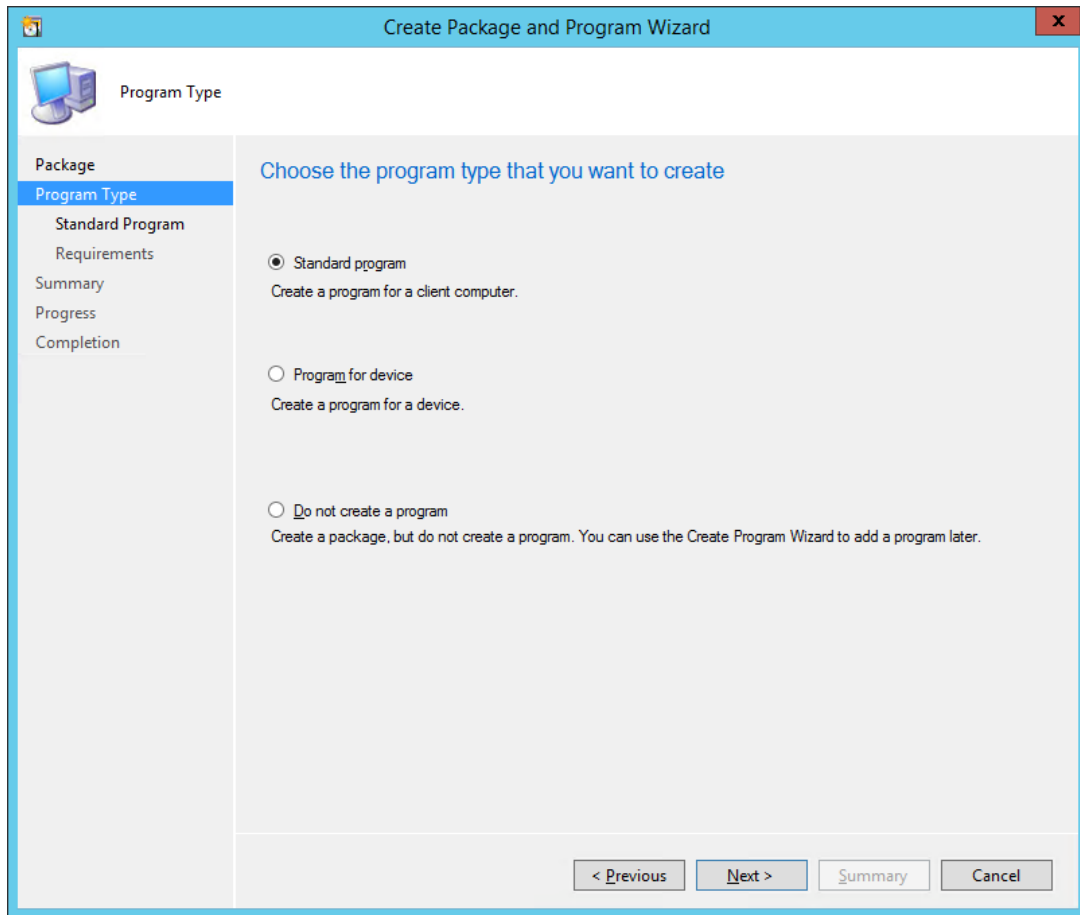
2. Save the installation file to a location where all the organization's Windows devices have access.
3. Start Microsoft System Center Configuration Manager.
4. In the Configuration Manager console, click Software Library.
5. In the Software Library workspace, expand Application Management.



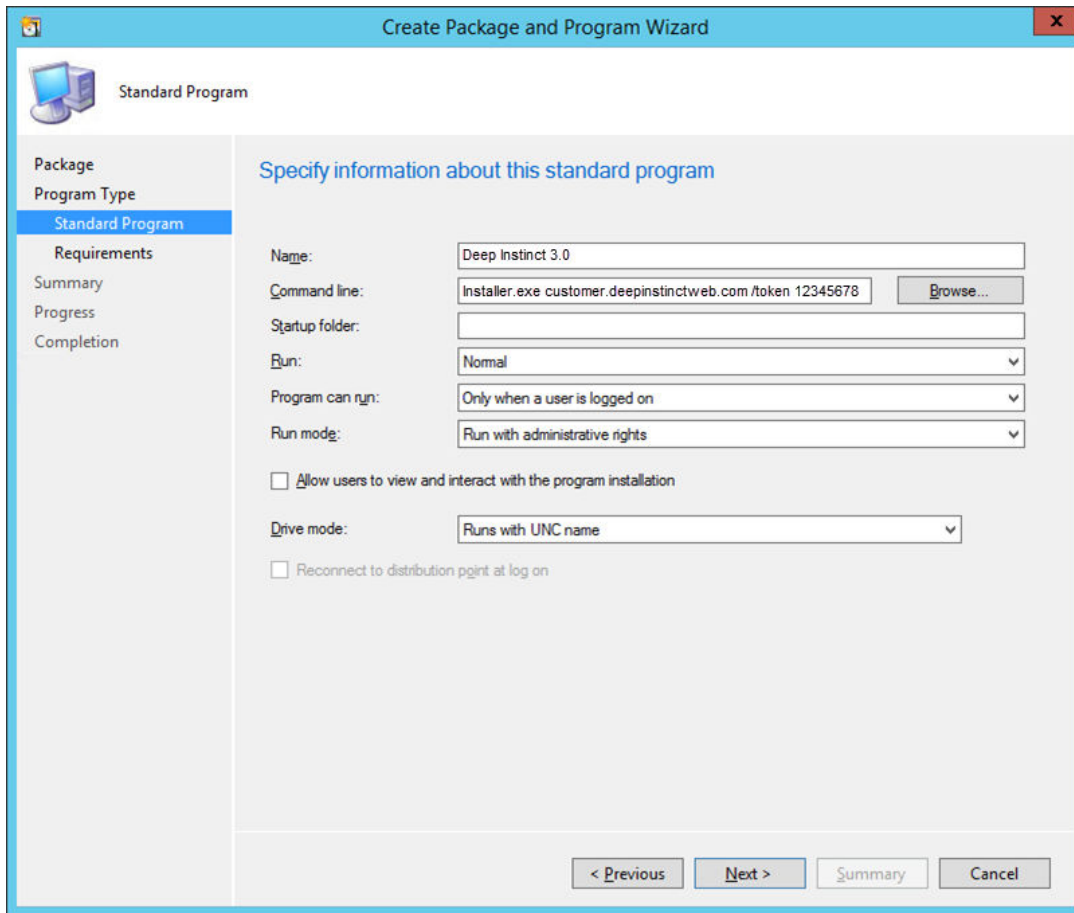
6. Right-click Packages and click Create Package. The Create Package and Program Wizard opens. Perform the following:



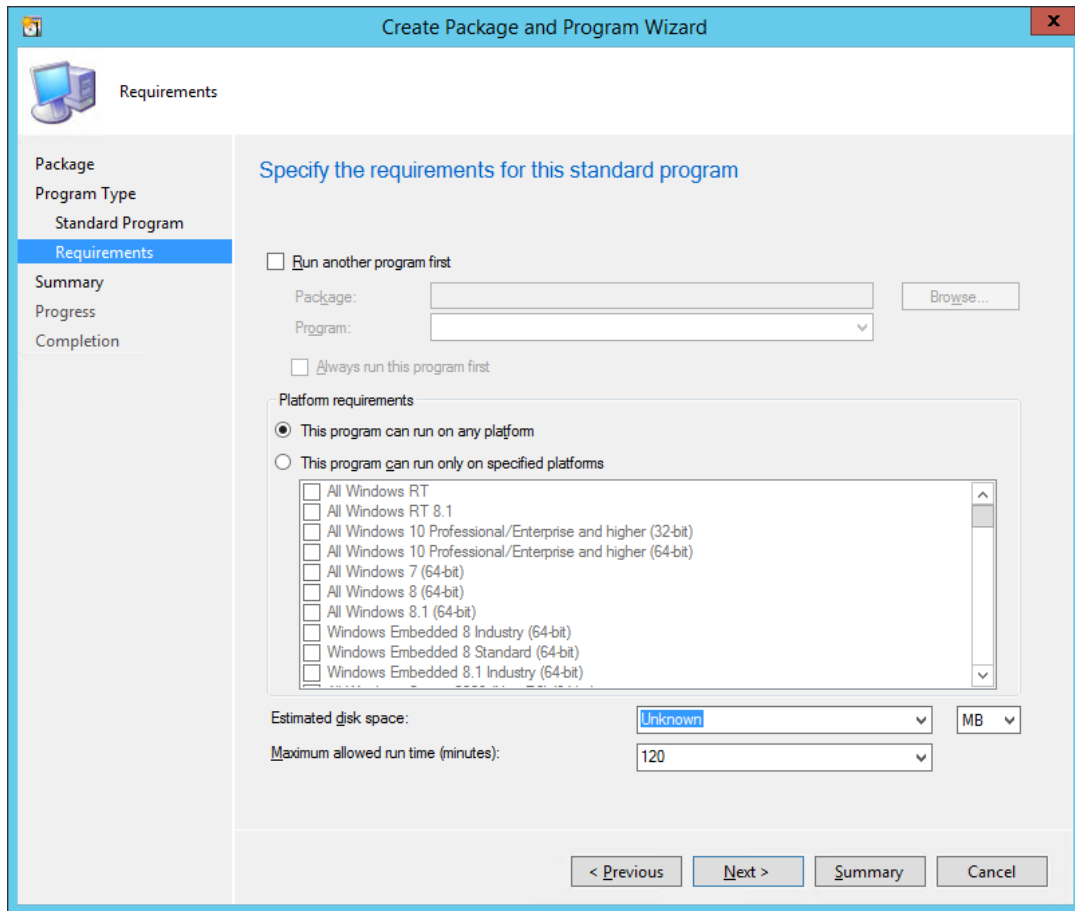
- a. Enter the name of the package.
- b. As an option, enter the description, manufacturer, language, and/or version of the package. It is recommended to enter the version number for version control.
- c. Select This package contains source files.
- d. Click Browse. Go to the folder where the installation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



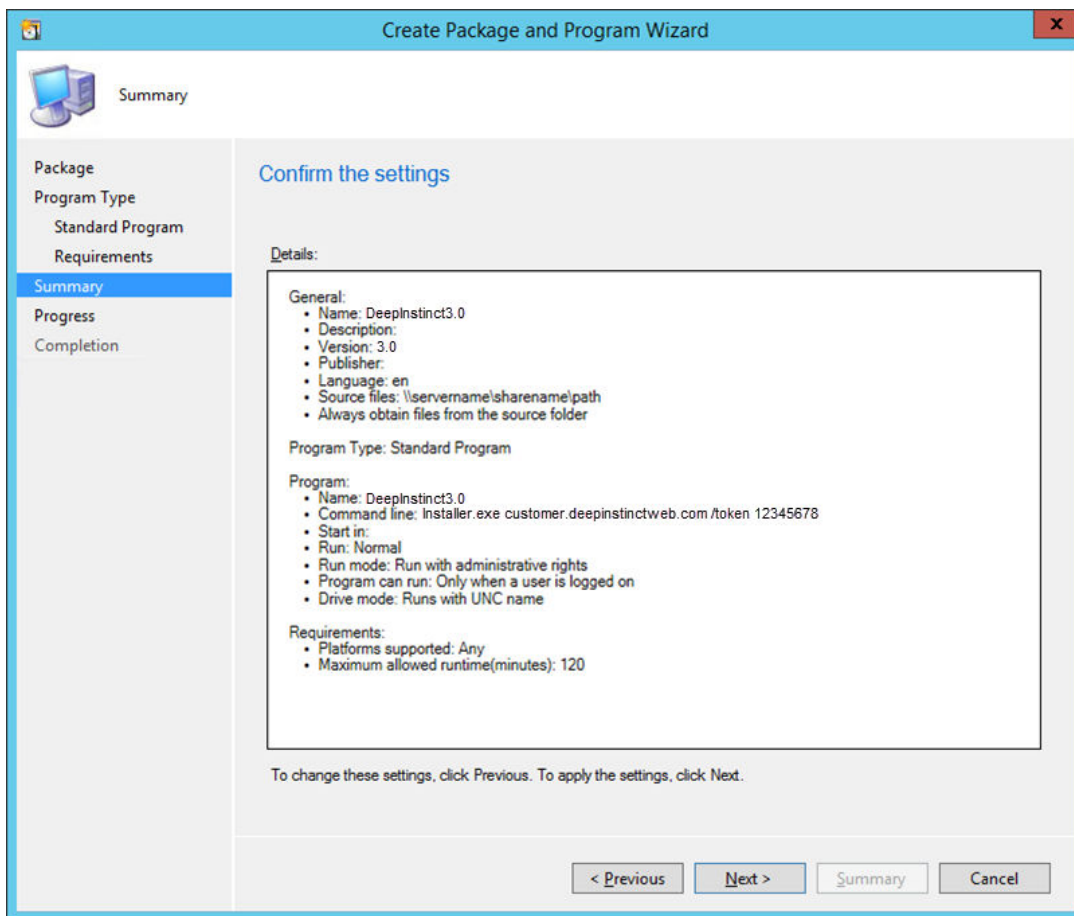
7. Select Standard program. Click Next and perform the following:



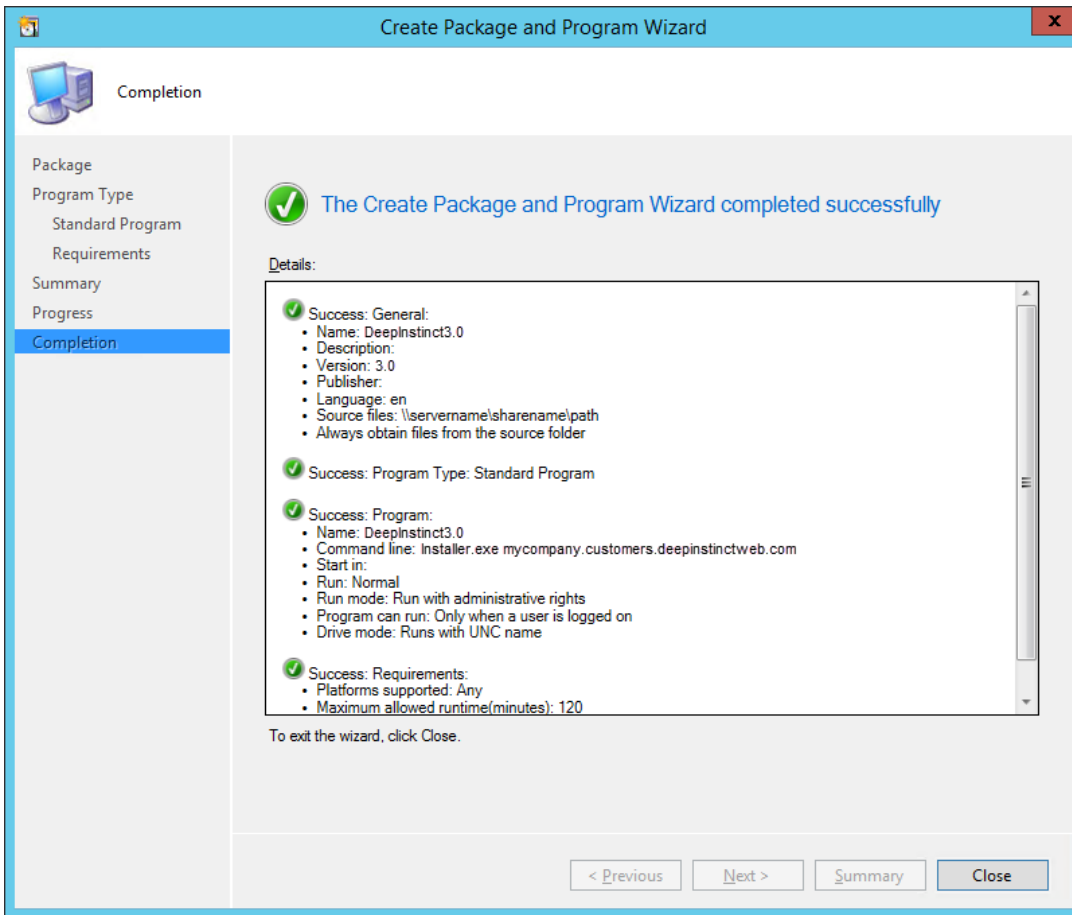
- a. Enter the name of the D-Client installation file.
- b. Type the CLI command with all required options and values in the Command line. For details on how to define the CLI command, see [Windows D-Client CLI Command](#).
- c. Change Run Mode to Run with administrative rights and click **Next**.



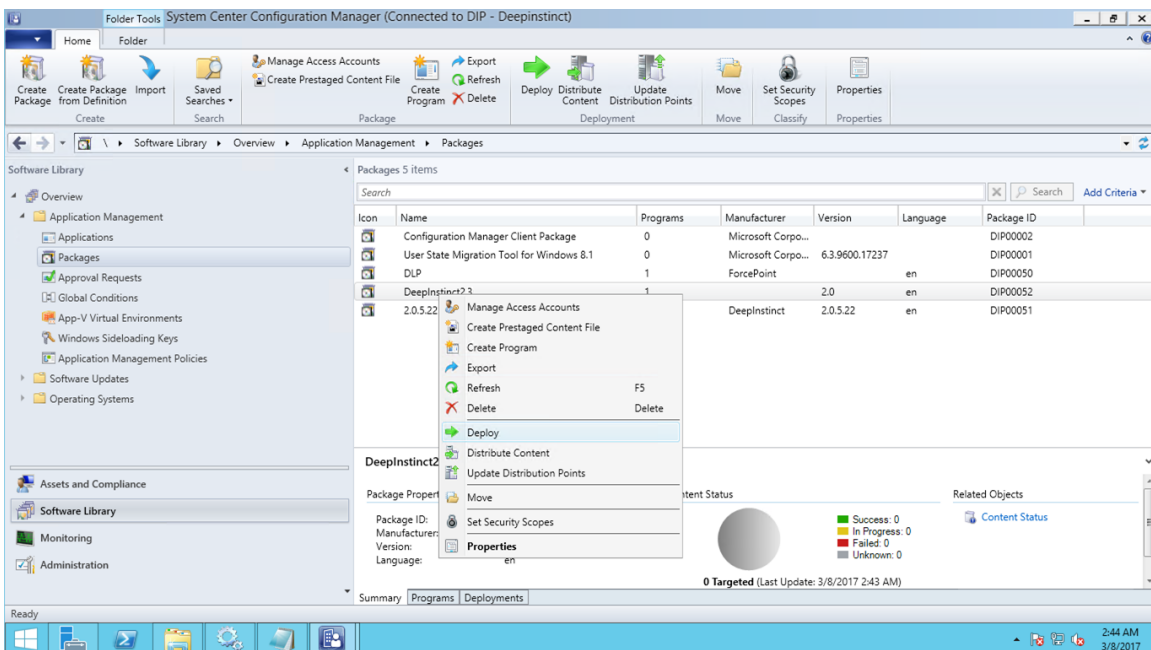
8. Click **Next** and a summary of the package settings are displayed.



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



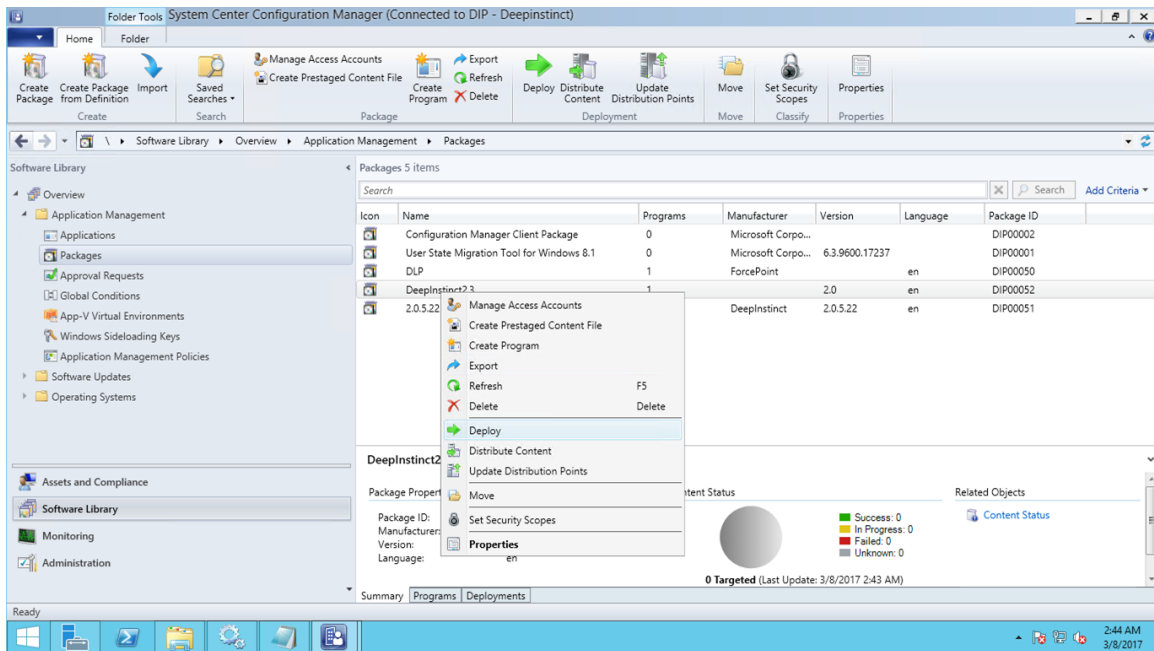
10. Click **Close** and the Deep Instinct deployment package appears in the list of packages.



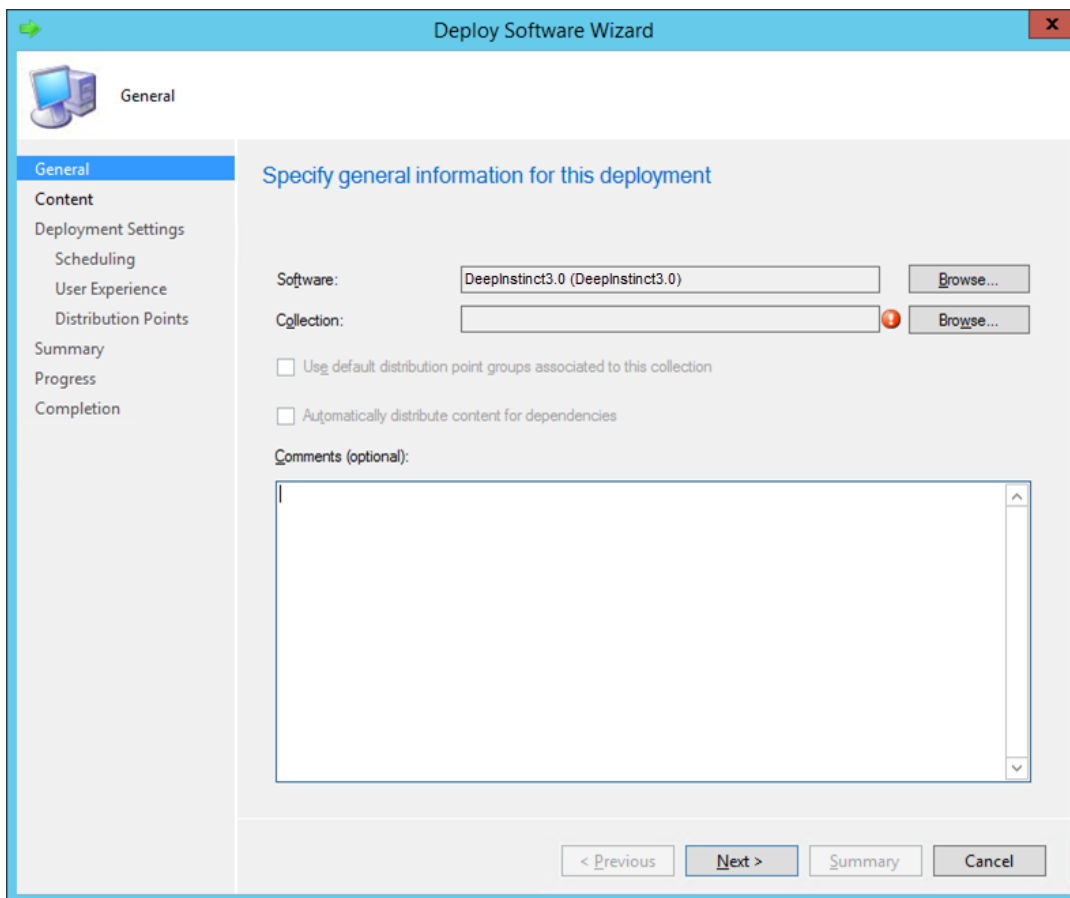
Deploying the D-Client Installation Package

To deploy the package using SCCM:

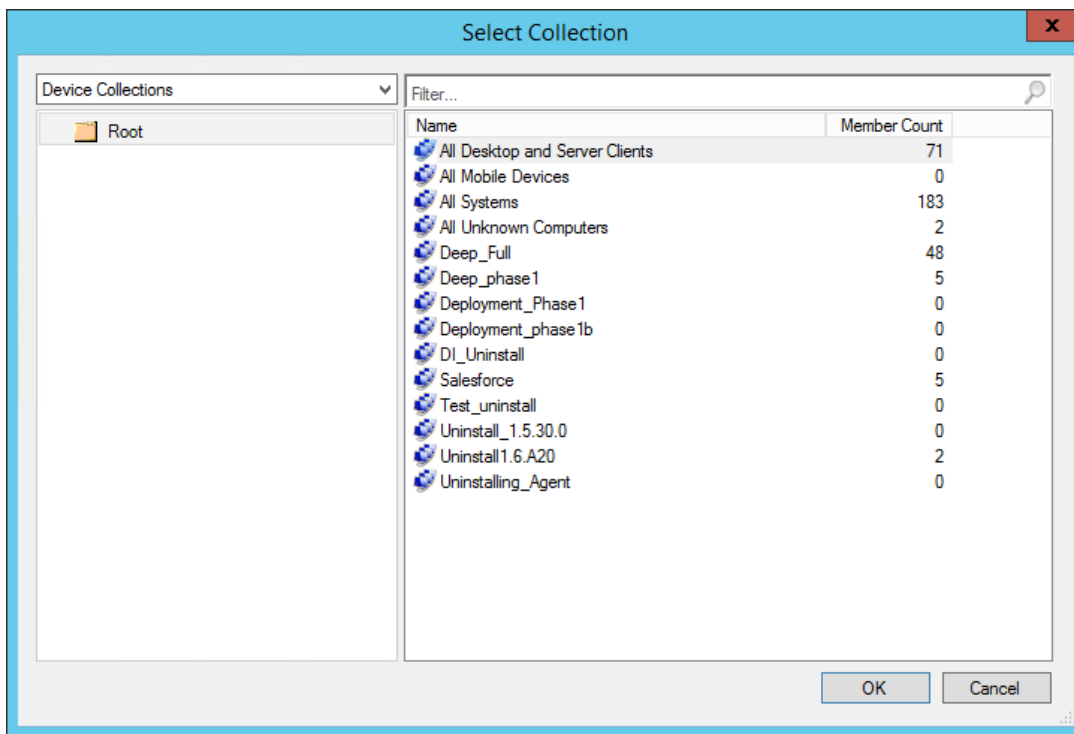
1. Start Microsoft System Center Configuration Manager.
2. In the Configuration Manager console, click **Software Library** → **Application Management** → **Packages**. The list of packages appears.



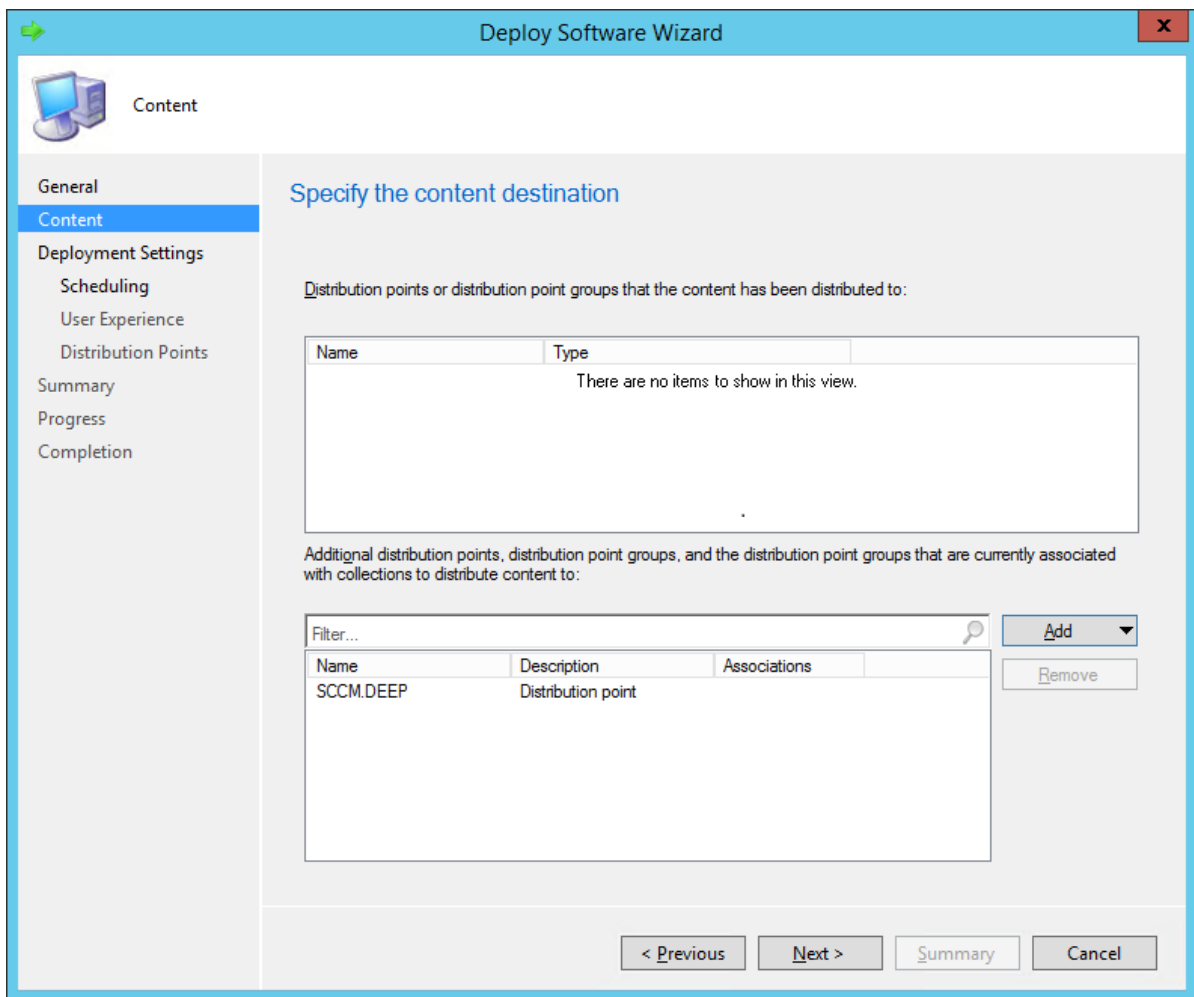
3. Right-click the Deep Instinct deployment package and click **Deploy**. The Deploy Software Wizard opens.



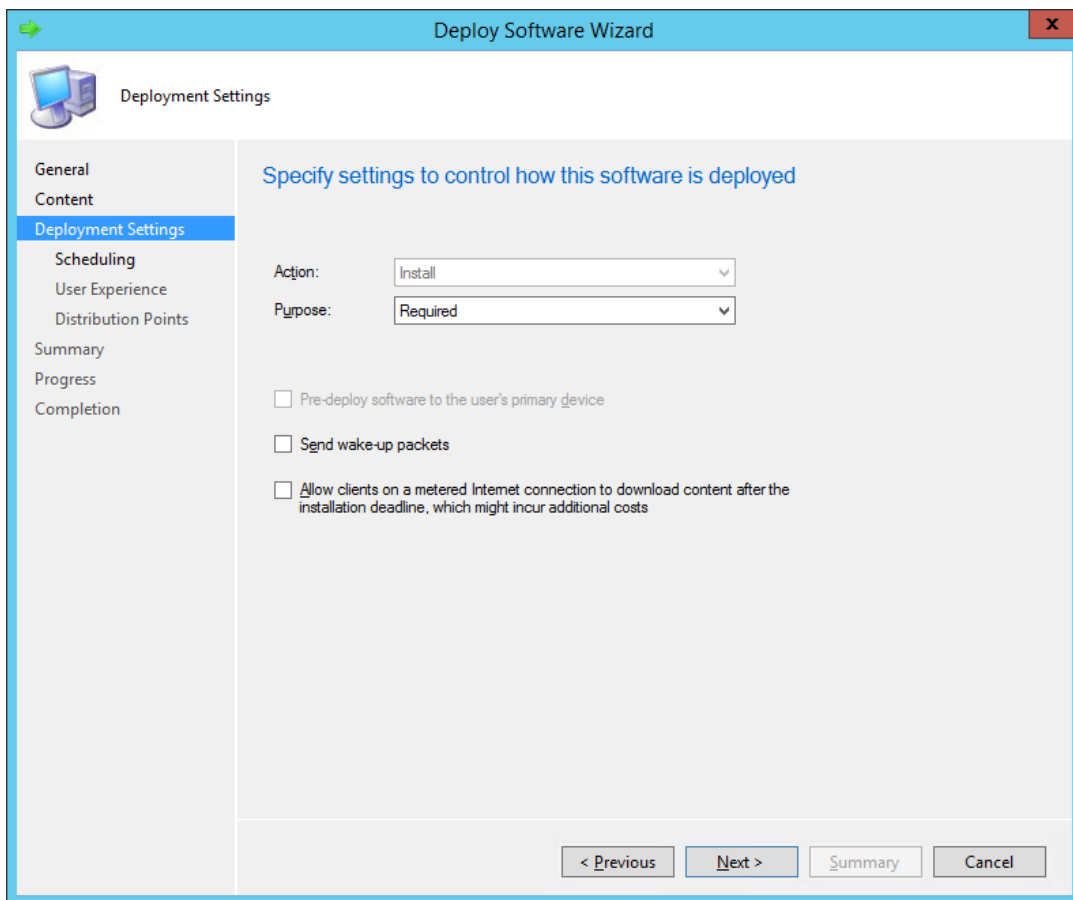
4. Click **Browse**, select the Device Collection for deployment and click **OK**.



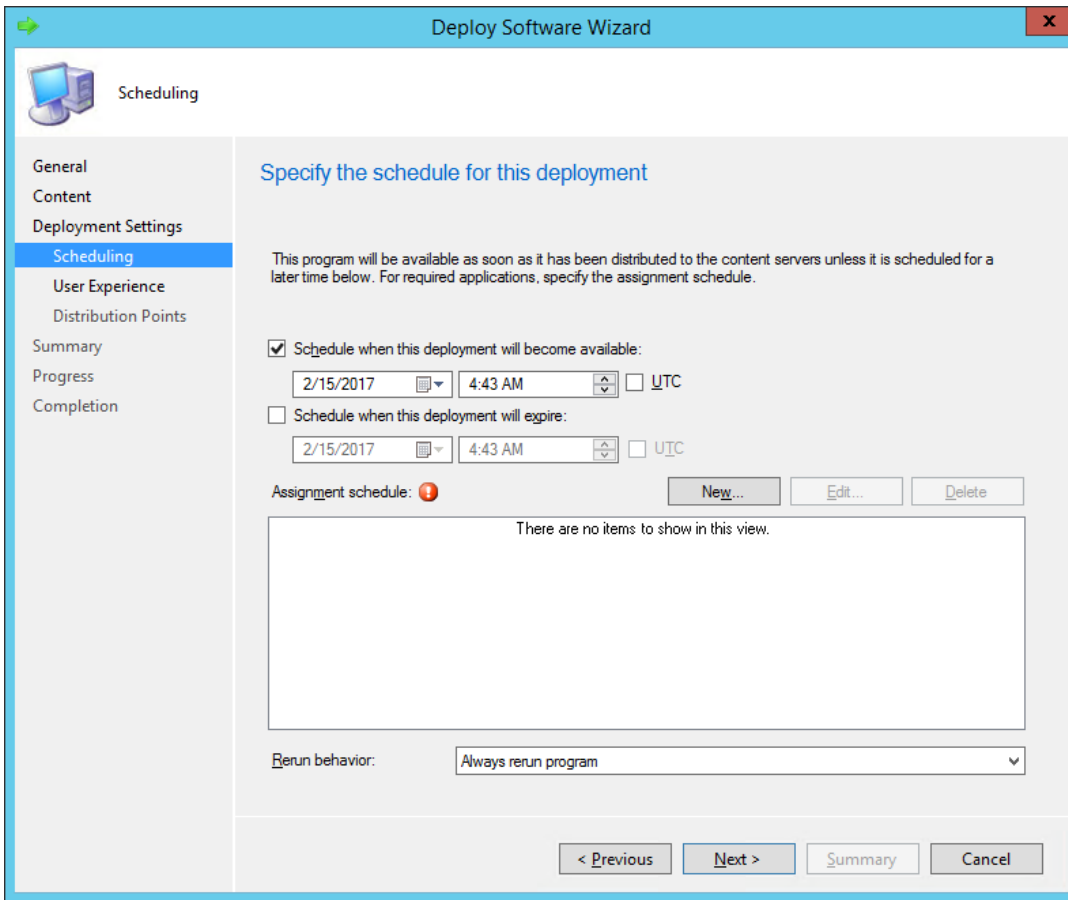
5. Click **Next**. Click **Add** + **Distribution Point** and select the distribution points for the content destination. This is typically the SCCM server.



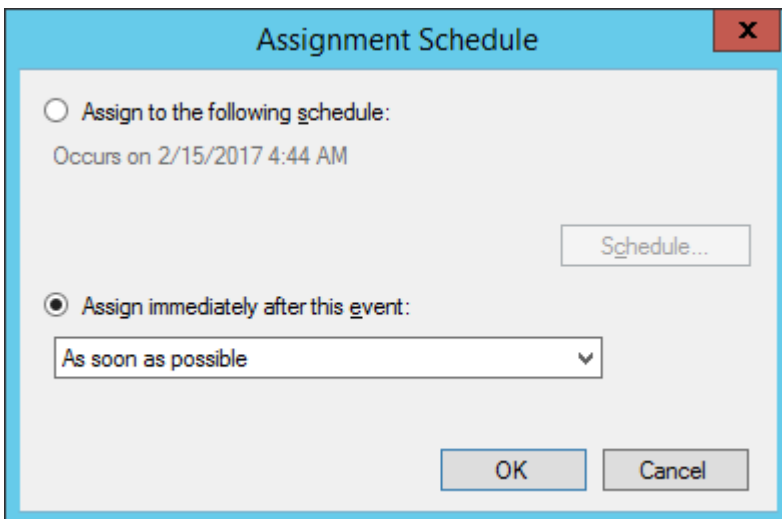
6. Click **Next** and make this a required installation, by selecting Required in the Purpose box.



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

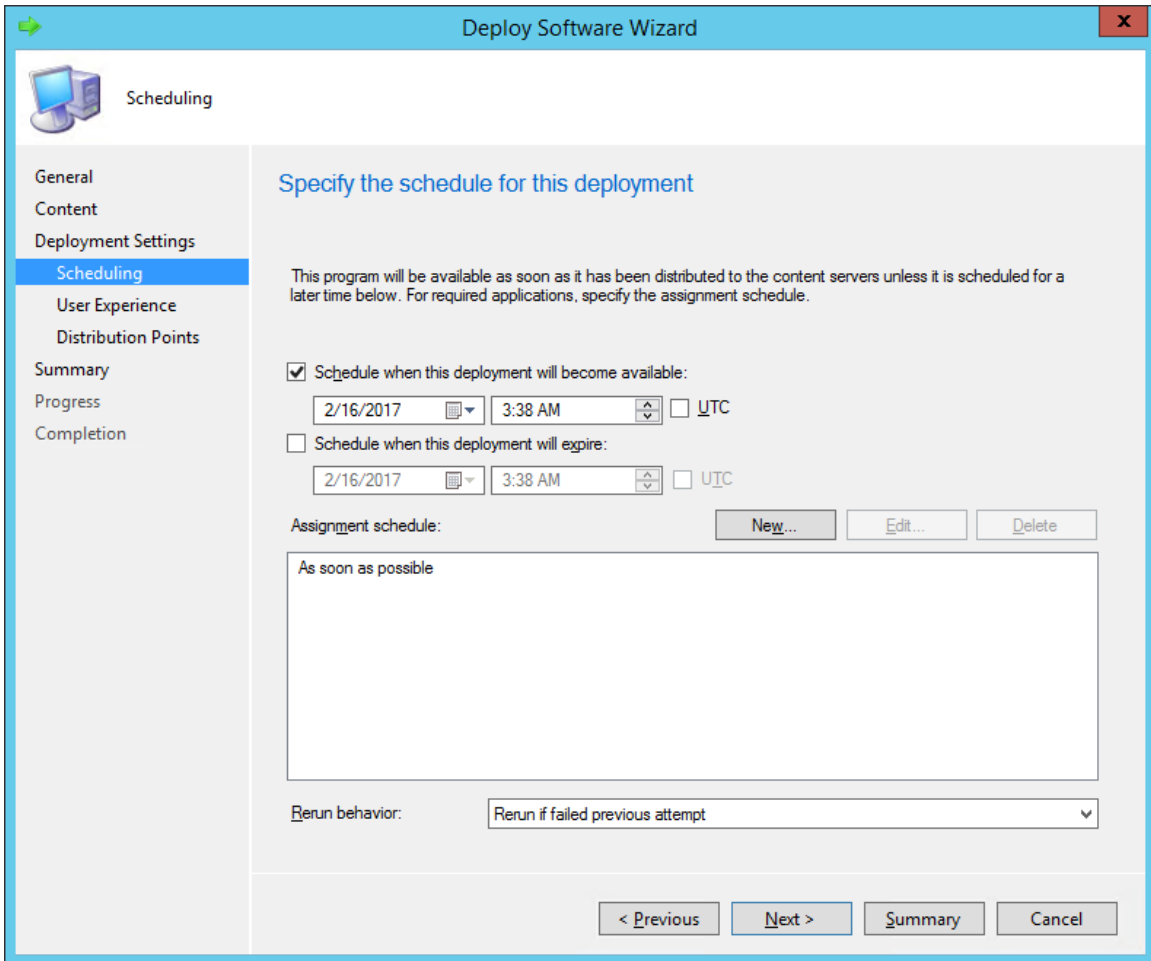


8. Select Schedule when this deployment will become available.
9. Click **New** and the Assignment Schedule dialog box opens.

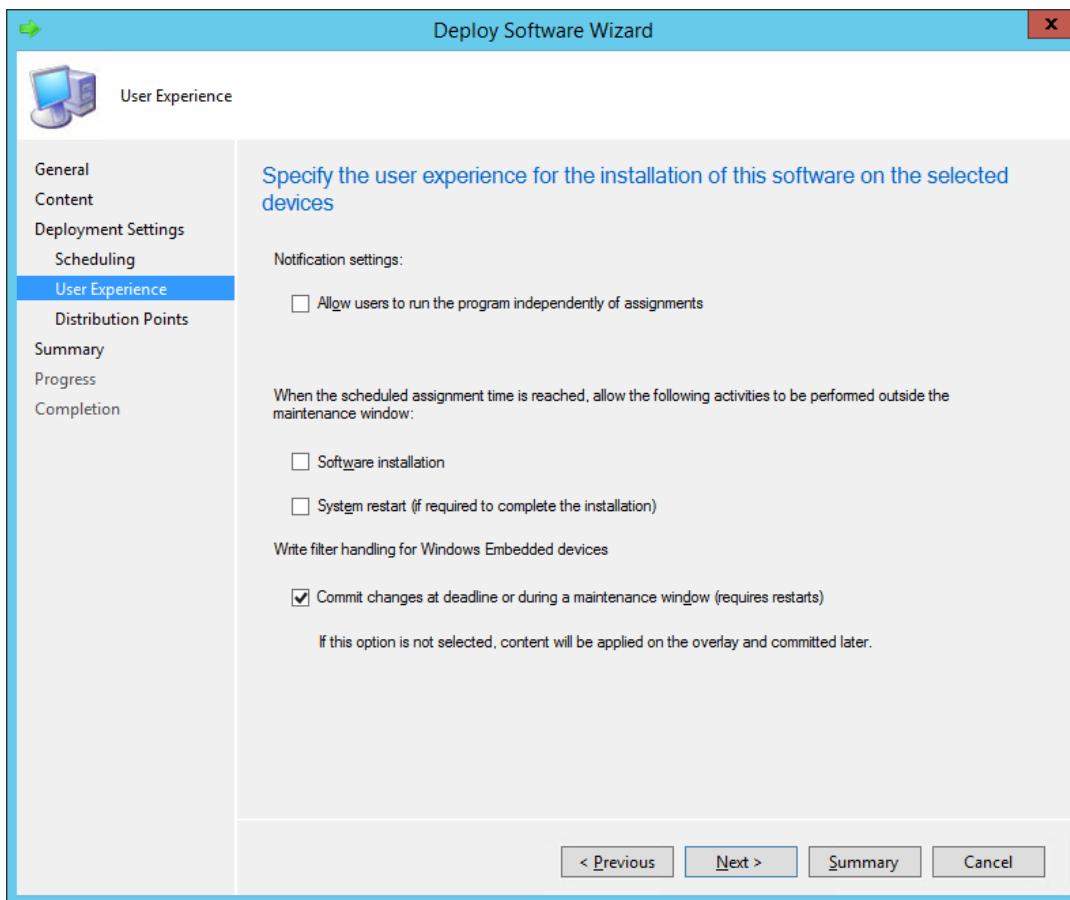


10. Select Assign immediately after this event and select As soon as possible from the drop-down box.

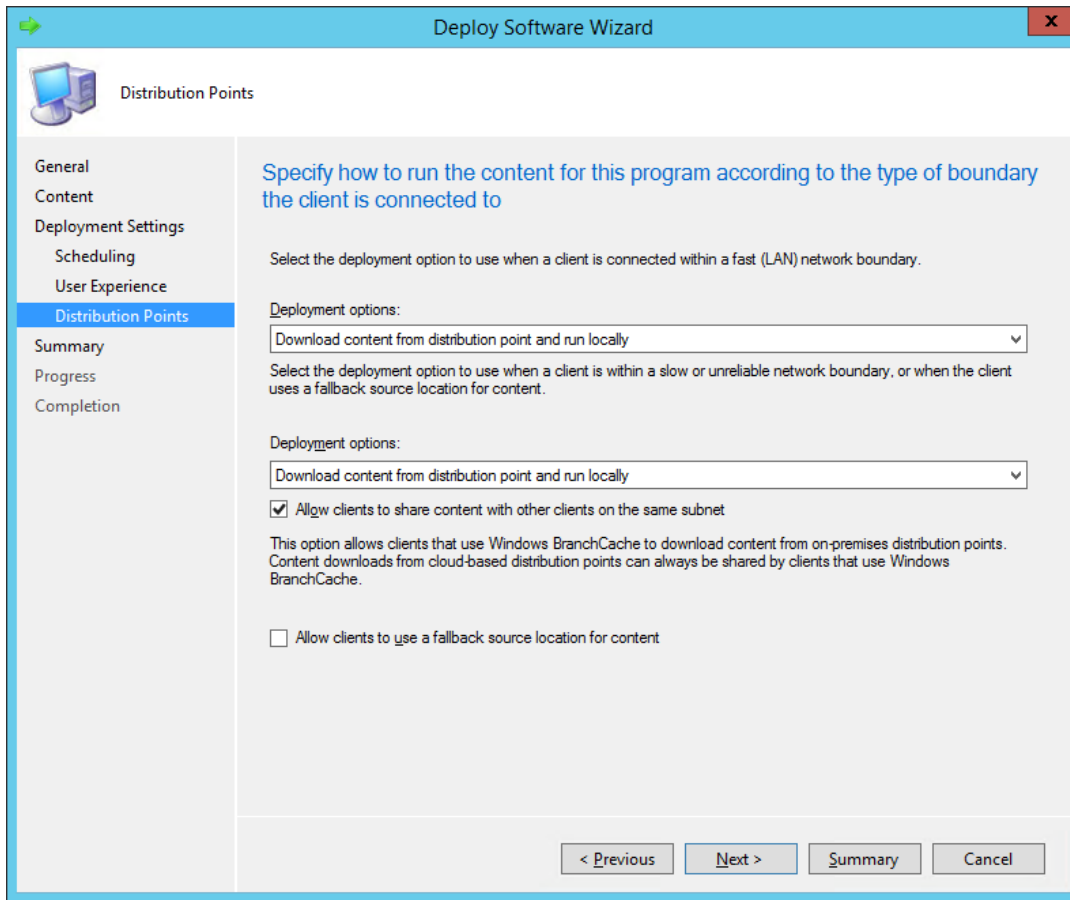
11. Click **OK** and 'As soon as possible' is added to the assignment schedule.



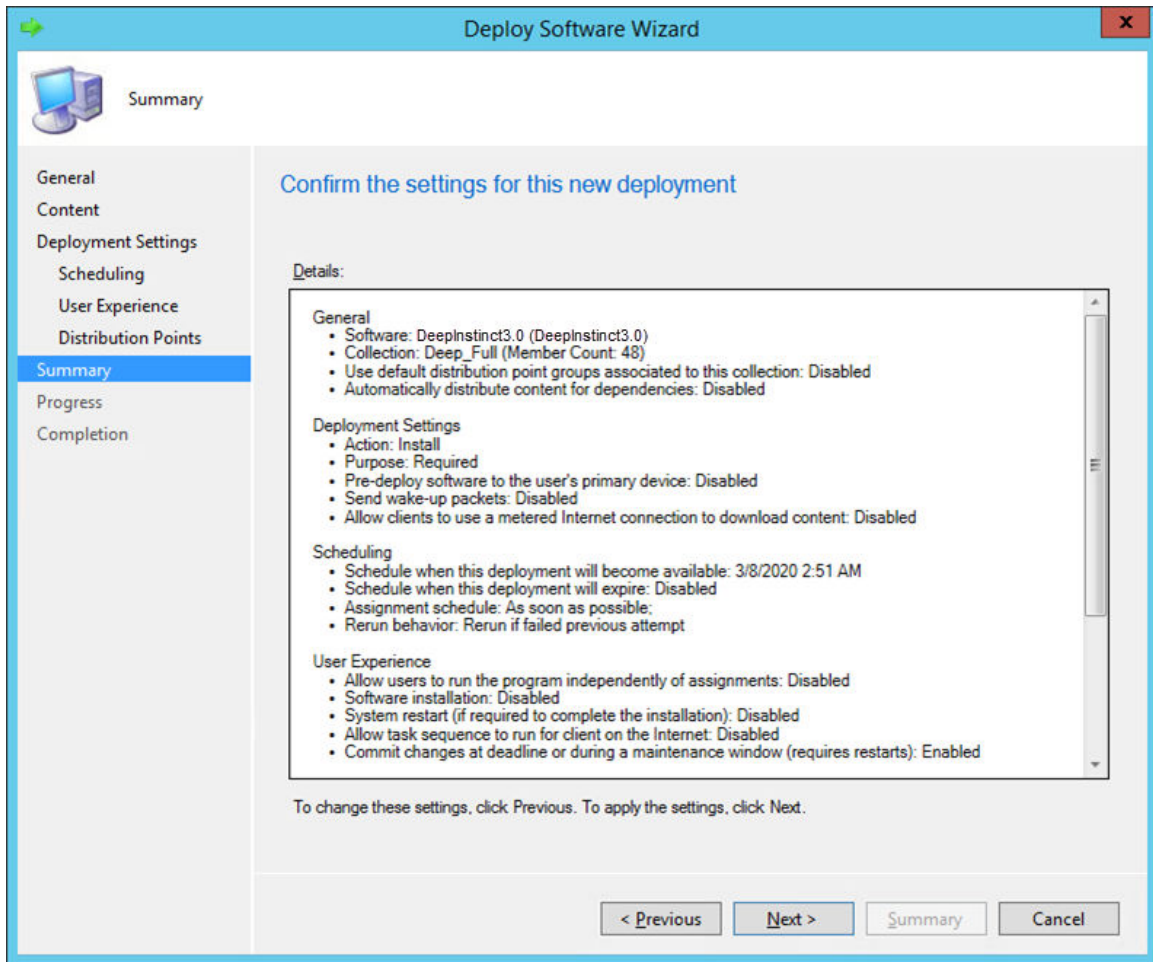
12. Click **Next** and the **User Experience** dialog box opens.



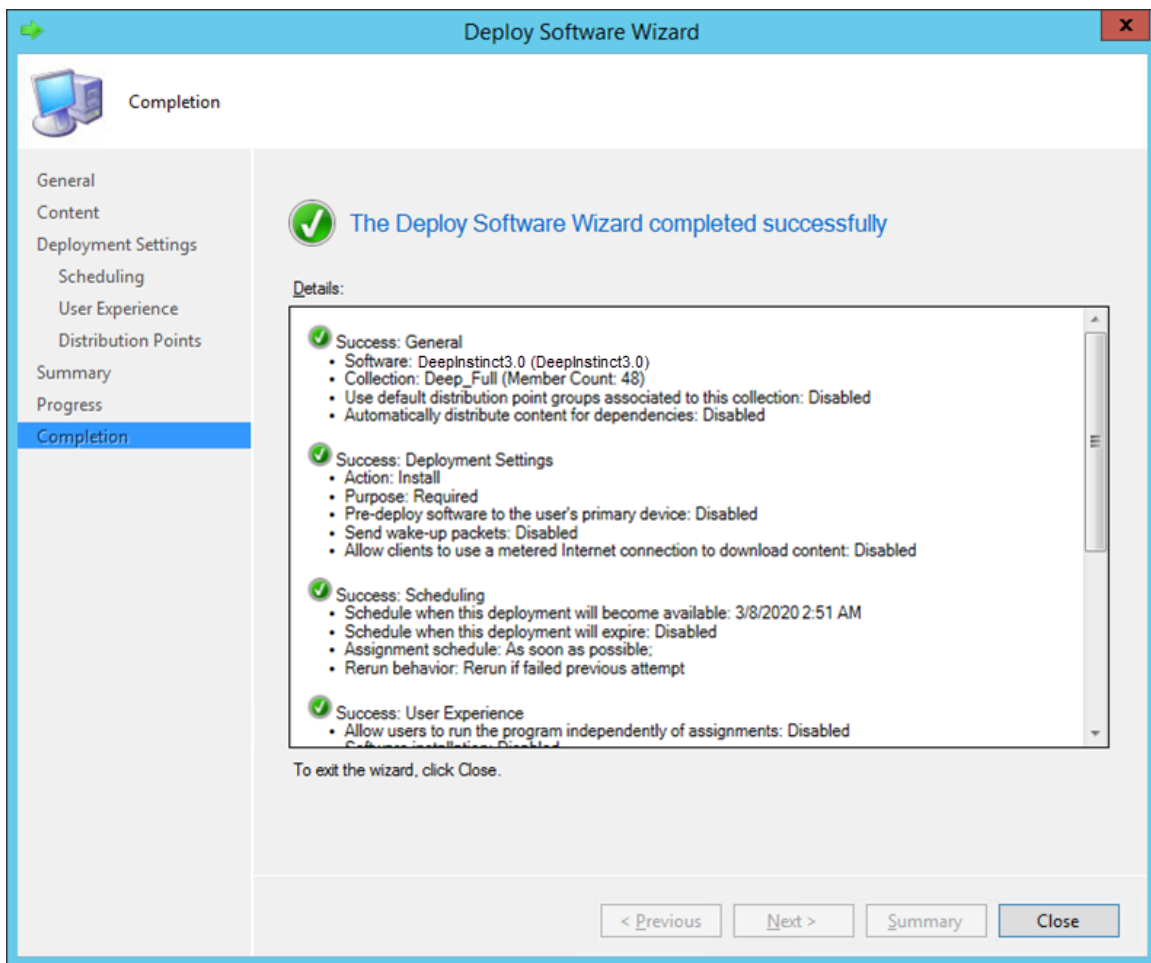
13. Click **Next** and the **Distribution Points** dialog box opens.



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.



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

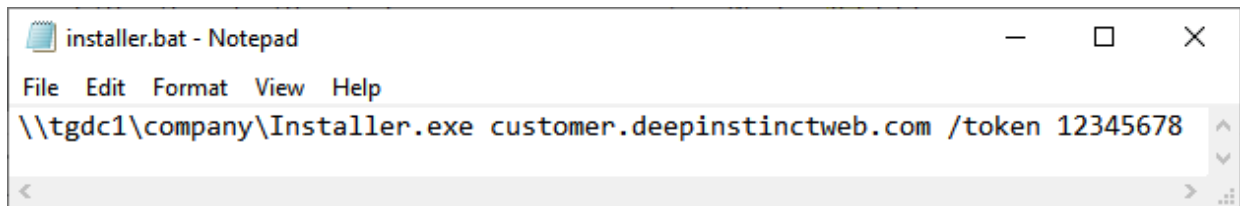
Before you can deploy the D-Client with GPO, you need to create an installation batch file. You can create the batch file with a text editor (such as Notepad).

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
\\tgdcl\company\Installer.exe customer.deepinstinctweb.com /token 12345678
```

Where:

- exe path = \\tgdcl\company\
■ installation file = Installer.exe
■ server address = customer.deepinstinctweb.com
■ installation token = 12345678

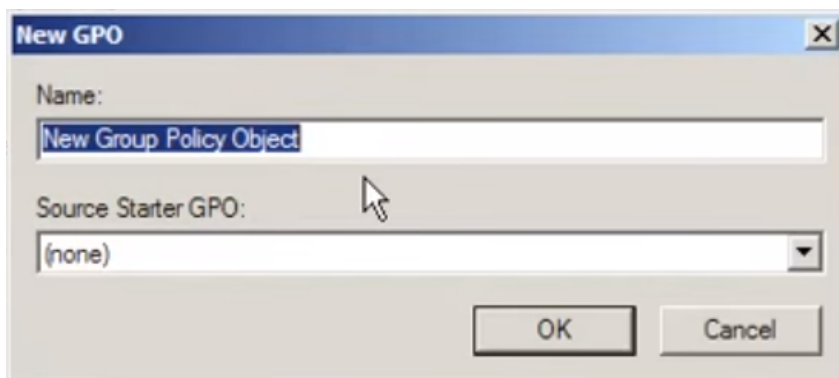
6. Copy the batch file to the same location the installation file was saved and to the location where the Windows deployment tool has access.

Deploying D-Clients using GPO

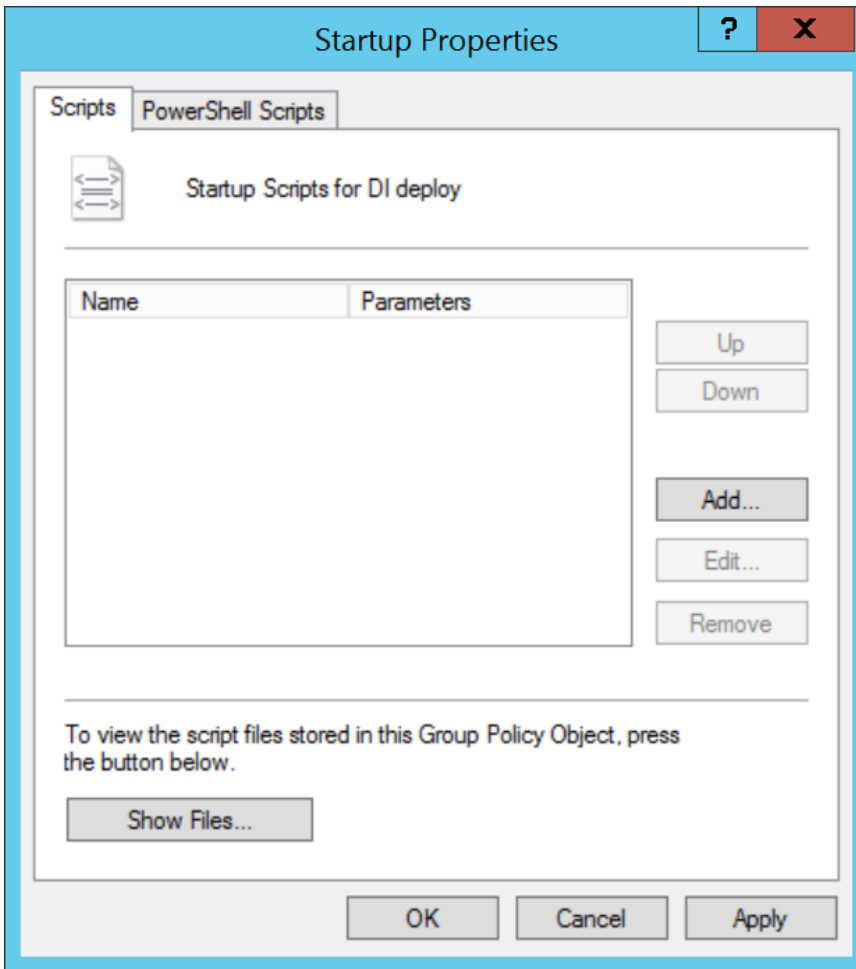
To deploy D-Clients using GPO:

1. Download the installation file from the [Windows Deployment Resources](#).

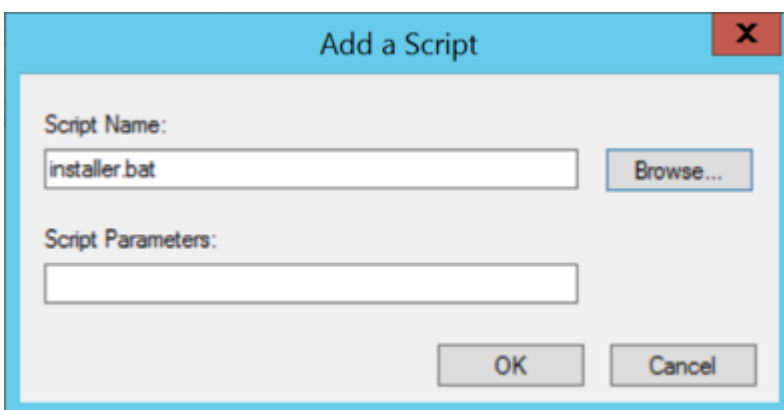
2. Create the installation batch file.
3. Save the installation batch file to the Startup Script folder.
4. Save the EXE and batch files to a location where all the organization's Windows devices have access.
5. Log on to the Domain Controller (DC) and start the Microsoft Group Policy Management Console (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.



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.



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



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.

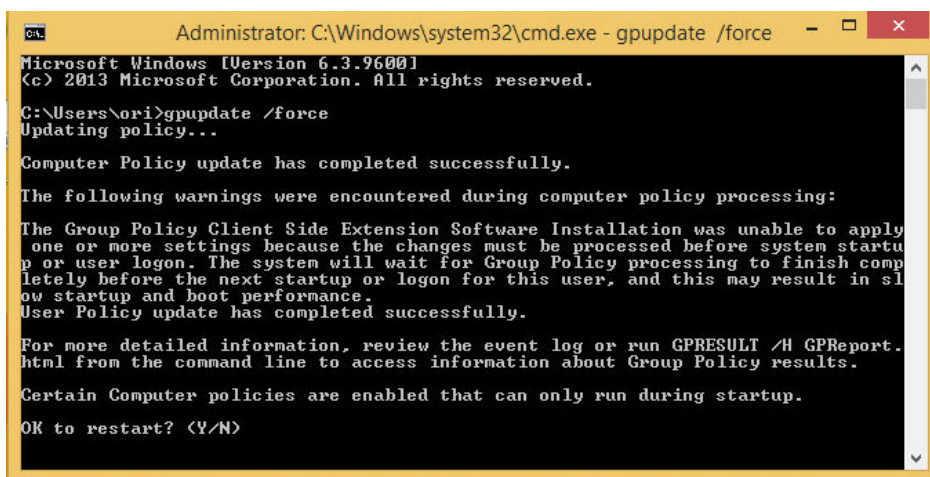
To install the D-Client immediately from a device, perform the procedure described in [Apply GPO to Deploy D-Client Manually](#).

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 `gpupdate /force`. The Command Prompt window indicates that the policy updated successfully.



```
Administrator: C:\Windows\system32\cmd.exe - gpupdate /force
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\ori>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.

The following warnings were encountered during computer policy processing:

The Group Policy Client Side Extension Software Installation was unable to apply
one or more settings because the changes must be processed before system startu
p or user logon. The system will wait for Group Policy processing to finish comp
letely before the next startup or logon for this user, and this may result in sl
ow startup and boot performance.
User Policy update has completed successfully.

For more detailed information, review the event log or run GPRESULT /H GPReport.
html from the command line to access information about Group Policy results.

Certain Computer policies are enabled that can only run during startup.

OK to restart? (Y/N)
```

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:

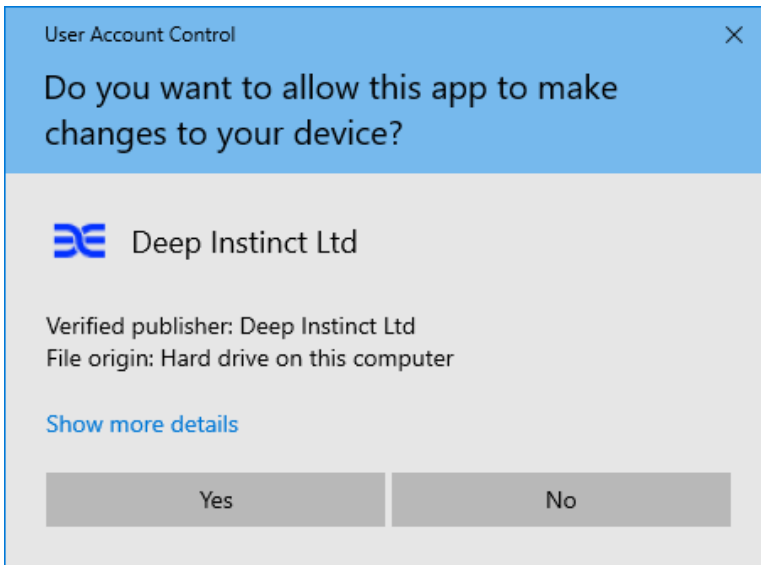
```
C:\Windows\system32> c:\users\administrator\downloads\Installer.exe  
customer.deepinstinctweb.com /token 12345678
```

4.2.3.2. Local deployment using the Installation screen

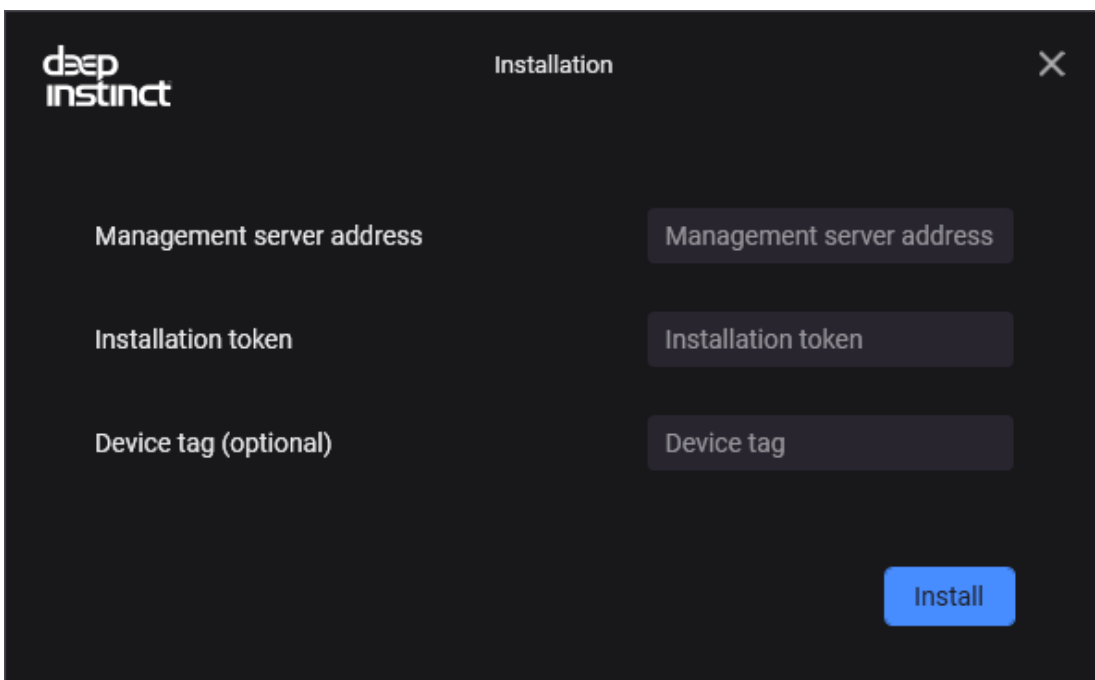
The D-Client can also be installed on each Windows device using the Installation screen and then monitored using the D-Client Console. This may be practical when only a few devices need to be installed or for devices that are not managed by the Active Directory.

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.

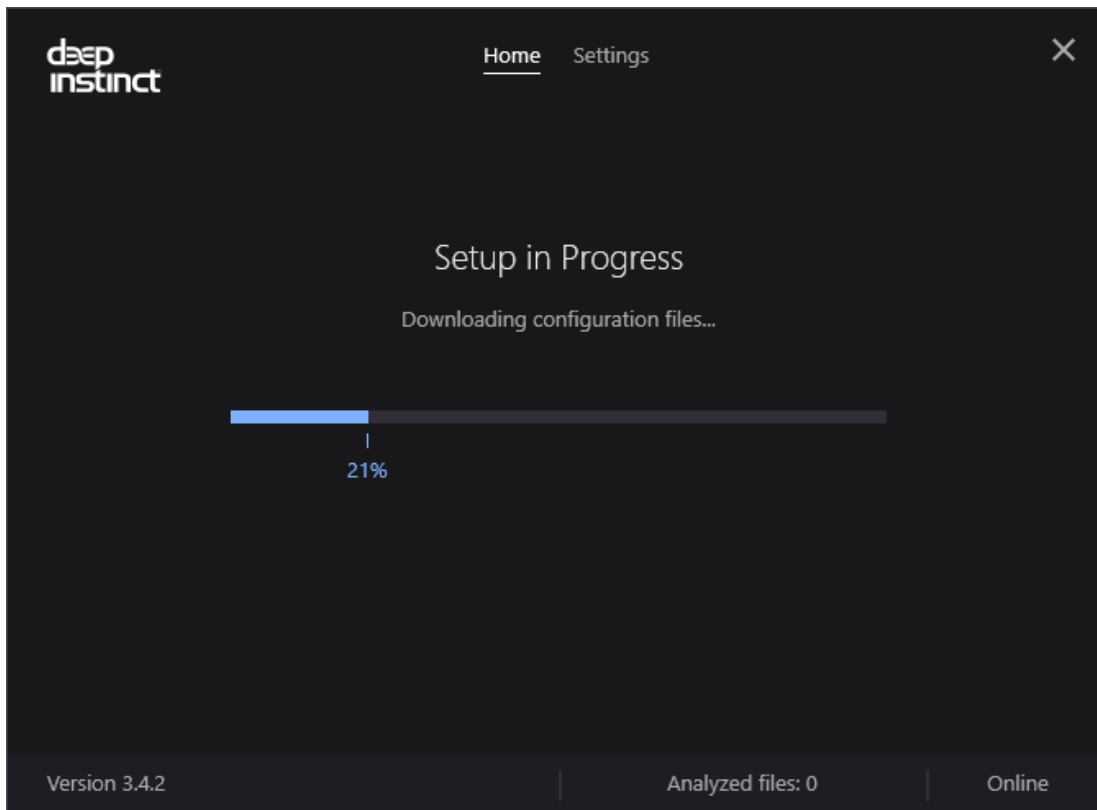



5. Enter the FQDN for the management server.
6. Enter the ID of the installation token, as displayed in the [Windows Deployment Resources](#) screen.
7. As an option, enter a tag associated with the deployed device. The Device Tag must comply to the following:
 - Maximum length is 256 characters

- 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 , the installation is in process.
10. To monitor the progress of the installation, you can open the D-Client Console by right-clicking the icon and selecting Show Console.



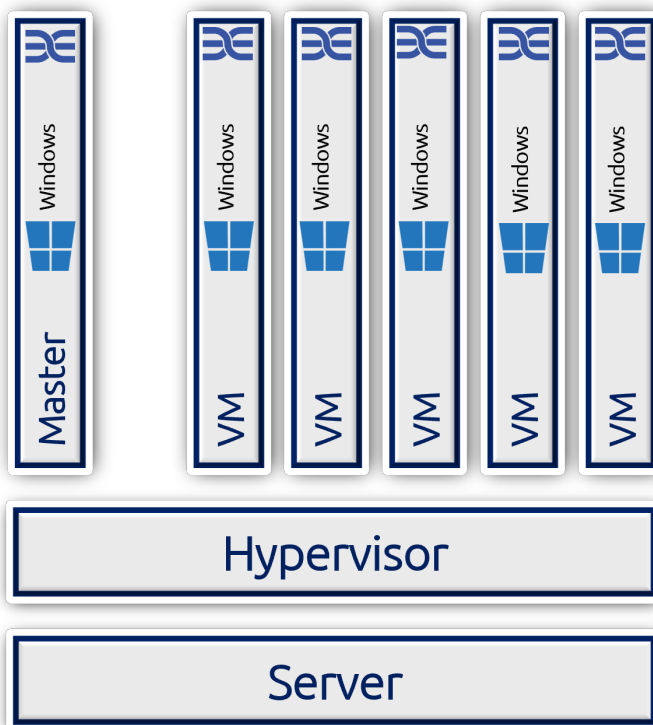
- When the installation completes successfully, the D-Client icon changes to a normal state  and a full scan is initiated.

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.

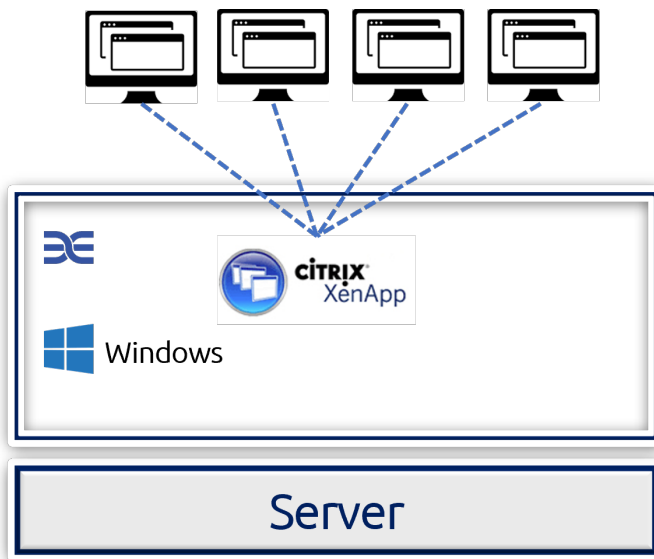


NOTE

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.



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:

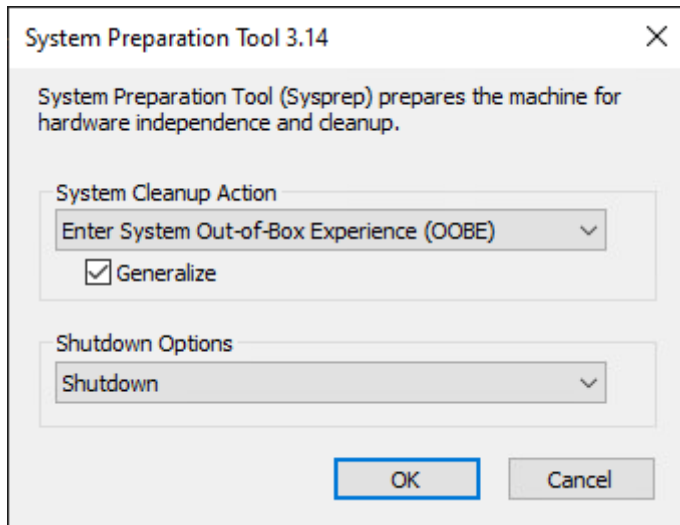
- exe path = c:\users\administrator\downloads\
- installation file = Installer.exe
- server address = customer.deepinstinctweb.com
- installation token = 12345678

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.



- 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.



NOTE

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 incorrect server URL or network issue	Failed_ManagementServerDoesNotExist = 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 exception	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 command 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

- [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

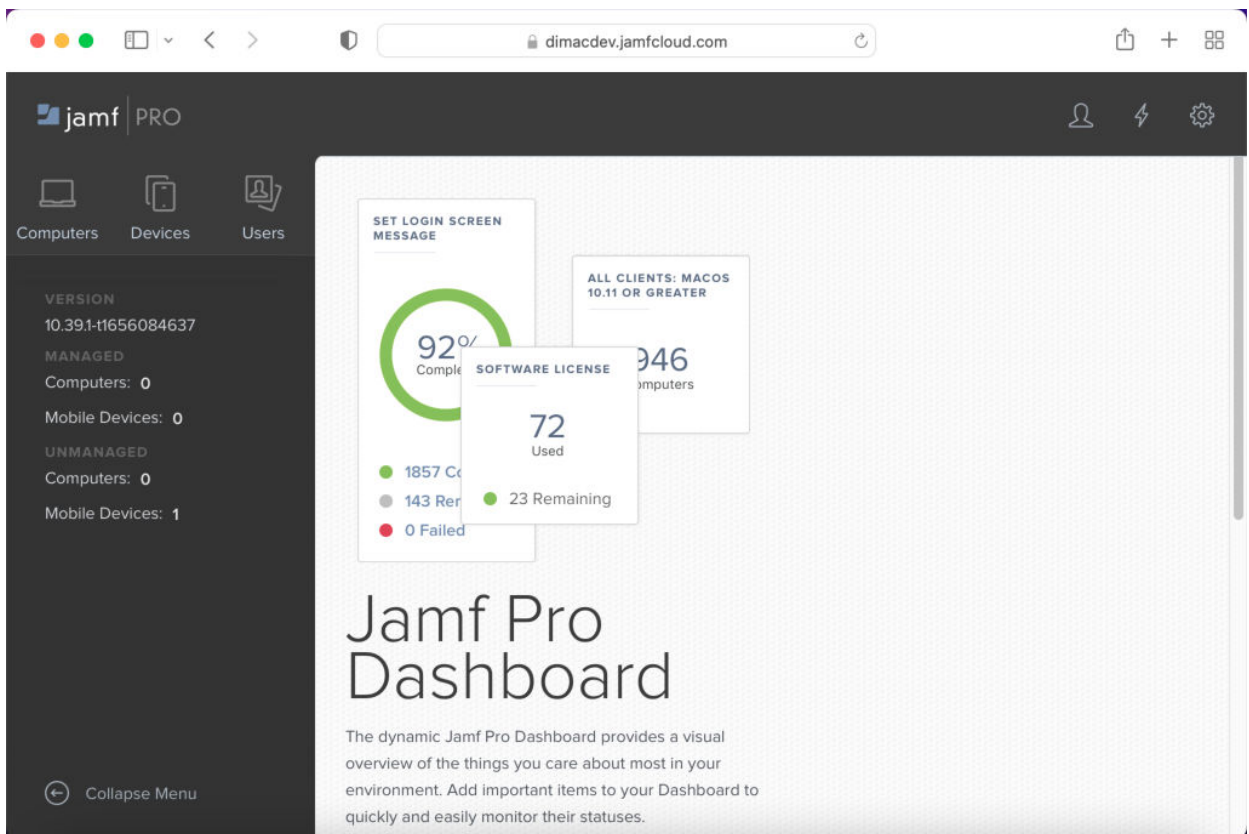
The Jamf Configuration Profile is used to define and enable the required macOS permissions.

Jamf Configuration Profile prerequisites

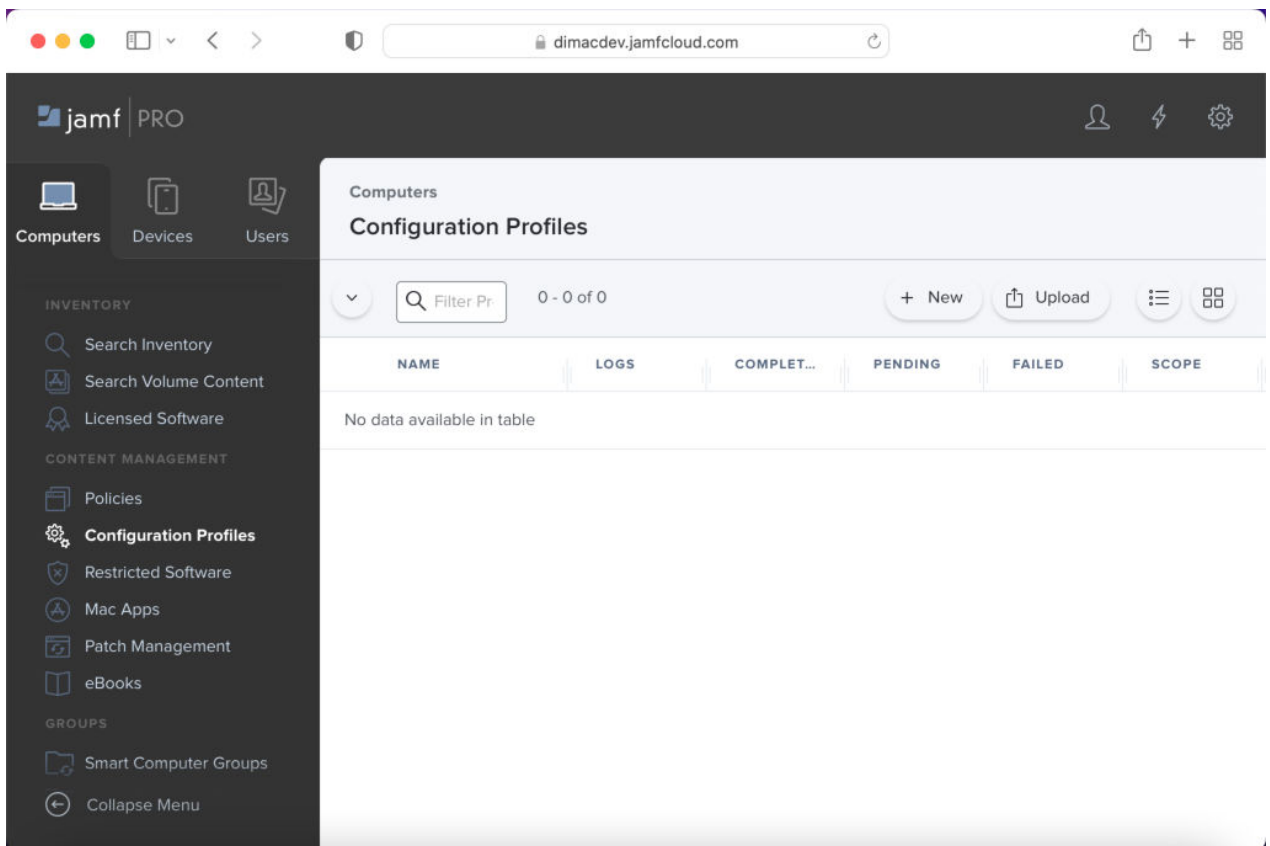
- Create a Jamf Profile
- Add Full Disk Access Permission
- Add System Extension Permission
- Allow the removal of Extension Permission
- Add Content Filter Permission
- Define the scope to which computers the profile is deployed

To create a Jamf Configuration Profile:

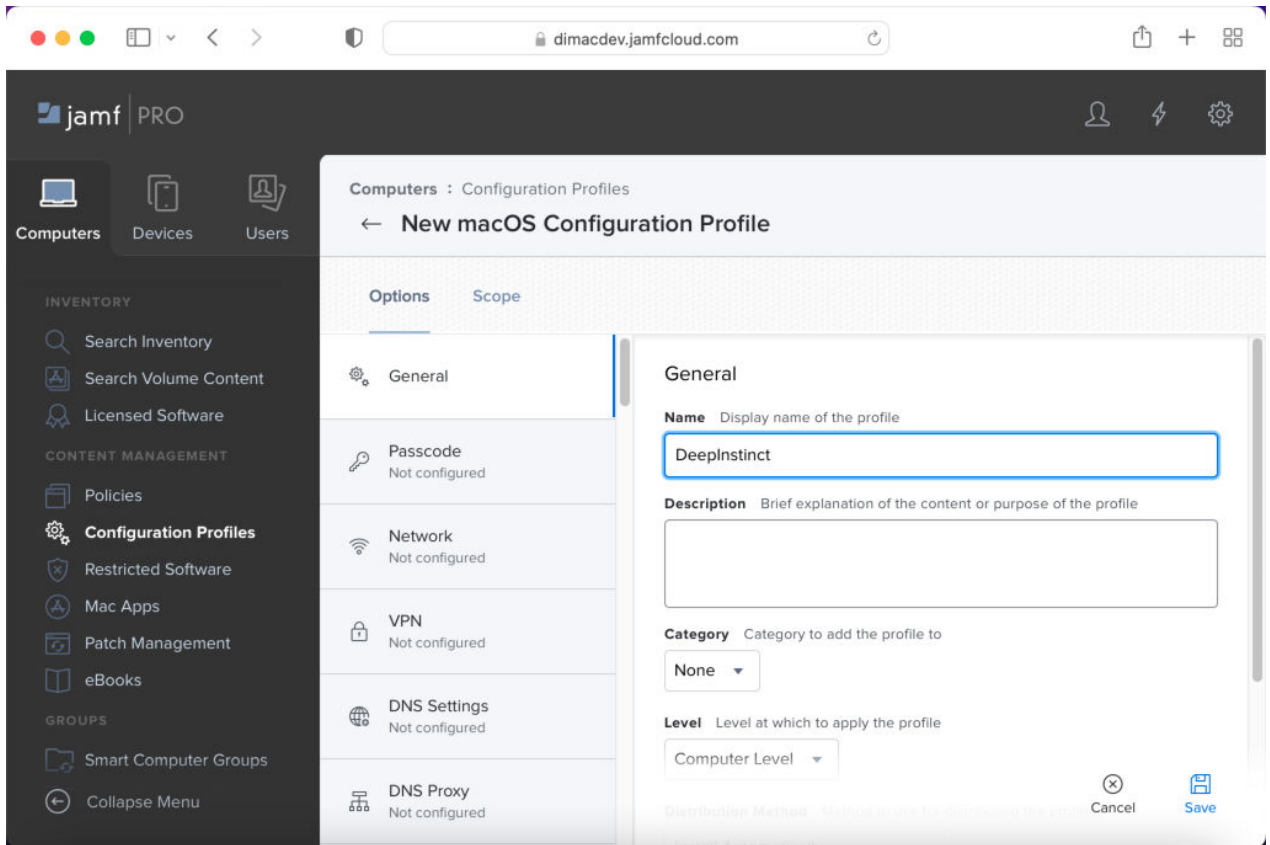
1. Start Jamf Pro.



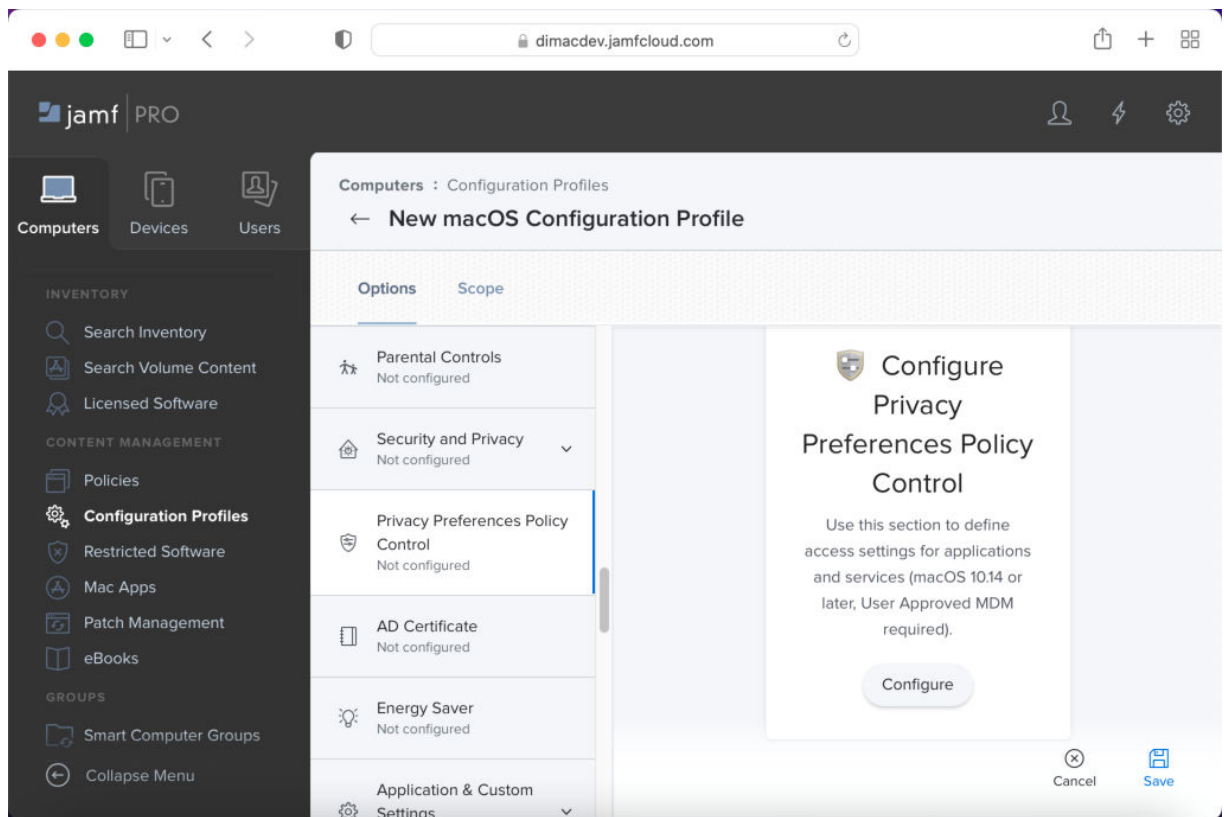
2. In the left pane, click **Computers** → **Configuration Profiles**.



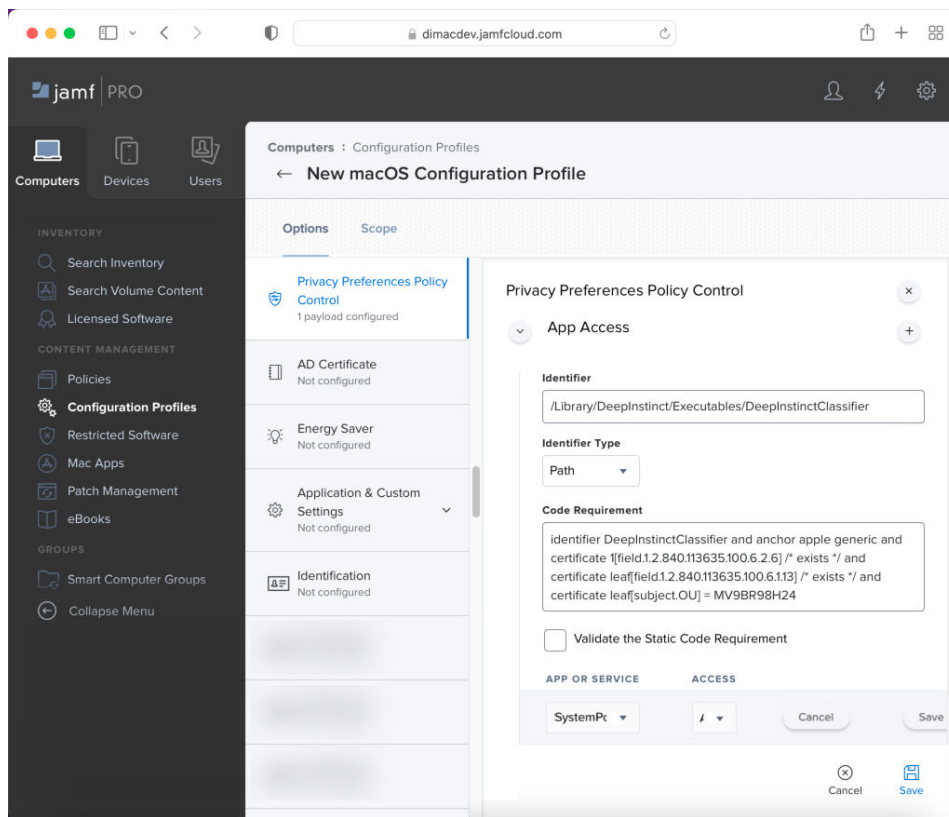
3. Click **New**, and type **DeepInstinct** as the name of the profile.



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 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.

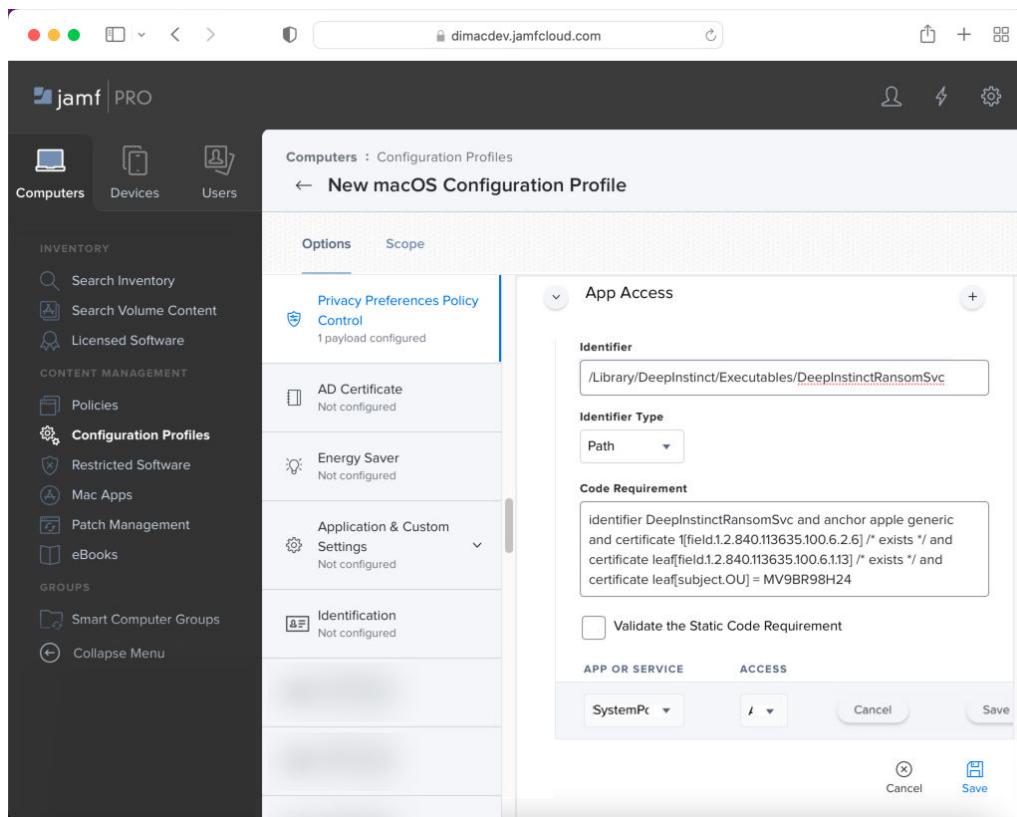
g. Select the **SystemPolicyAllFiles** service and set the access to Allow.

h. Click **Save** to save the Apple service and then click **Save** to save the Configuration Profile.

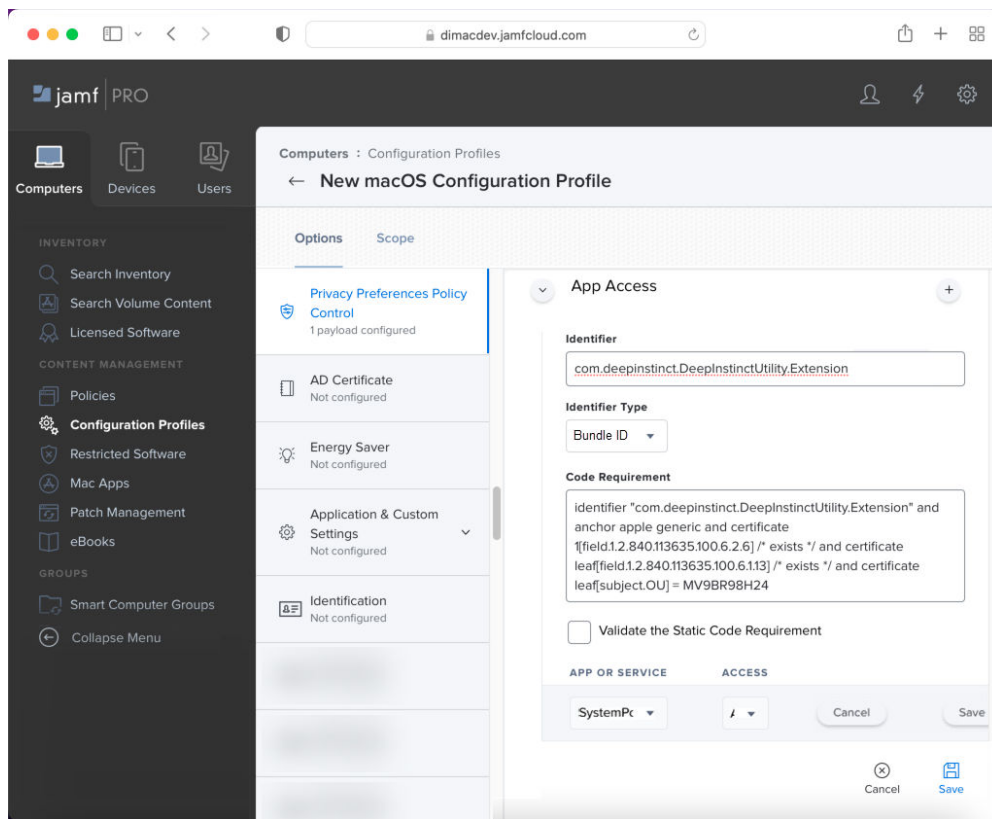
5. Configure the second Full Disk Access Permission, as follows:

a. Click **Edit**, and then click **+** for App Access.

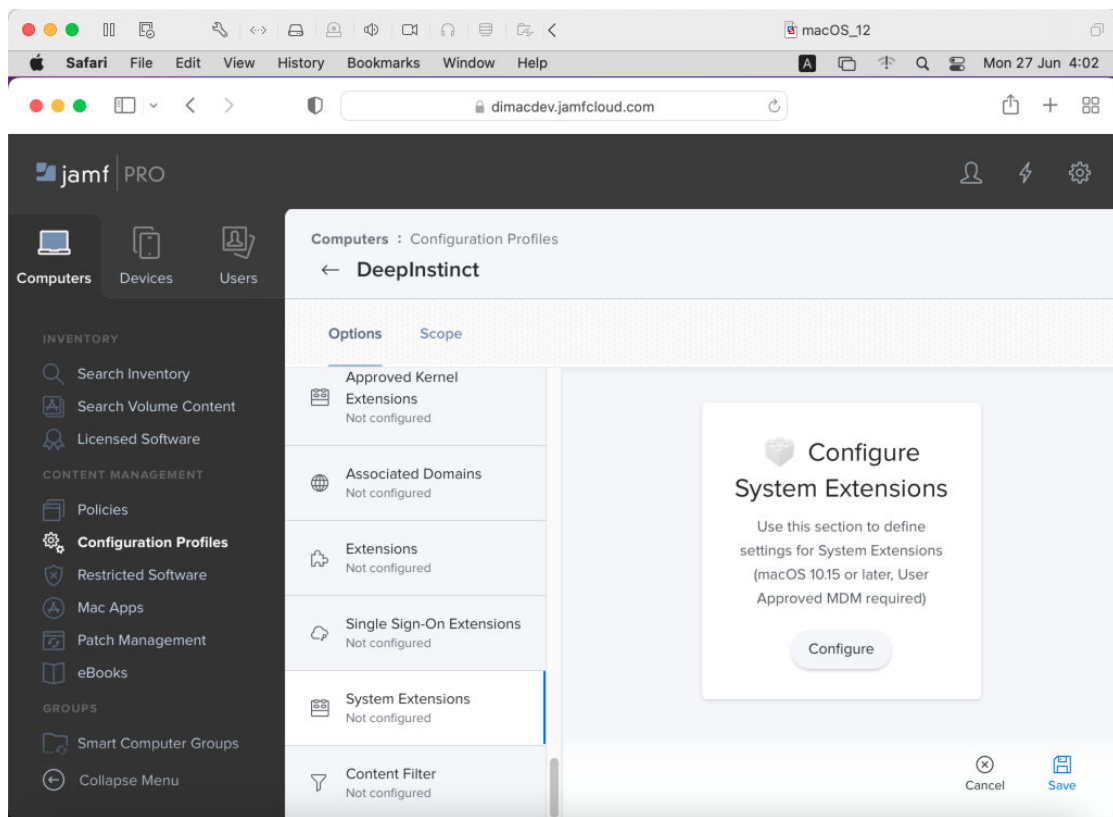
b. Scroll down to the new App Access entry.



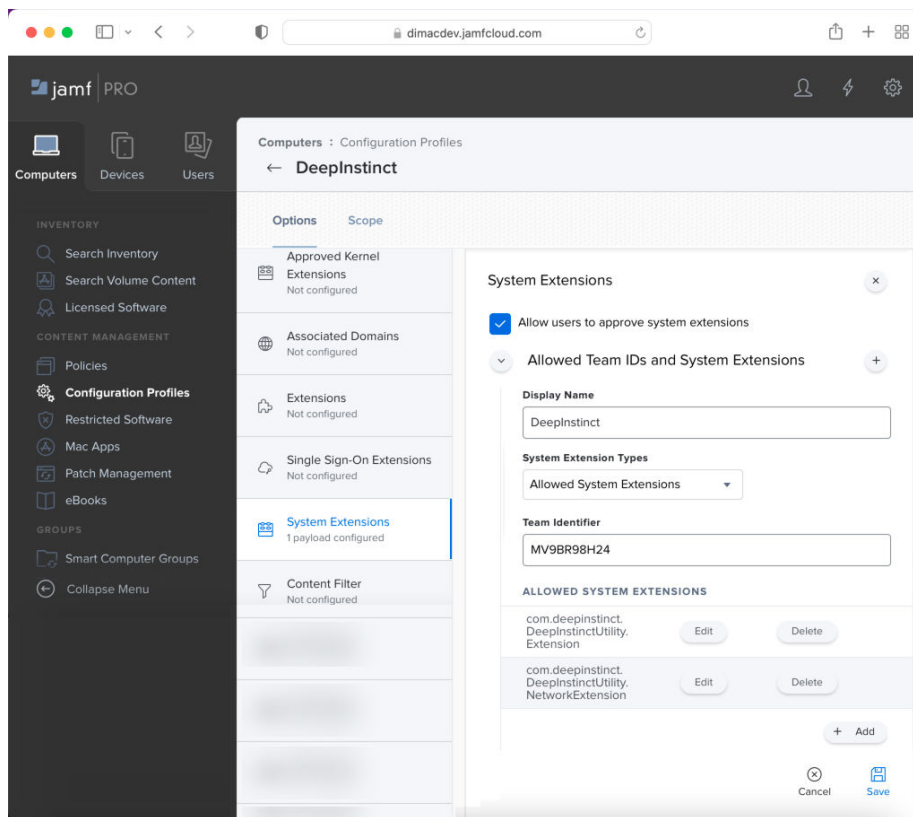
- c. Enter the identifier. Type or copy the following: `/Library/DeepInstinct/Executables/DeepInstinctRansomSvc`
 - d. Set the identifier type to Path.
 - e. Enter the code requirement. Type or copy the following: `identifier DeepInstinctRansomSvc and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* 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.



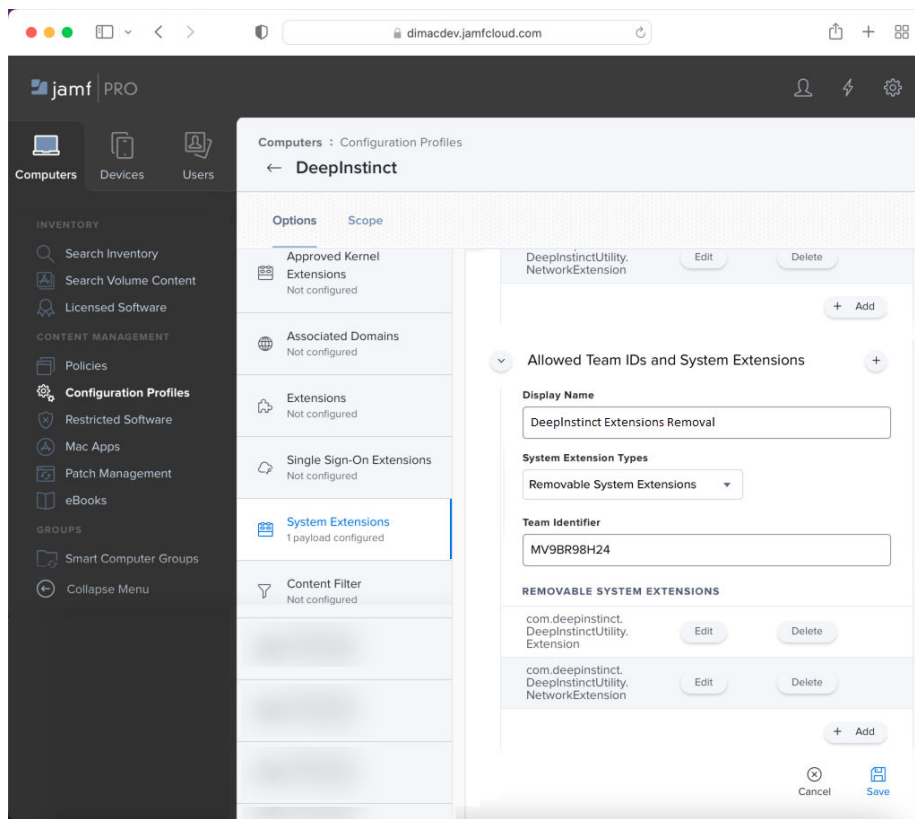
- c. Enter the identifier. Type or copy the following: `com.deepinstinct.DeepInstinctUtility.Extension`
 - d. Set the identifier type to **Bundle ID**.
 - e. Enter the code requirement. Type or copy the following: `identifier "com.deepinstinct.DeepInstinctUtility.Extension" and anchor apple generic and 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.



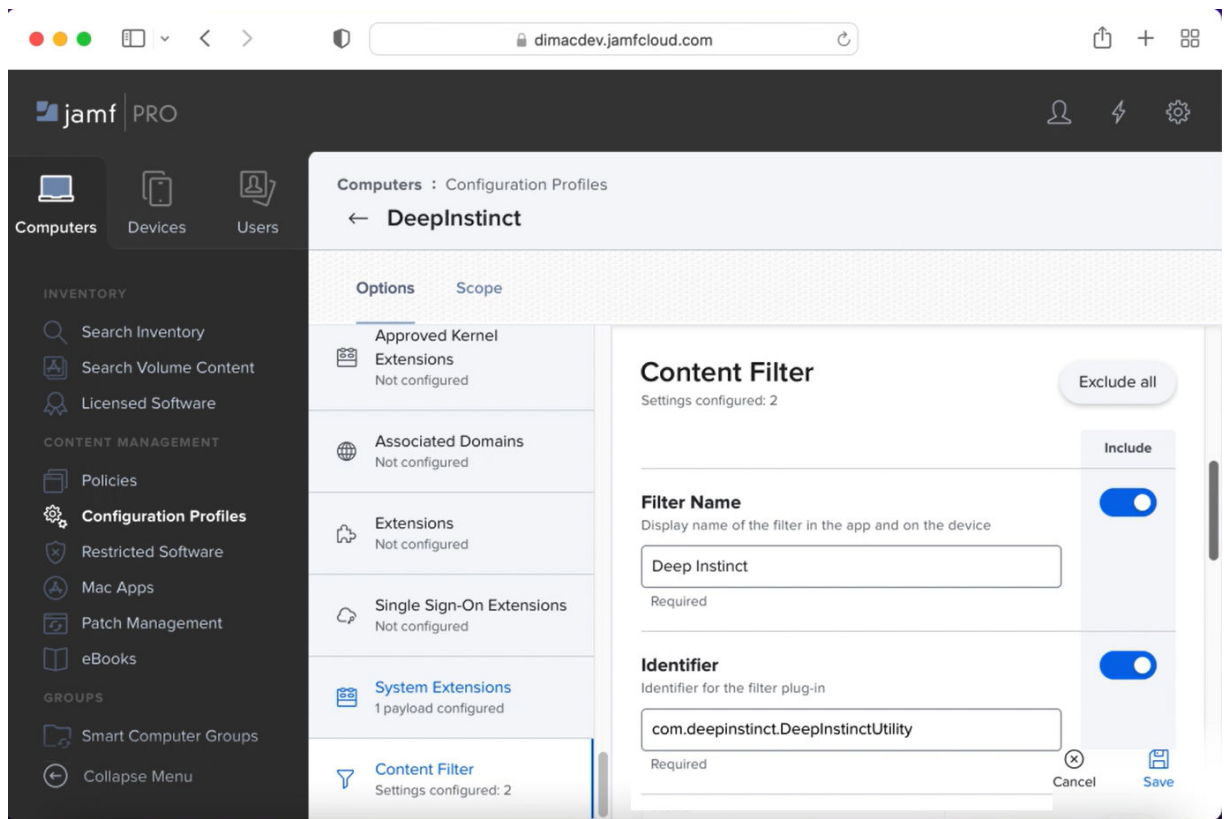
b. Click **Configure**.



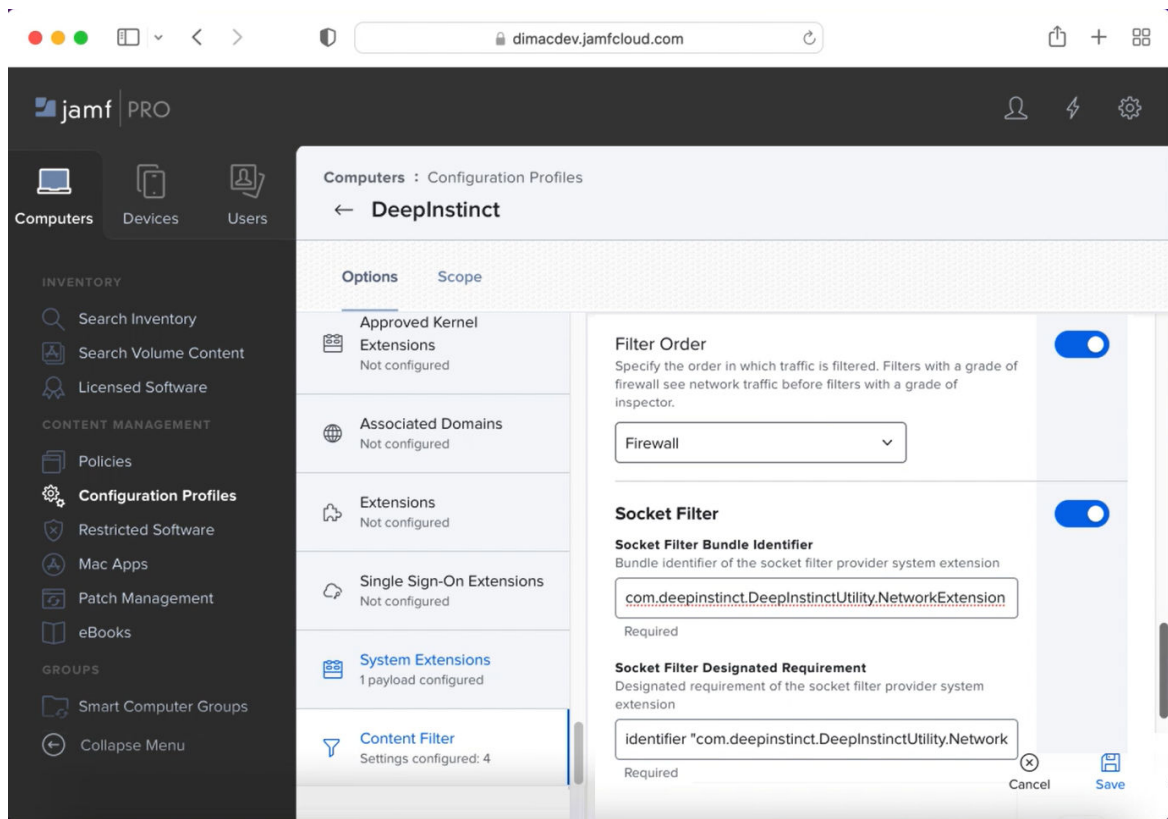
- c. Type "DeepInstinct" as the Display Name.
 - d. Select Allowed System Extensions for the System Extension Types.
 - e. Enter the Team Identifier. Type or copy the following: MV9BR98H24
 - f. Click Add and enter the first System Extension. Type or copy the following: `com.deepinstinct.DeepInstinctUtility.Extension`
 - 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 **+** 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.

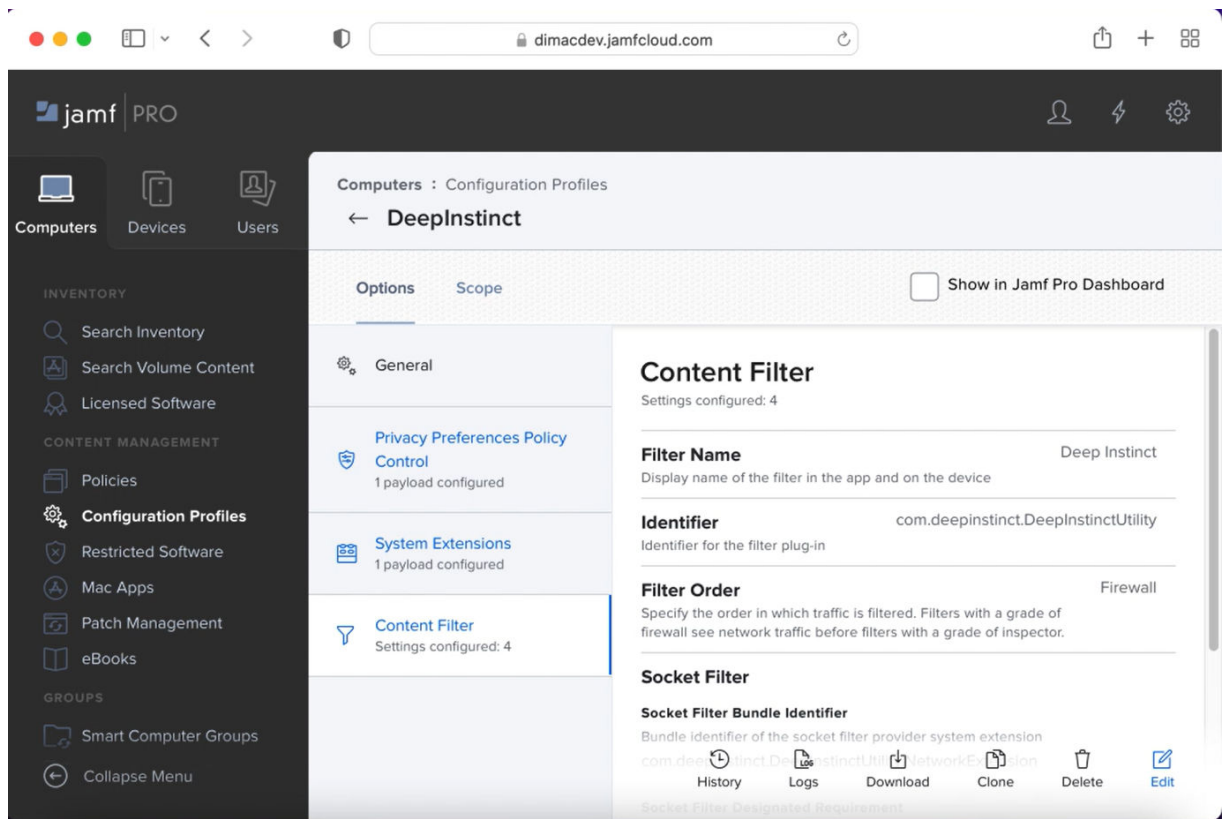


- b. Type **Deep Instinct** as the Filter Name.
- c. Enter the Identifier. Type or copy the following: `com.deepinstinct.DeepInstinctUtility`
- d. Scroll down to Filter Order.



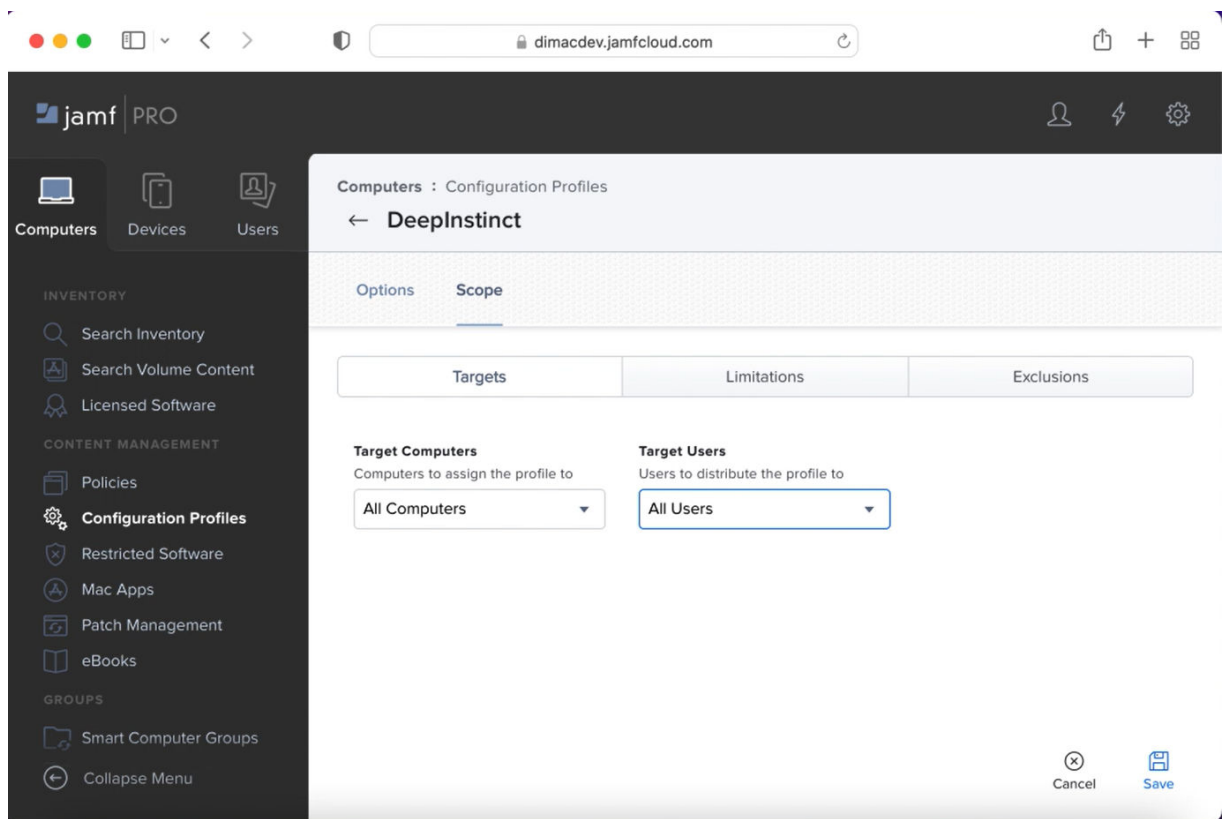
- e. Select Firewall for the Filter Order. Verify that Filter Order is enabled by the blue toggle.
- f. Enter the Socket Filter Bundle Identifier. Type or copy the following: `com.deepinstinct.DeepInstinctUtility.NetworkExtension`
- g. Enter the Socket Filter Designated Requirement. Type or copy the 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.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`
- h. Click **Save**.



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. 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 Element	Description	Comment
<server address>	FQDN for the Management Server (D-Appliance)	N/C
<installation token>	ID of the installation token as displayed in the macOS Deployment Resources screen	N/C
<tag>	Adds a tag associated with the deployed devices	<ul style="list-style-type: none"> ■ Optional ■ Use quotation marks to enter values with spaces or special characters ■ The Device Tag must comply to the following: <ul style="list-style-type: none"> ■ Maximum length is 256 characters ■ Case sensitive ■ Valid characters: <ul style="list-style-type: none"> ■ Letters (a-z, A-Z) ■ Numbers (0-9) ■ Spaces representable in UTF-8 ■ Special characters: + - = . _ : / @ <p>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.</p>

Command Element	Description	Comment
-disabled	D-Client is disabled during the installation when this is included in the command. 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

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:

```
#!/bin/sh

## postinstall

hdiutil attach -nobrowse /private/tmp/DeepInstinct.dmg

sudo sh /Volumes/Deep\ Instinct/installer.sh customer.deepin-
stinctweb.com -token 12345678

hdiutil unmount /Volumes/Deep\ Instinct/

#delete file

rm -rf /private/tmp/DeepInstinct.dmg

exit 0 ## Success
```

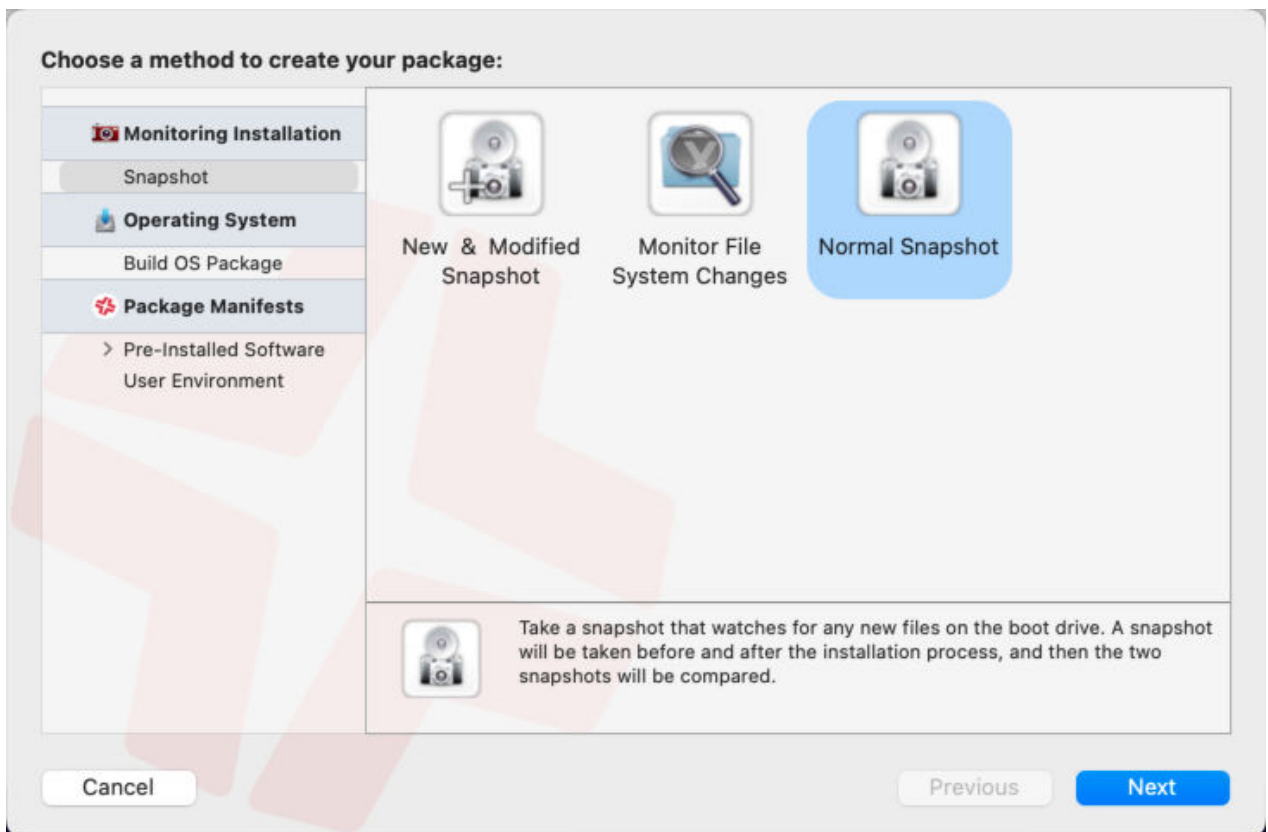
5. Save this file, as the content of this file can be copied to the Jamf Package when you create the package, as detailed in [Creating a Jamf Package for D-Client Deployment](#).

Creating a Jamf package for D-Client deployment

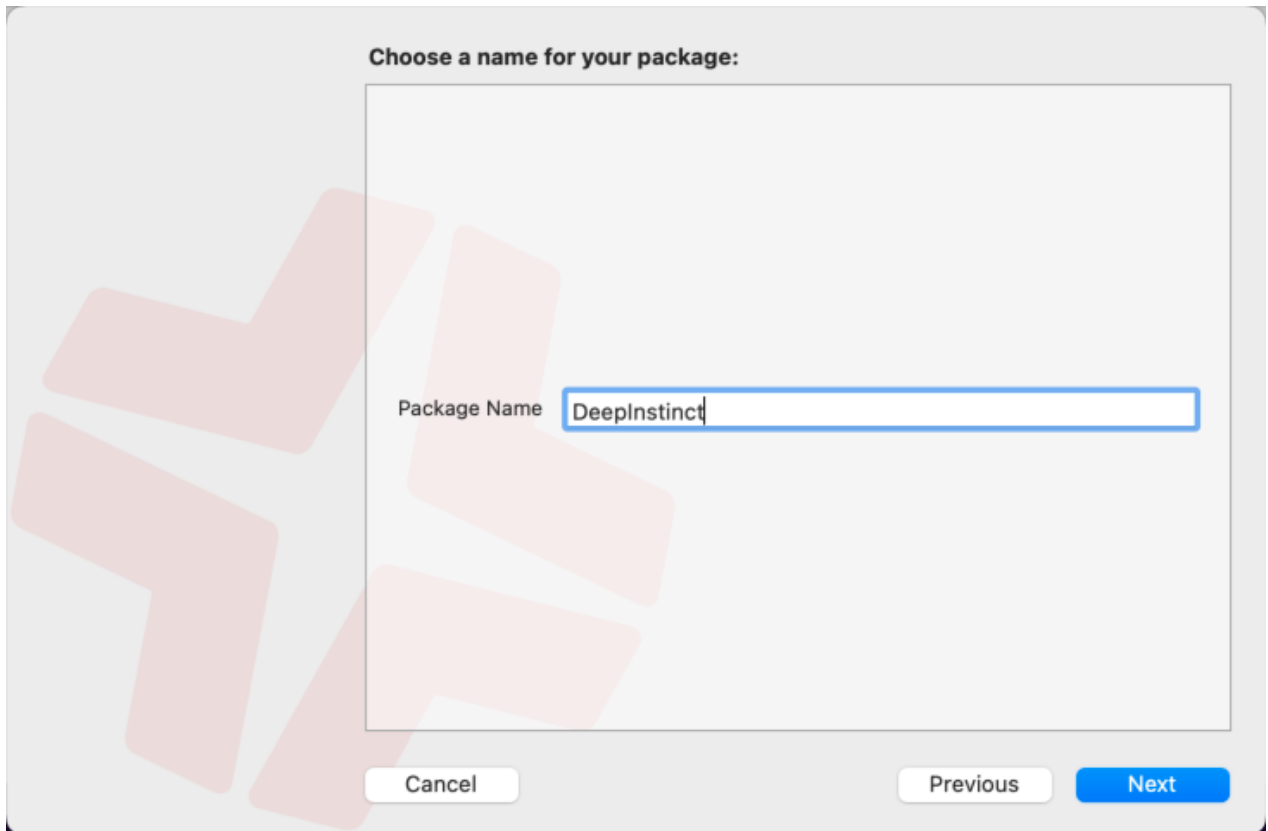
The Jamf Package with the Jamf Script defines the actions that are performed on a macOS device during deployment.

To create a Jamf package for deployment:

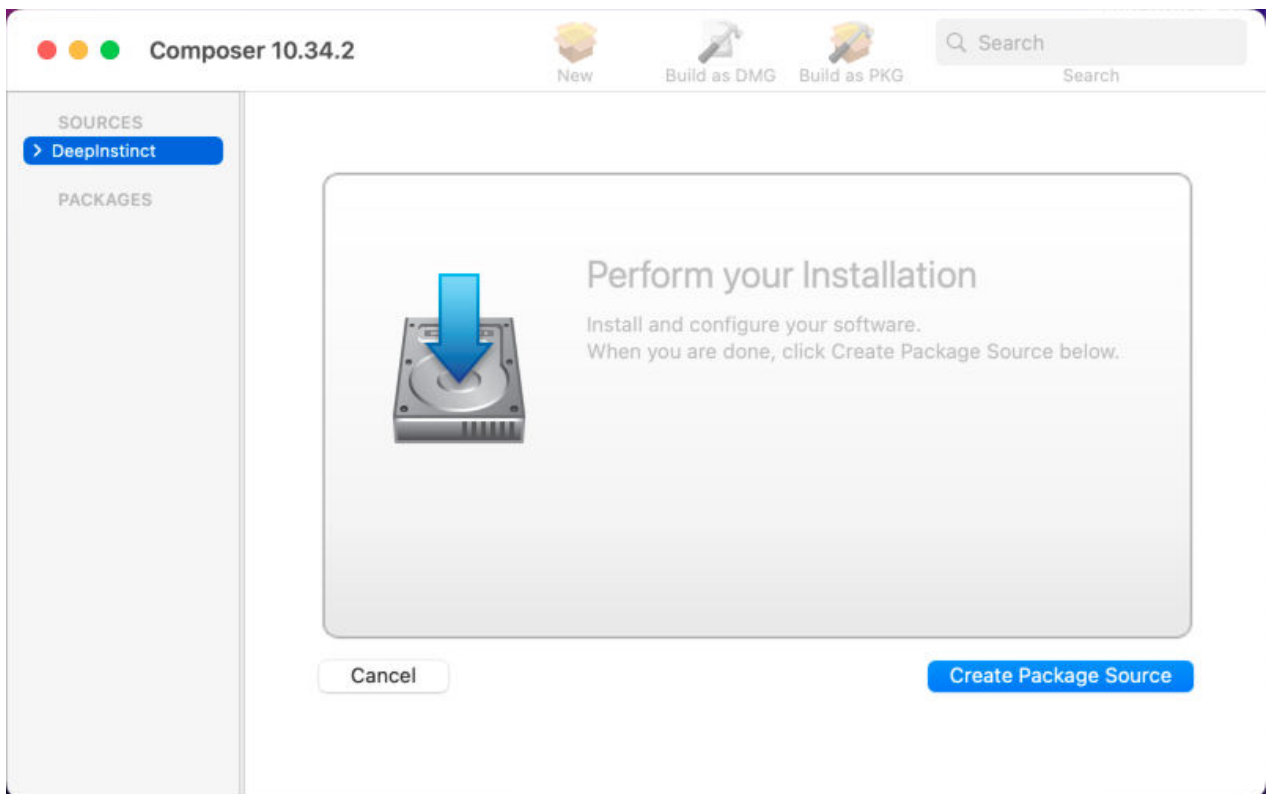
1. Download the installation file from the [macOS Deployment Resources](#) screen.
2. Save the installation DMG file to the folder /private/tmp.
3. Create the Jamf Script, as described in [Create a Jamf Script](#).



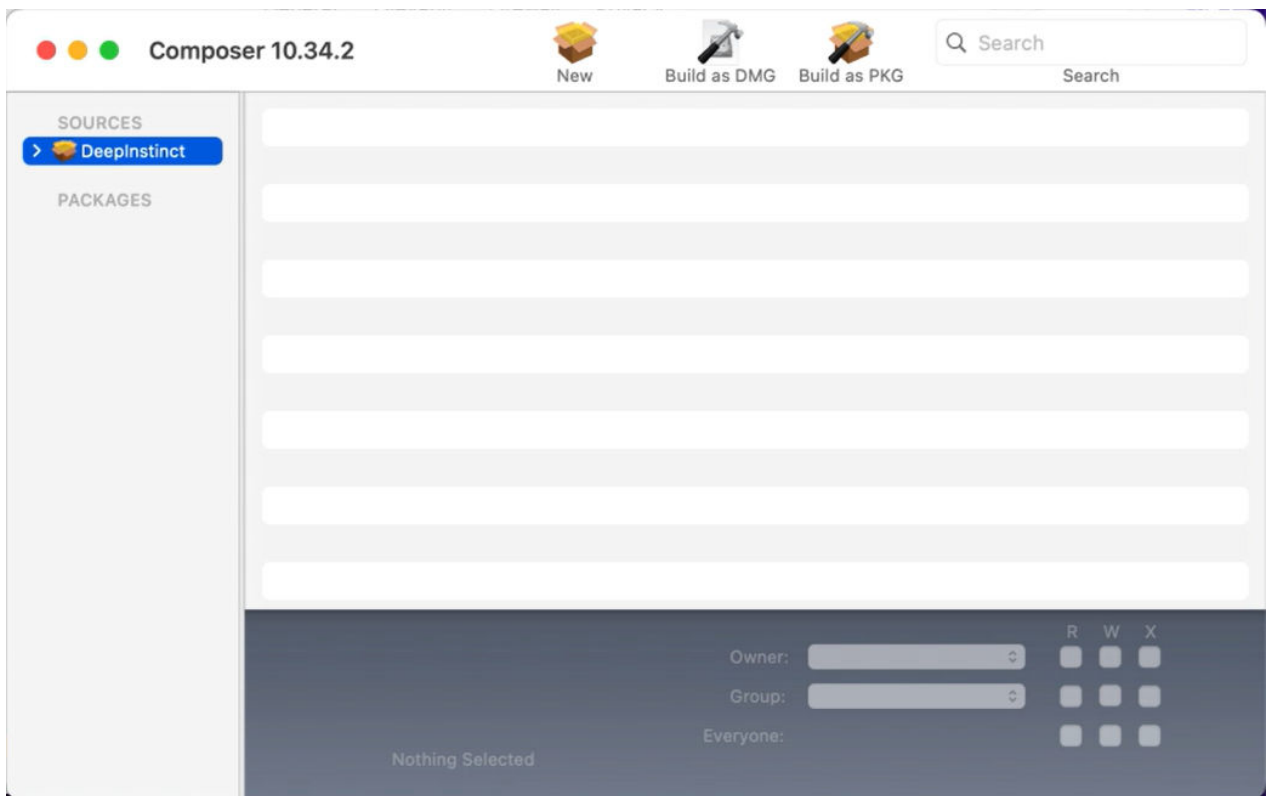
4. Start Jamf Composer to create a new package.
5. Select Normal Snapshot and click **Next**.



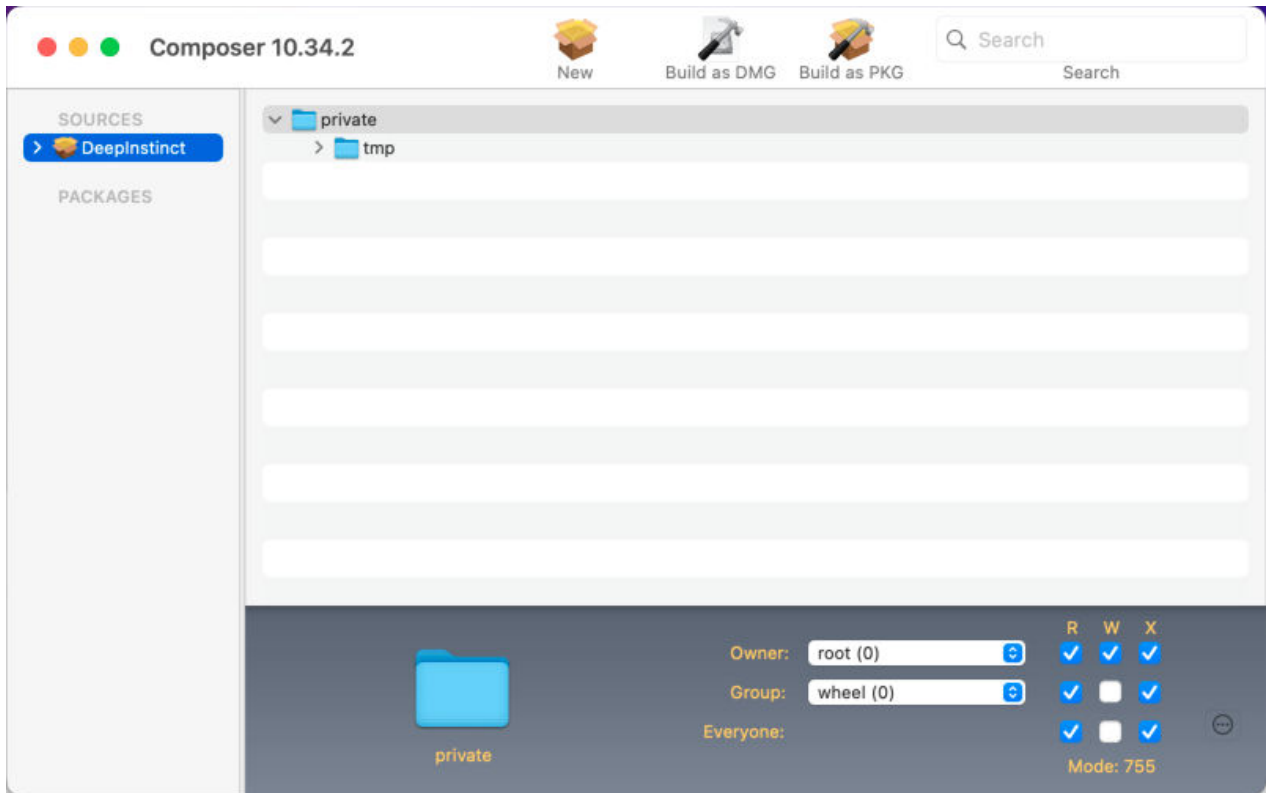
6. Type **DeepInstinct** as the name of the package, and click **Next**. A progress bar is displayed to indicate the progress of the Before Snapshot.




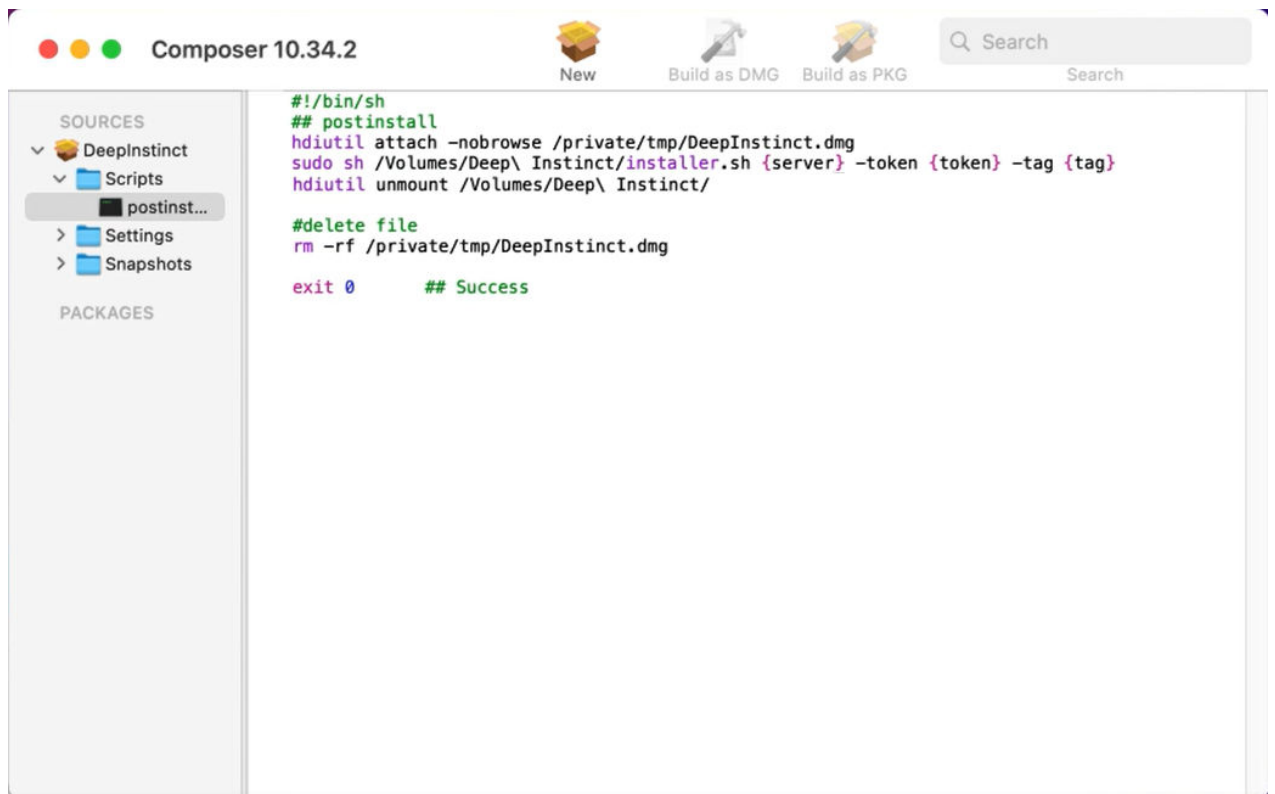
- Click **Next**, and a progress bar is displayed to indicate the progress of the After Snapshot. Once completed, an icon to the left of DeepInstinct Source in Composer is displayed.




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



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 → Scripts → 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  on the top of the screen.
- c. Select **Desktop** as the location and click **Save**.

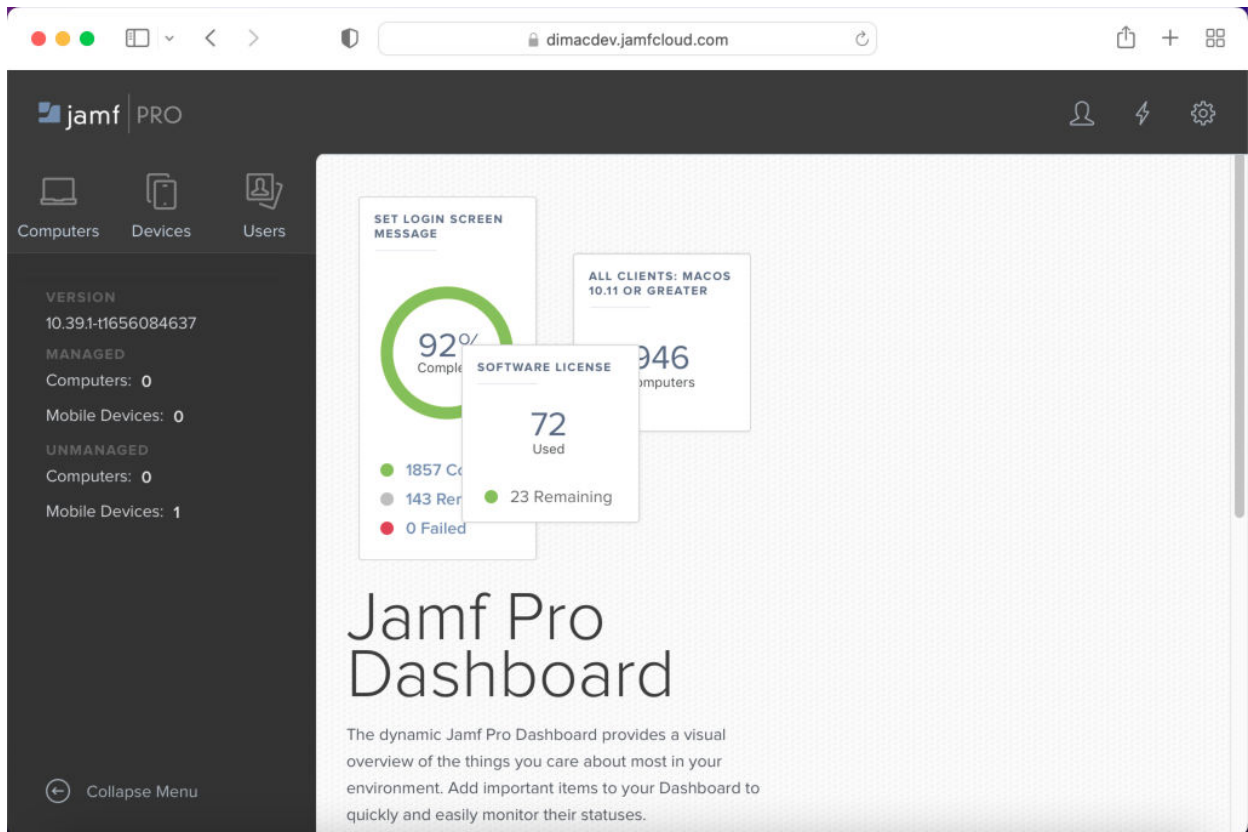
Creating a Jamf policy for D-Client deployment


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:

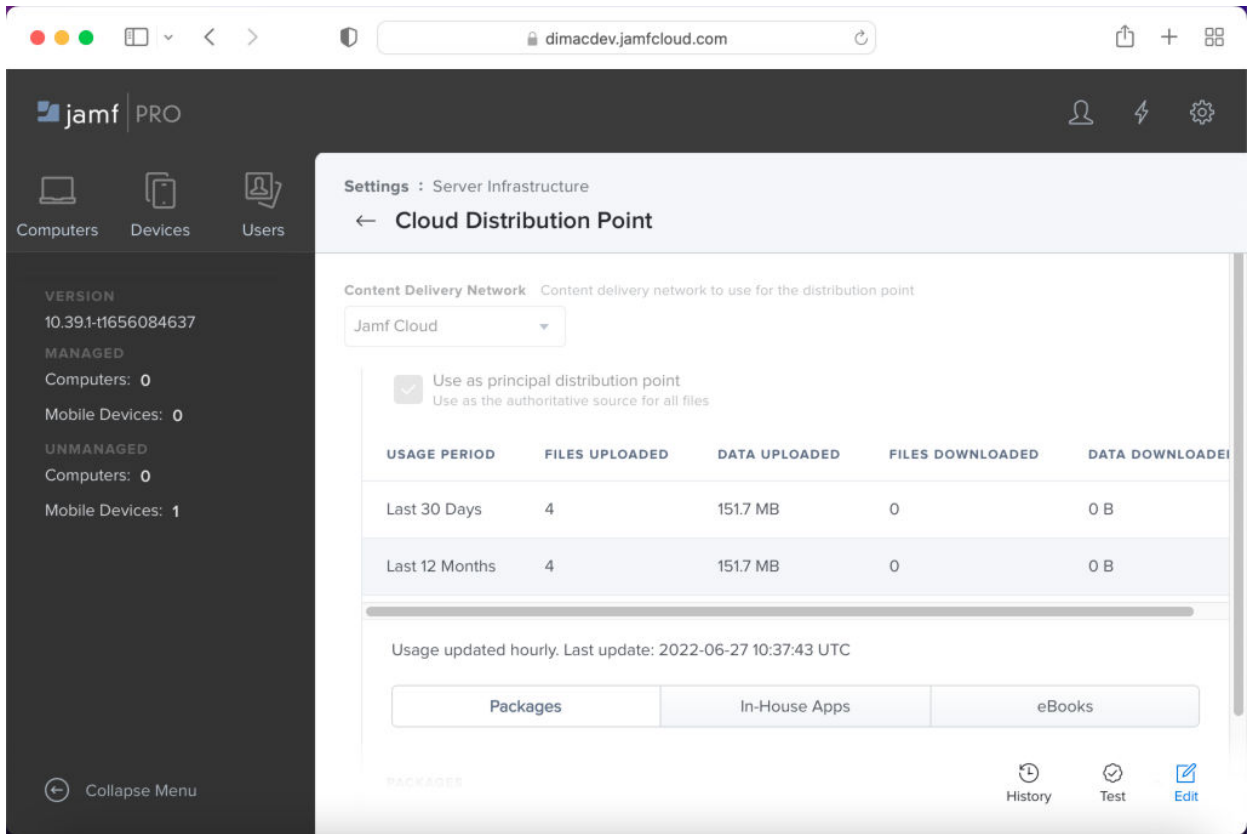
- Configure Jamf Console
- Upload Jamf Package
- Create a new Jamf Policy
- Configure the policy
- Define the scope for deployment


To create a Jamf policy for deployment:

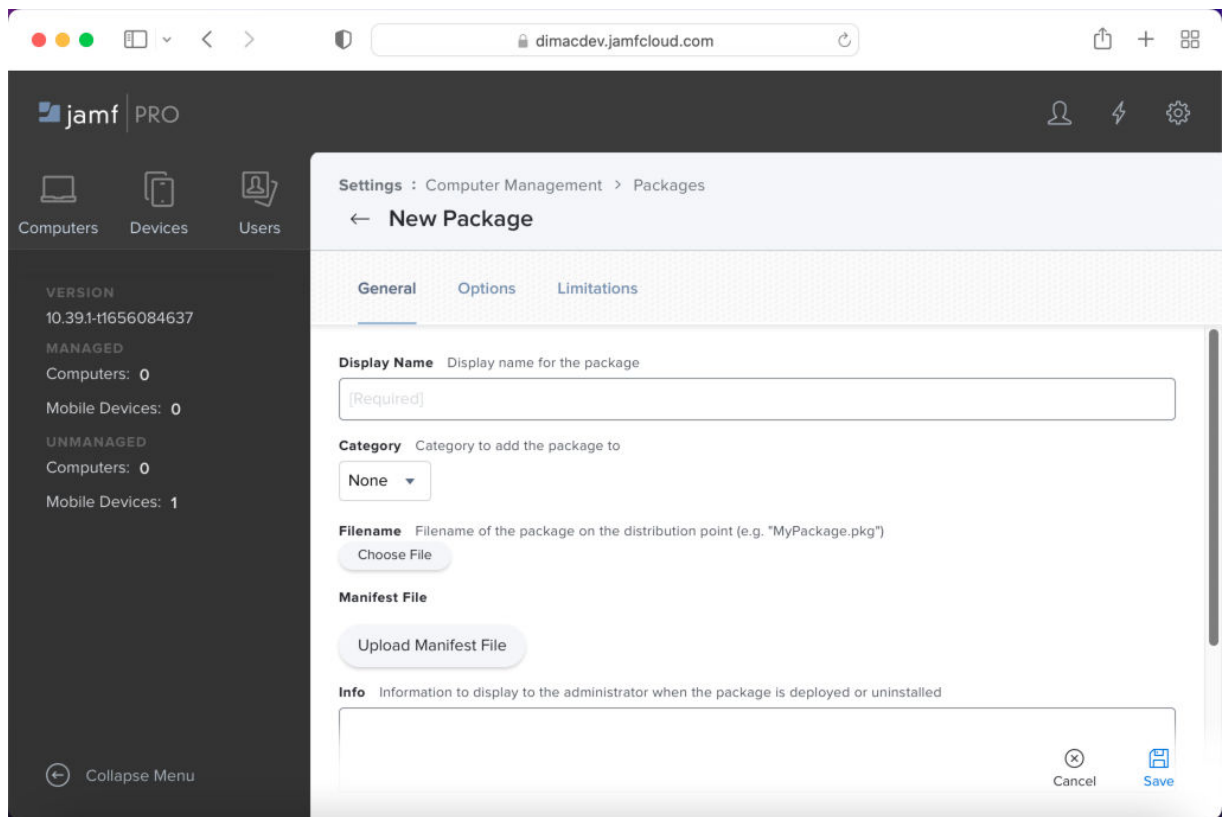
1. Start Jamf Pro.



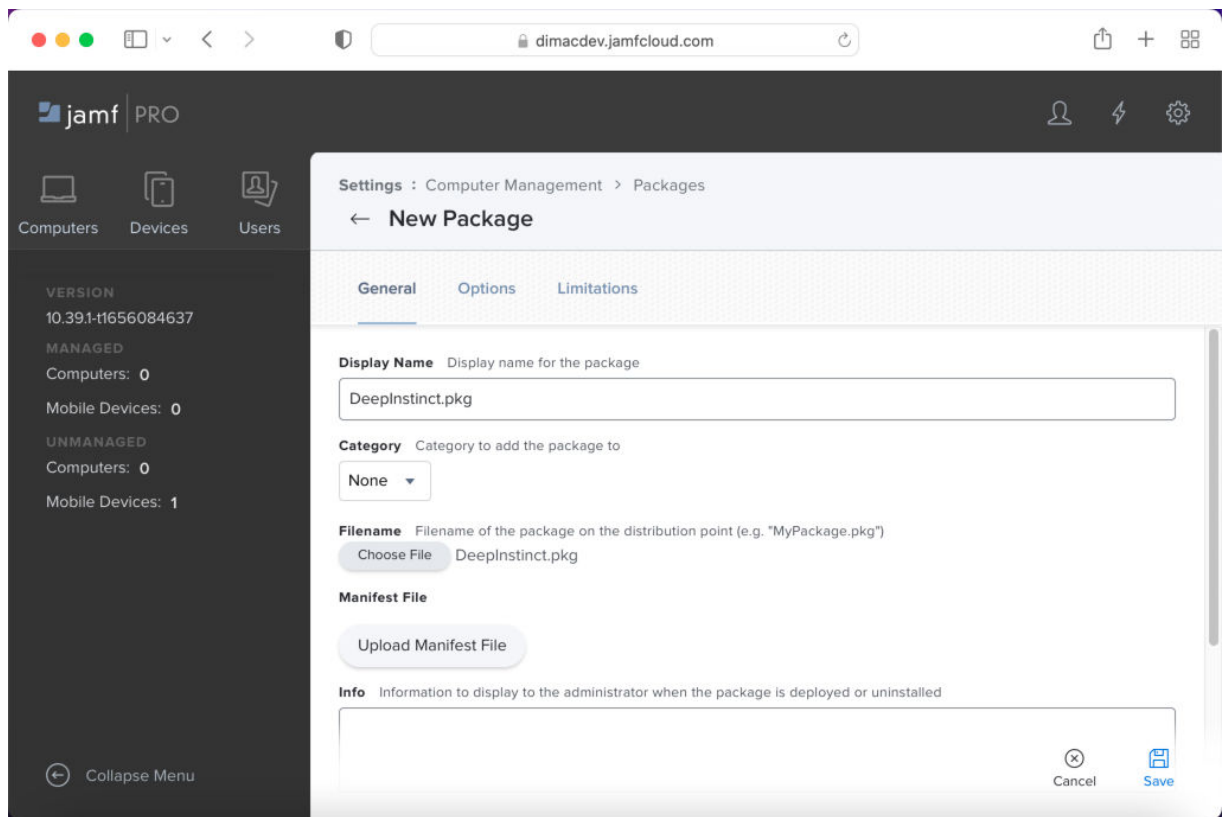
2. Click  on the top-right of the screen.
3. Click Server Infrastructure → Cloud Distribution Point.
4. From the Cloud Distribution Point panel, set the Content Delivery Network to **Jamf Cloud**.



5. Upload the [DeepInstinct Package](#), as follows:
 - a. Click  on the top-right of the screen.
 - b. Click [Computer Management](#) → [Packages](#).
 - c. From the New Packages panel, click [New](#).

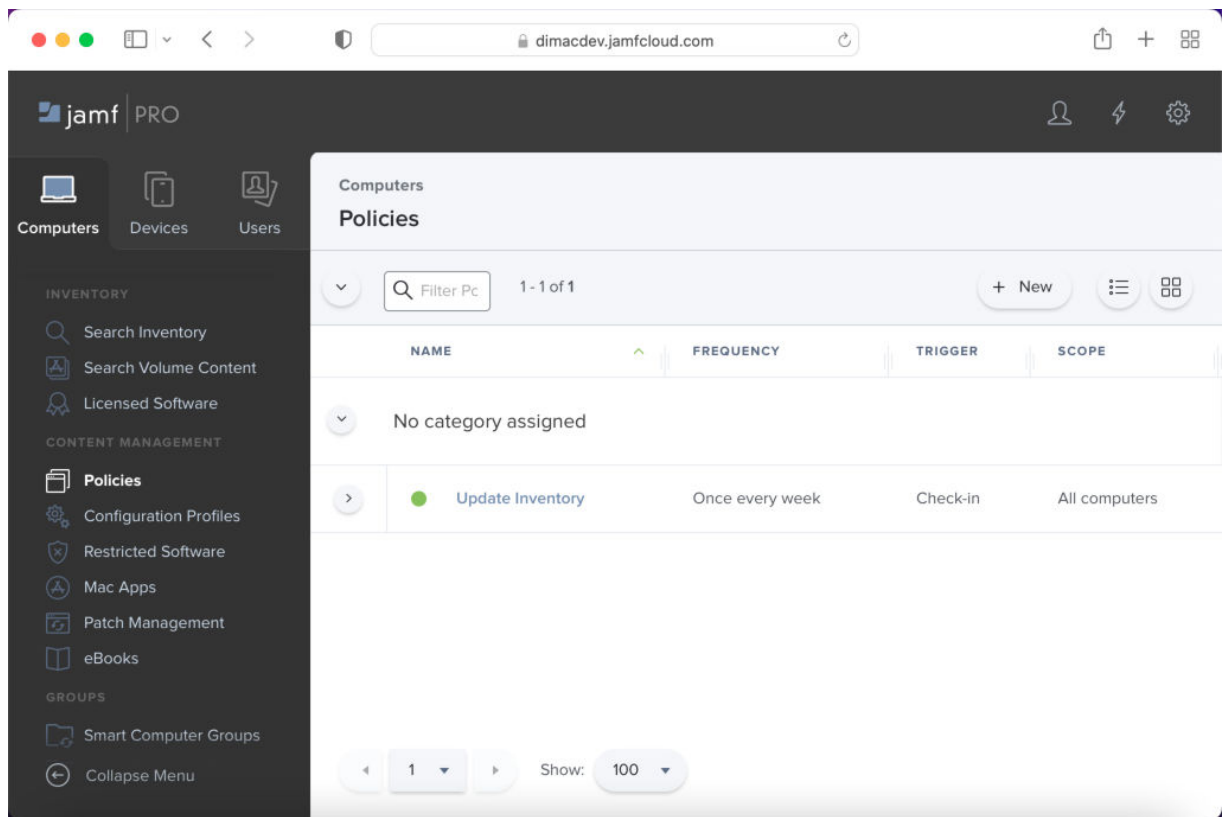


- d. Click **Choose File** for the Filename.
- e. Select **DeepInstinct.pkg** from the Desktop, and click **Upload**. The Display Name changes to **DeepInstinct.pkg**.

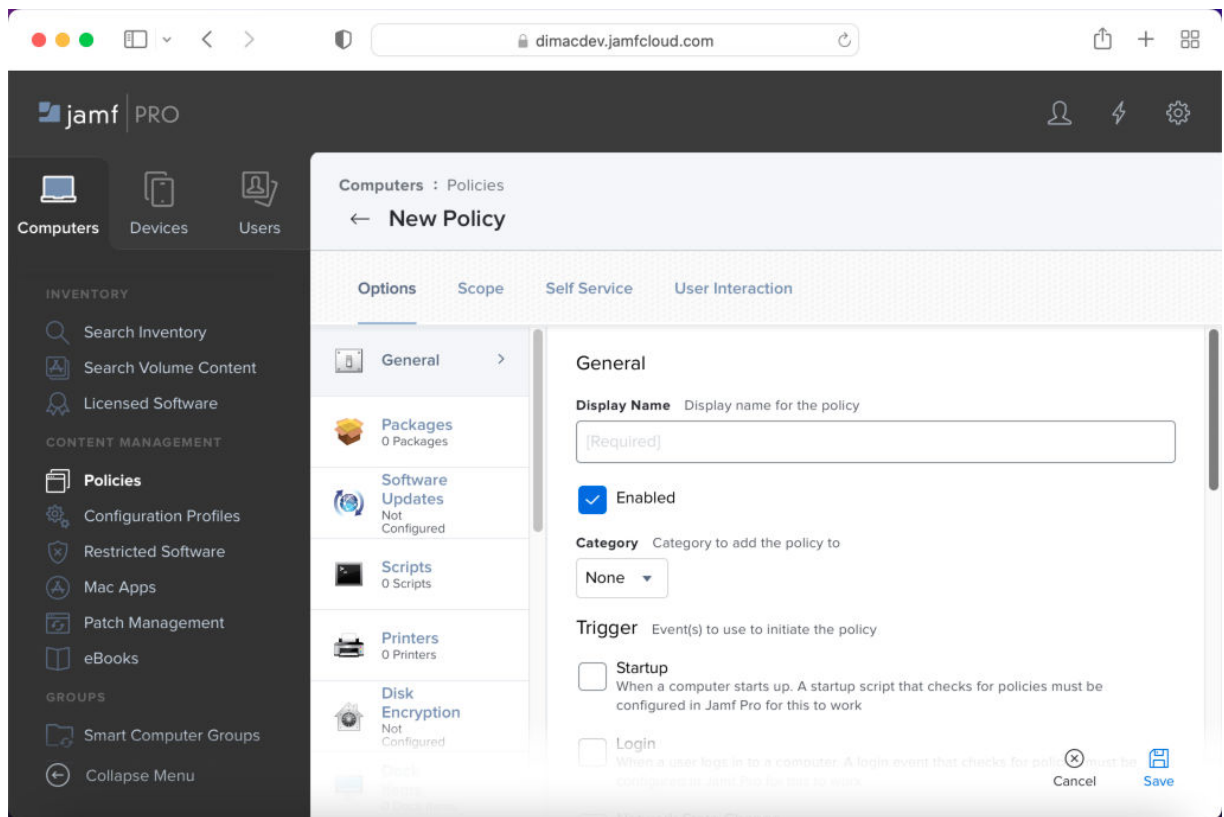


f. Click **Save**.

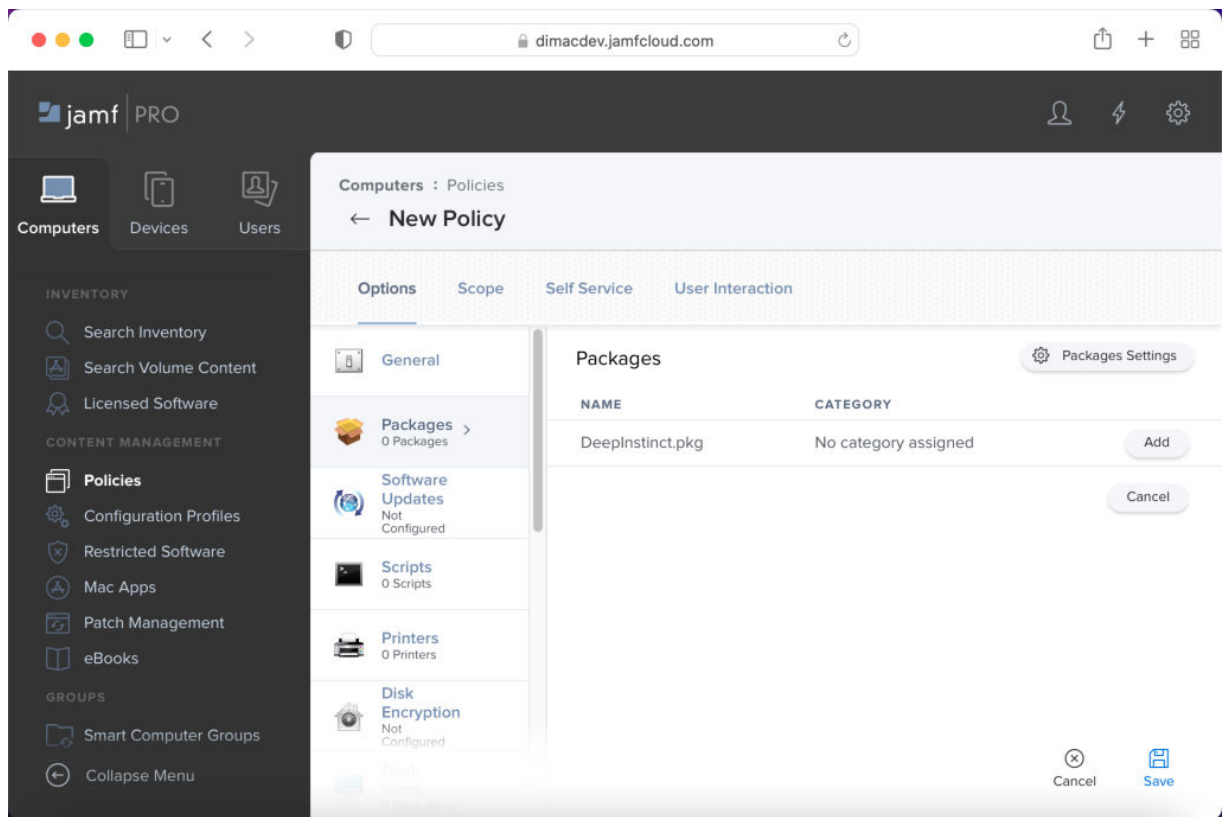
6. Once the package is uploaded, create a new policy:
 - a. In the left pane, click **Computers** → **Policies**. The Policies panel opens.



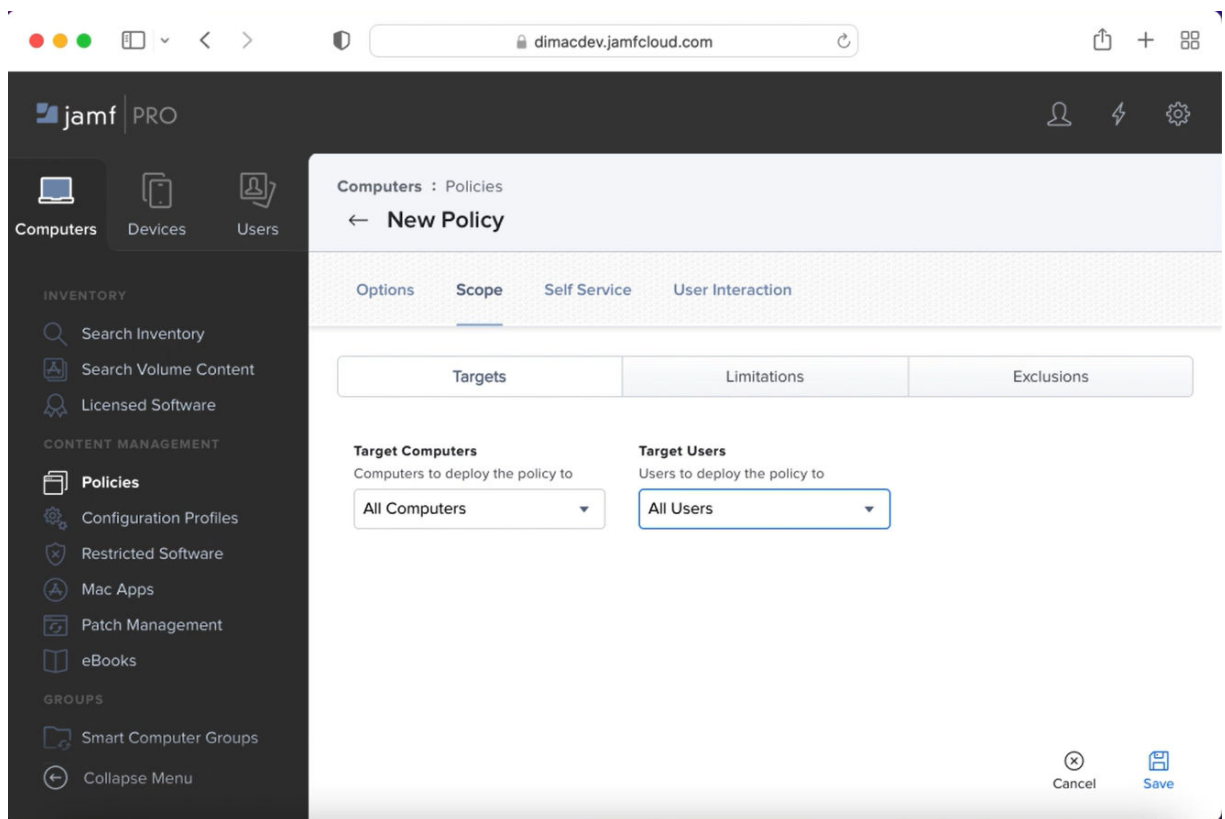
b. From the Policies panel, click **New**.



- 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.



- 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 Element	Description	Comments
<server address>	FQDN for the Management Server (D-Appliance)	N/C
<installation token>	ID of the installation token, as displayed in the macOS Deployment Resources screen	N/C
<tag>	Adds a tag associated with the deployed devices	<ul style="list-style-type: none"> ■ Optional ■ Use quotation marks to enter values with spaces or special characters ■ Maximum length is 256 characters ■ Case sensitive ■ Valid characters: <ul style="list-style-type: none"> ■ Letters (a-z, A-Z) ■ Numbers (0-9) ■ Spaces representable in UTF-8 ■ Special characters: + - = . _ : / @ <p>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.</p>
-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 Element	Description	Comments
-nfs	Starts the D-Client without performing 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:

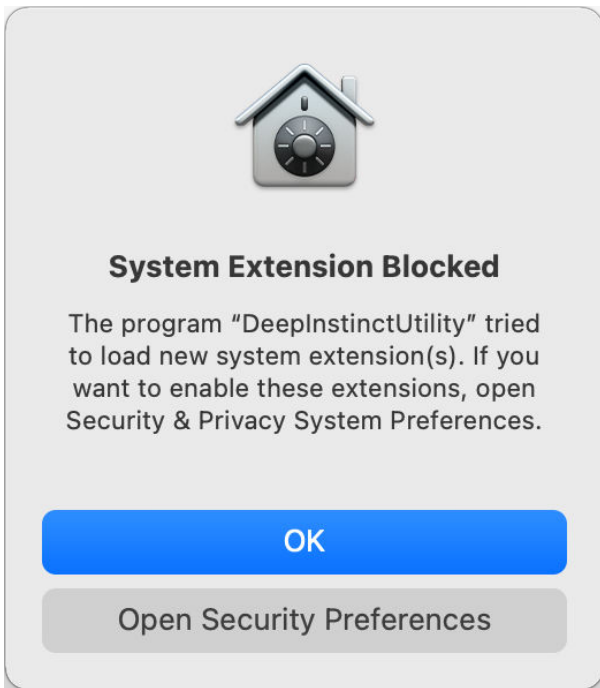
- path = /Users/user/Downloads/
- installation file = 2.4.0.1_DeepInstinct_installer.dmg
- server address = customer.deepinstinctweb.com
- installation token = 12345678

The commands will look like this:

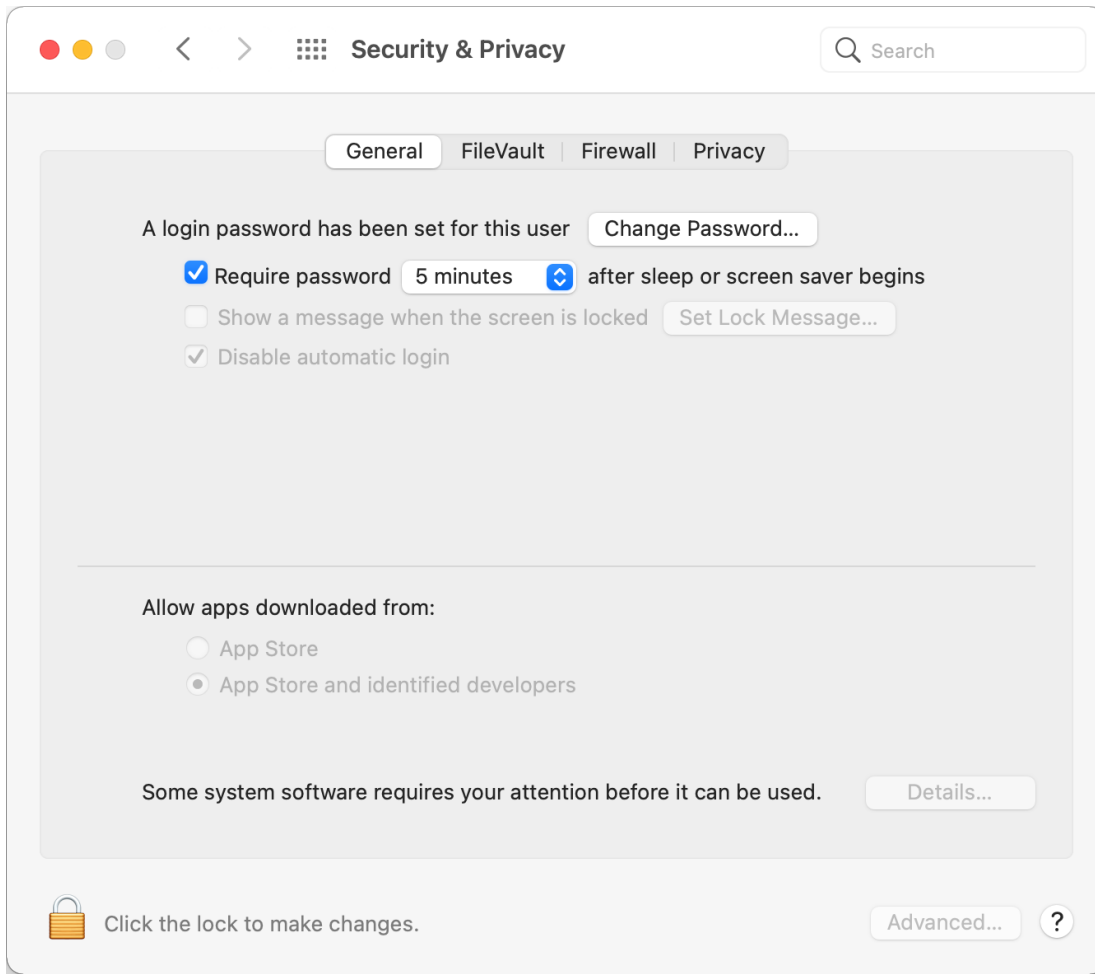
- Macbook-Pro:Desktop user\$ open /Users/user/Downloads/2.4.0.1_DeepInstinct_installer.dmg
- Macbook-Pro:Desktop user\$ sudo "/Volumes/Deep Instinct/installer.sh"customer.deepinstinctweb.com -token 12345678
- Password: Macbook-Pro:Desktop user\$


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.

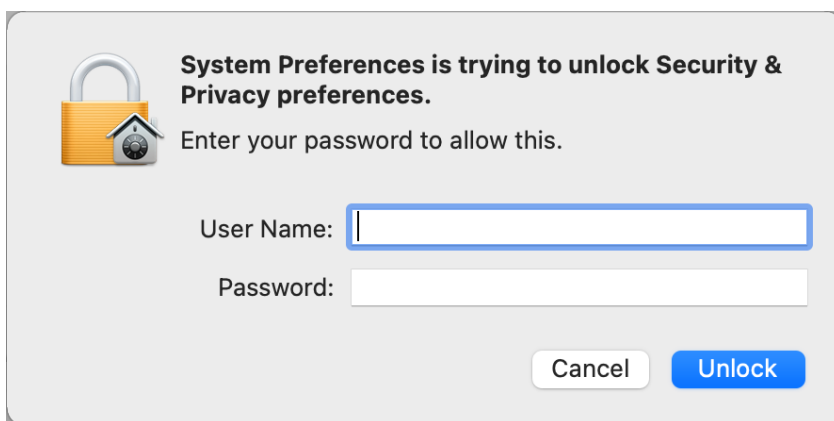
The Deep Instinct extensions must be allowed to load. If permissions are required, the System Extension Blocked message opens and perform the following:



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



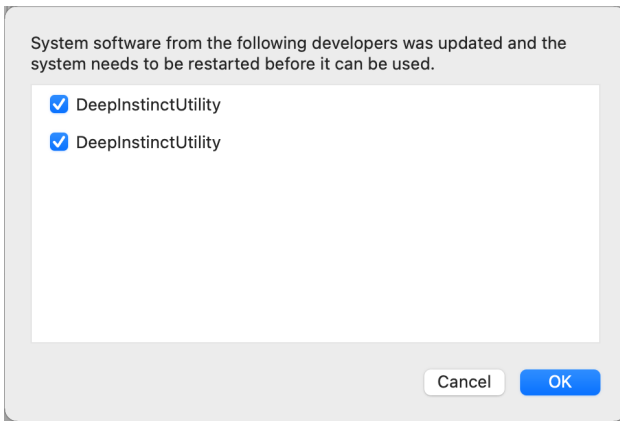
Click the Lock icon  at the bottom left corner of the screen. A dialog box opens for you to enter your administrator credentials.



Enter the administrator's username and password.

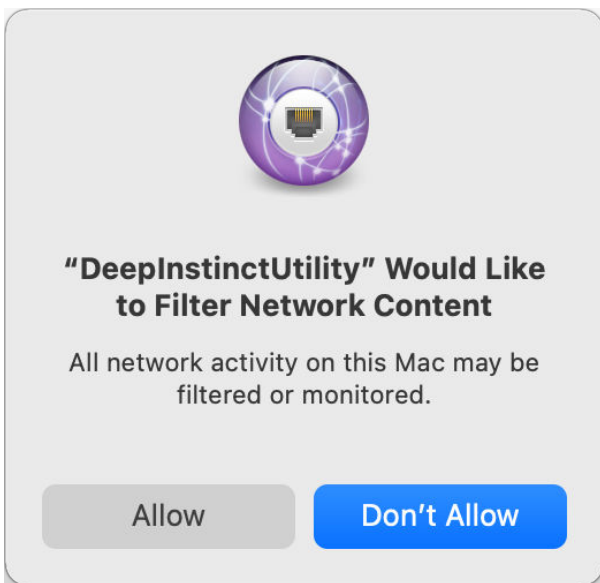
Click Unlock to unlock the Security & Privacy screen.

Click Details to continue.

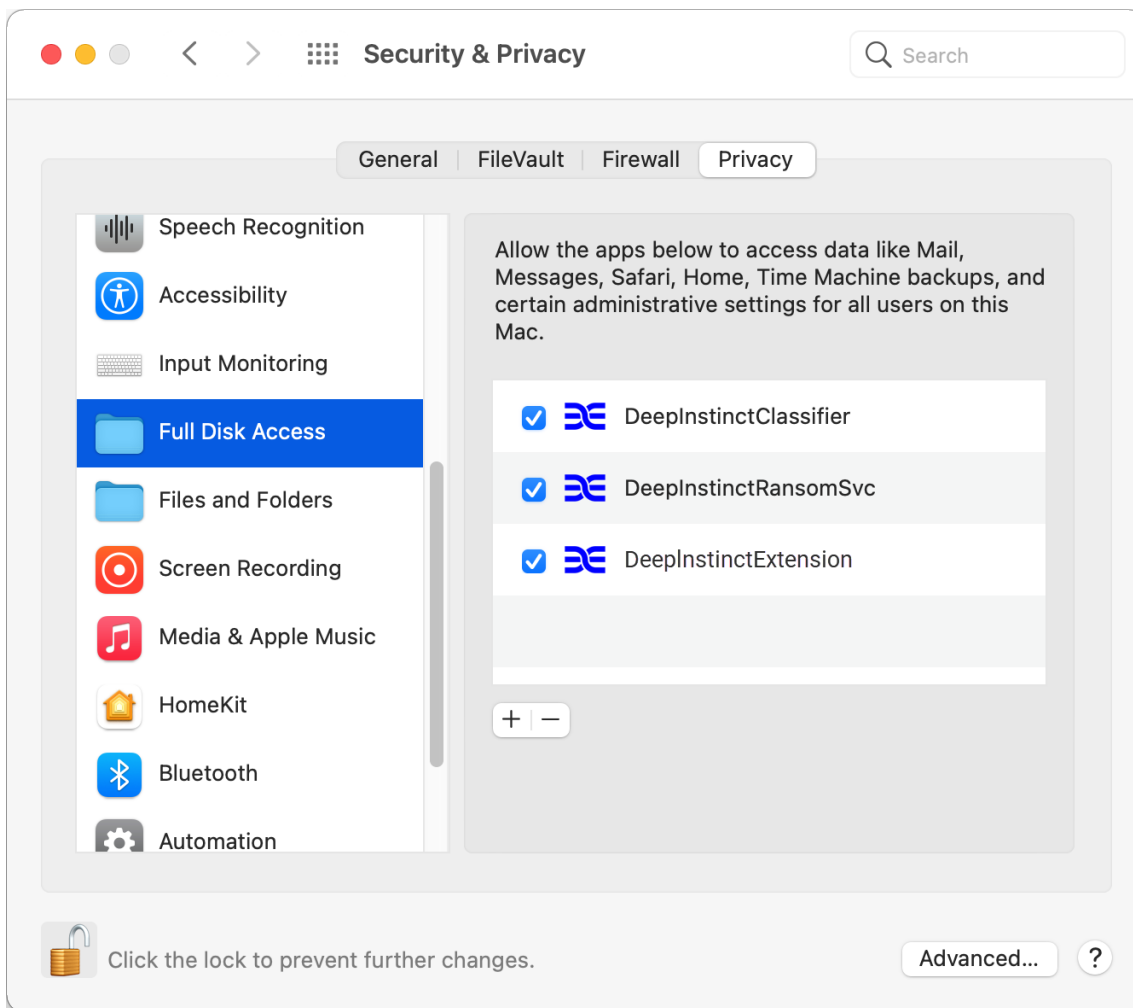


Select all instances of "DeepInstinctUtility" and click OK to permit Deep Instinct to load the required system extensions.

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



For **Full Disk Access Permission**, perform the following:



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](#).

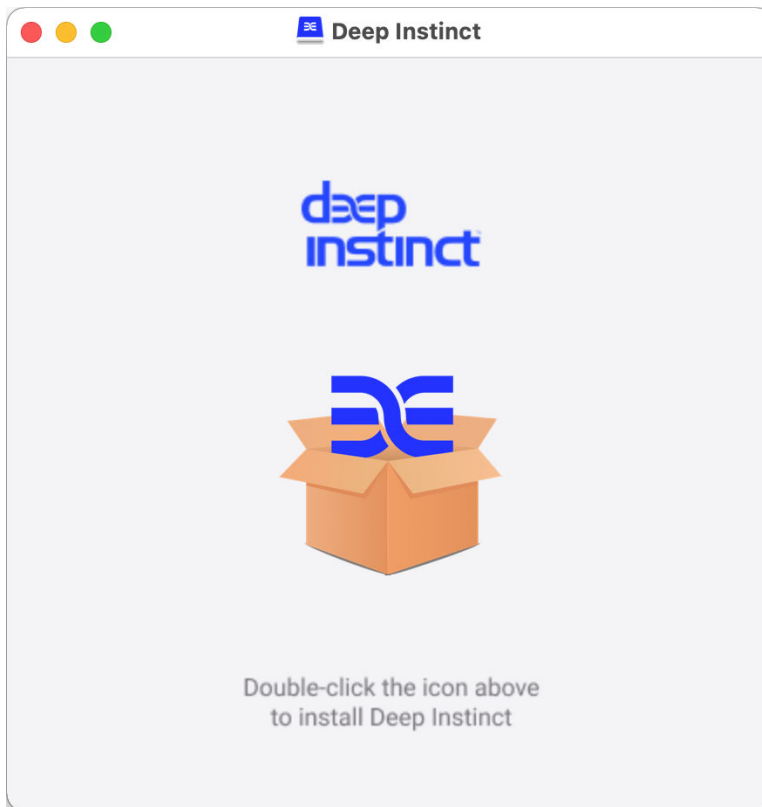
4.3.1.4. D-Client local installation with the Wizard

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:

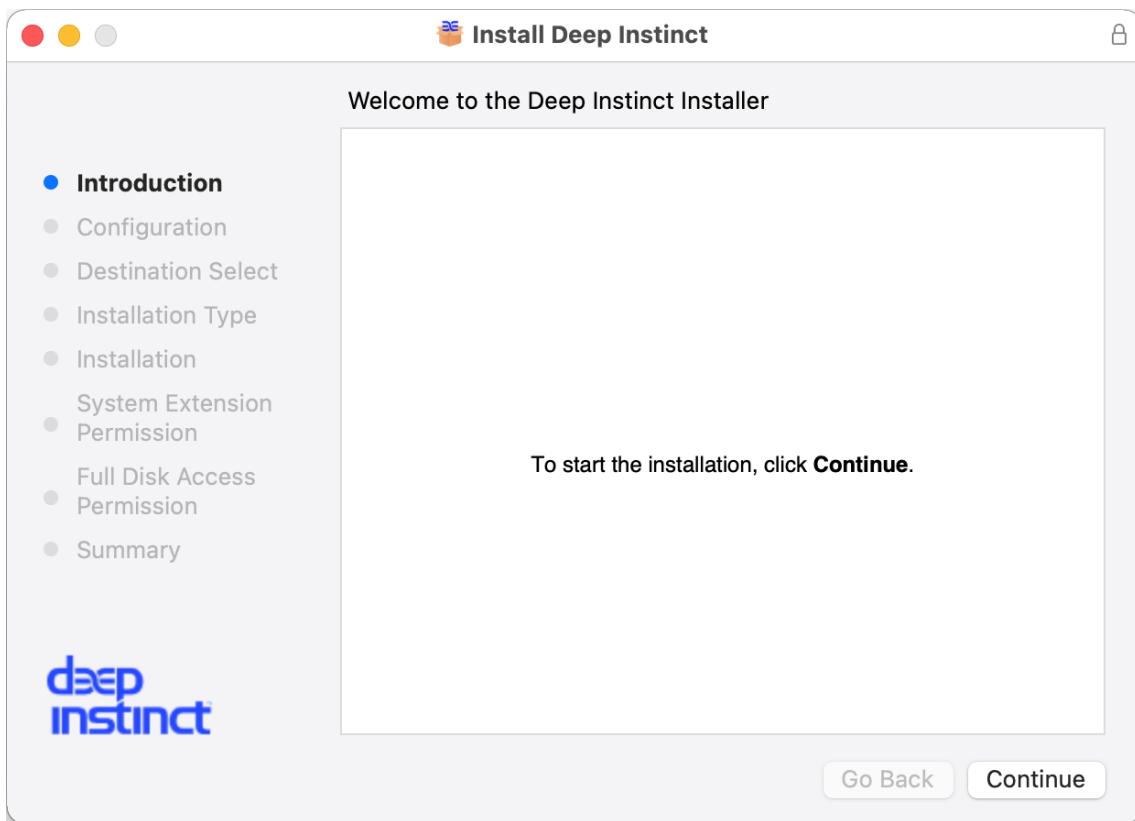
1. Download the installation file from the [macOS Deployment Resources](#) screen and save it to a location where the macOS device has access.

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

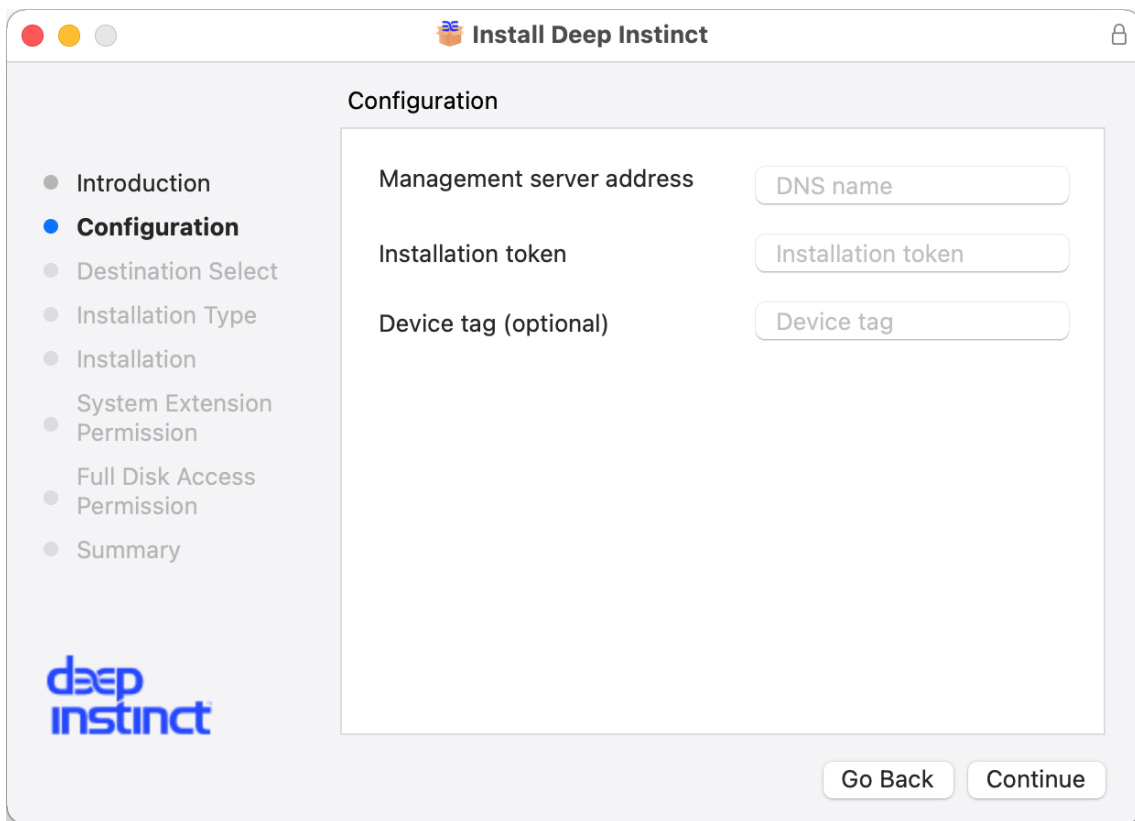


3. Double-click the Deep Instinct icon and click **Allow** in the confirmation dialog to open the wizard.

The **Deep Instinct Installer** appears.



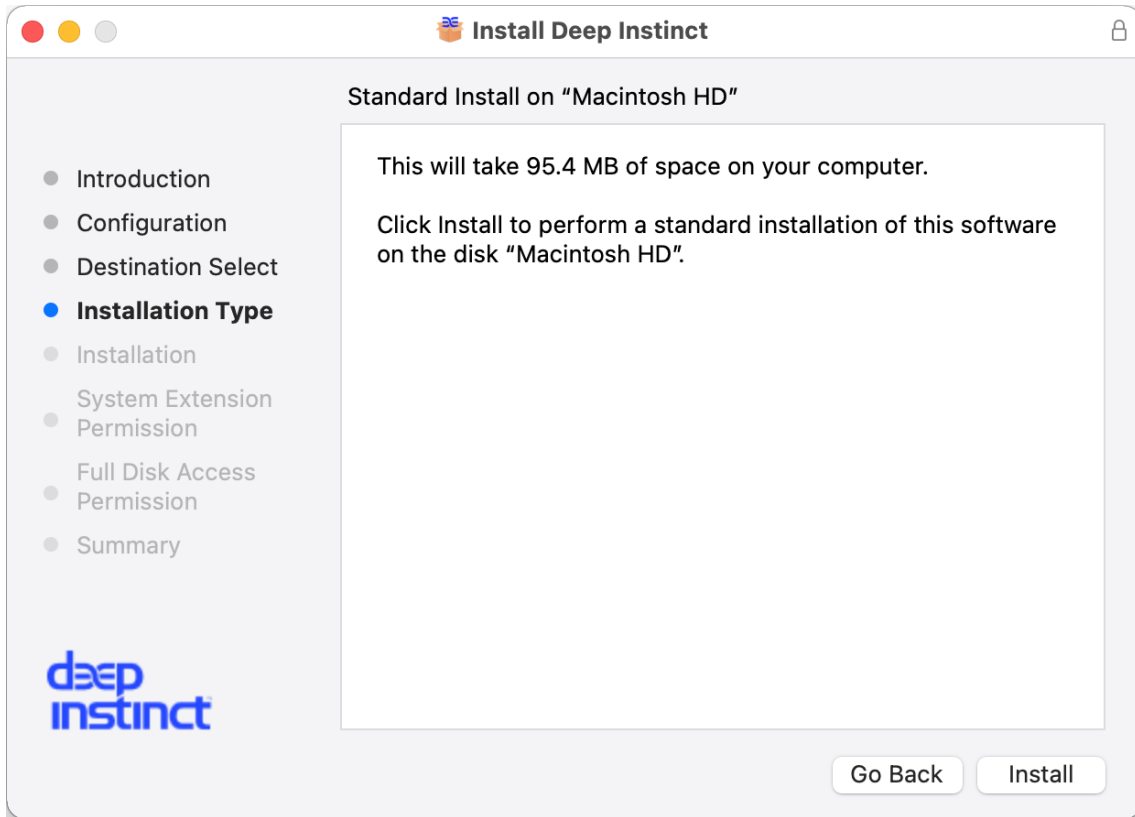
4. Click **Continue** to start the installation. The **Configuration** dialog box opens.



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.



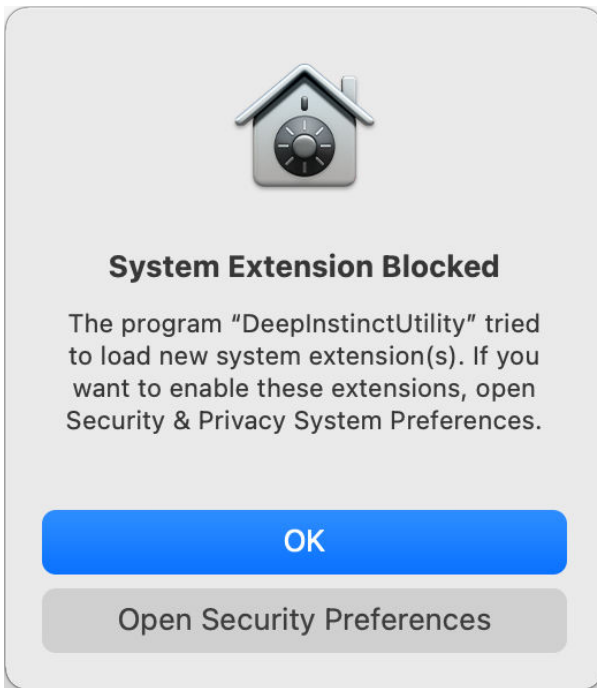
9. Click **Install**. A confirmation dialog appears.

10. Enter your administrator credentials and click **Install Software**.

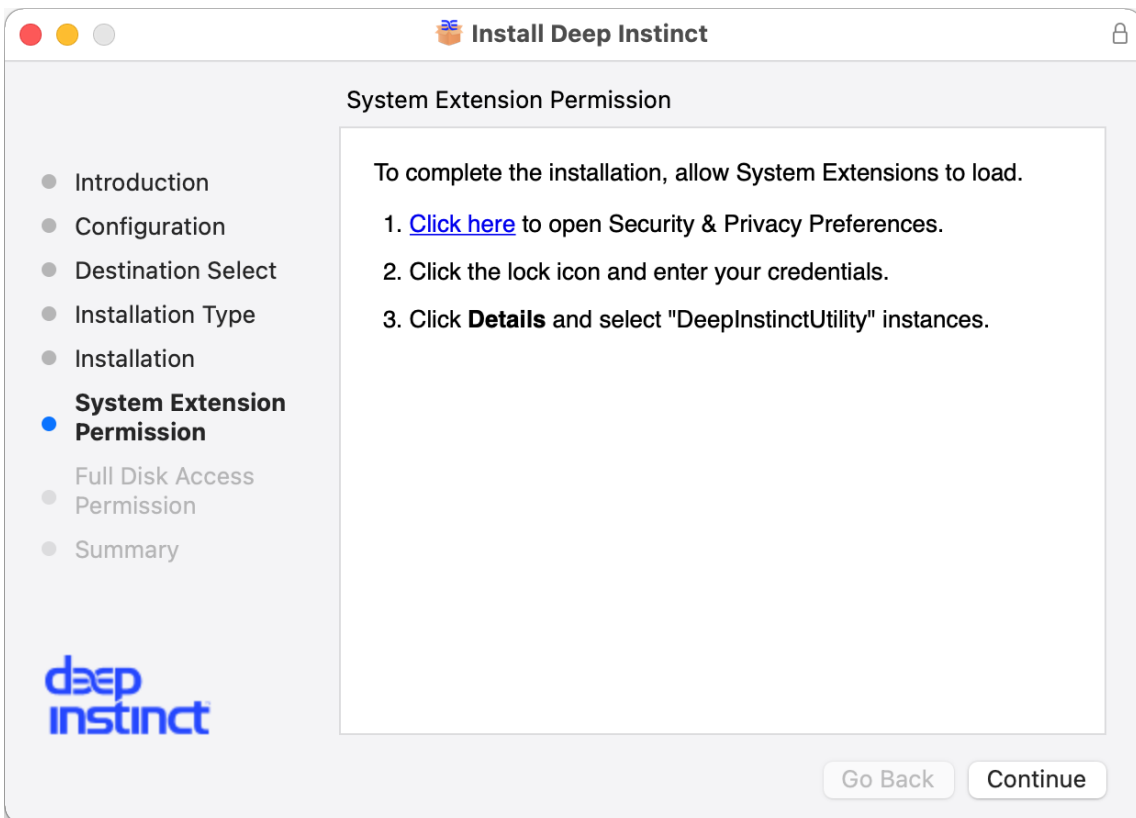
 **NOTE**

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.

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

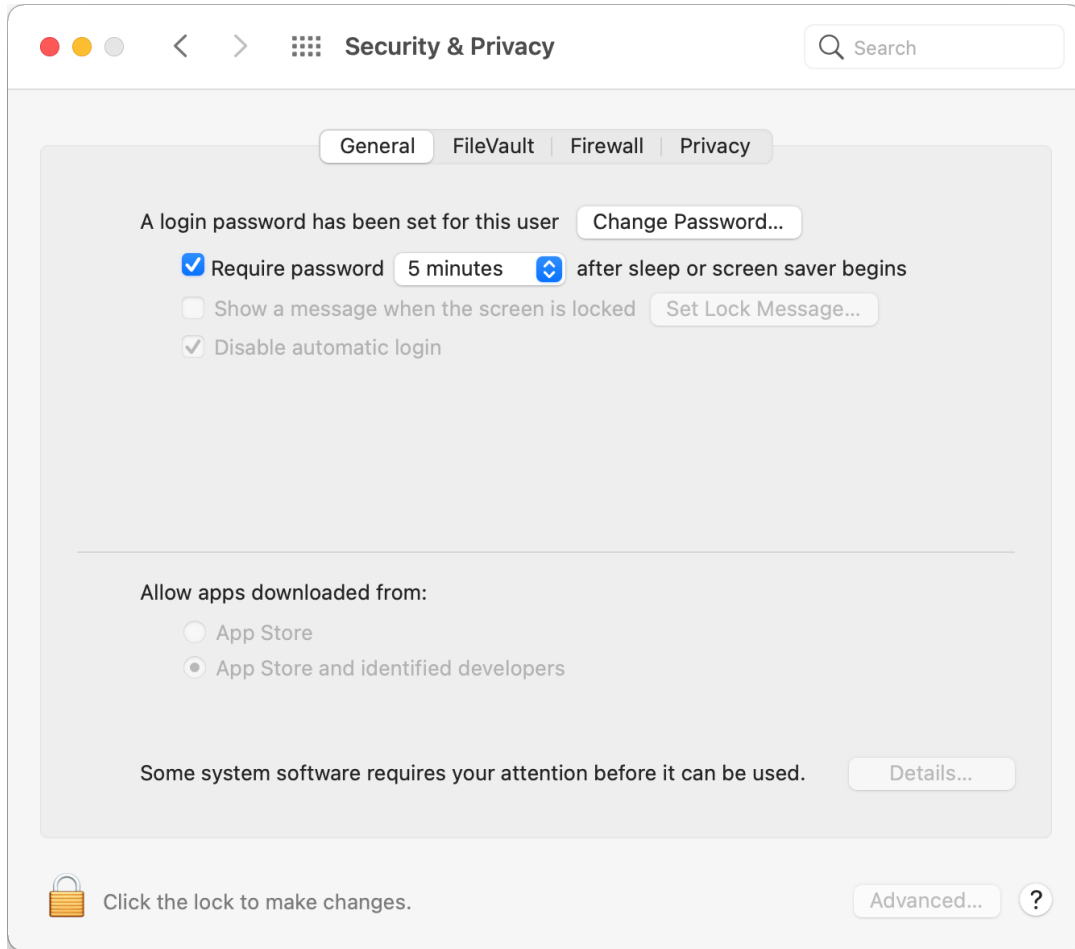



12. Click **OK**. The System Extension Permission screen appears.

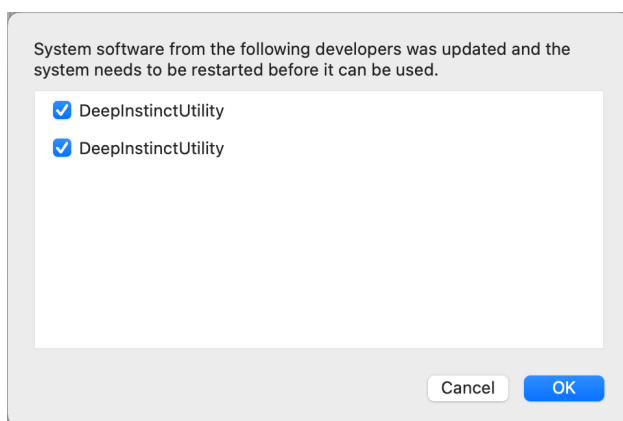


Perform the following:

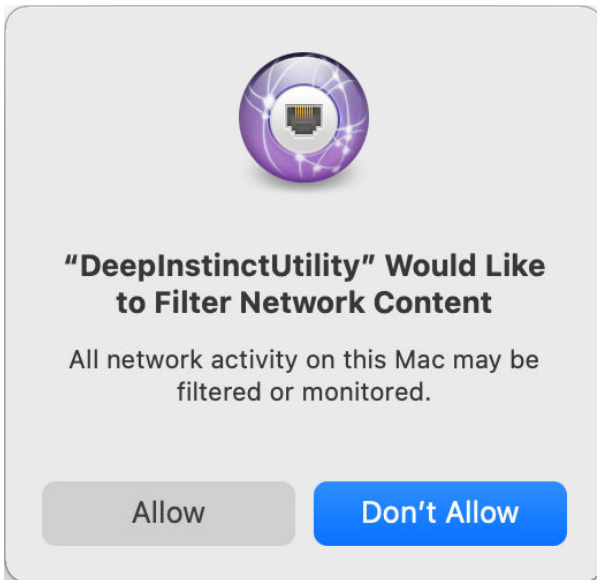
- a. Click [Click here](#) and the **Security & Privacy** screen opens.



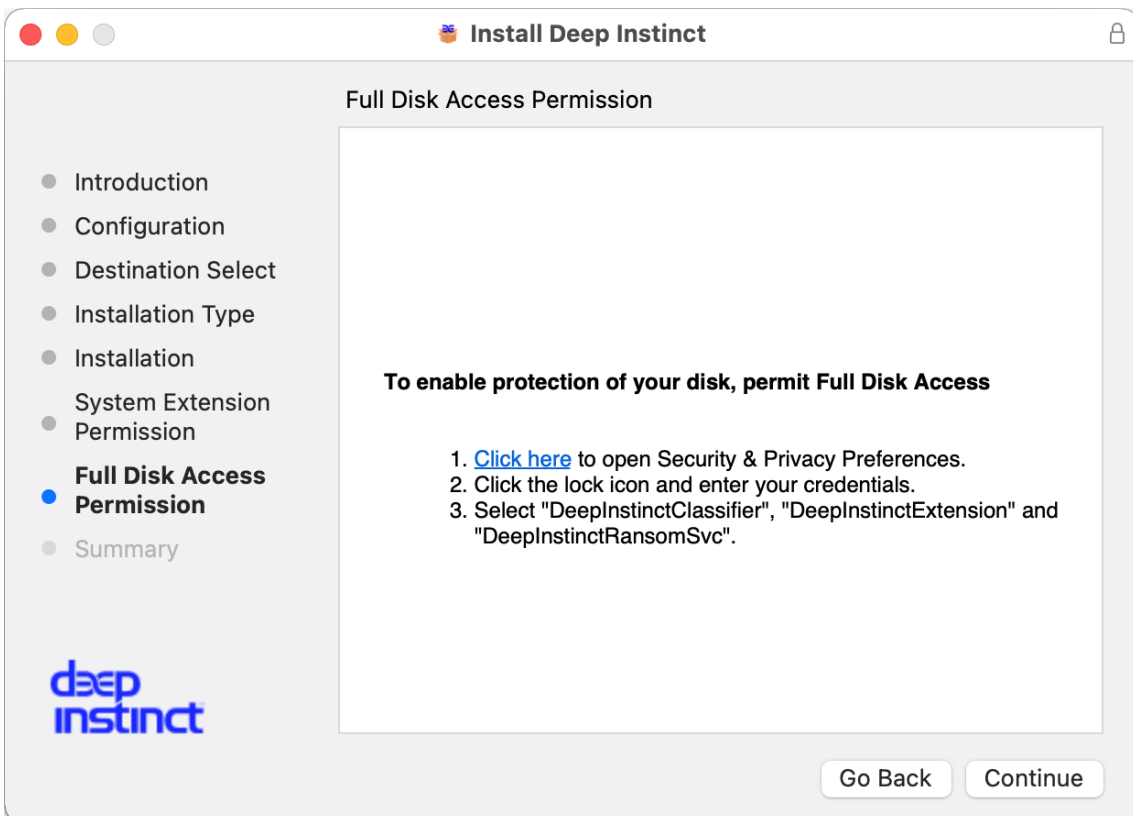
- b. Click  at the bottom left corner of the screen. A confirmation dialog requesting your credentials appears.
- c. Enter the administrator's username and password.
- d. Click **Unlock** and then Details to continue.



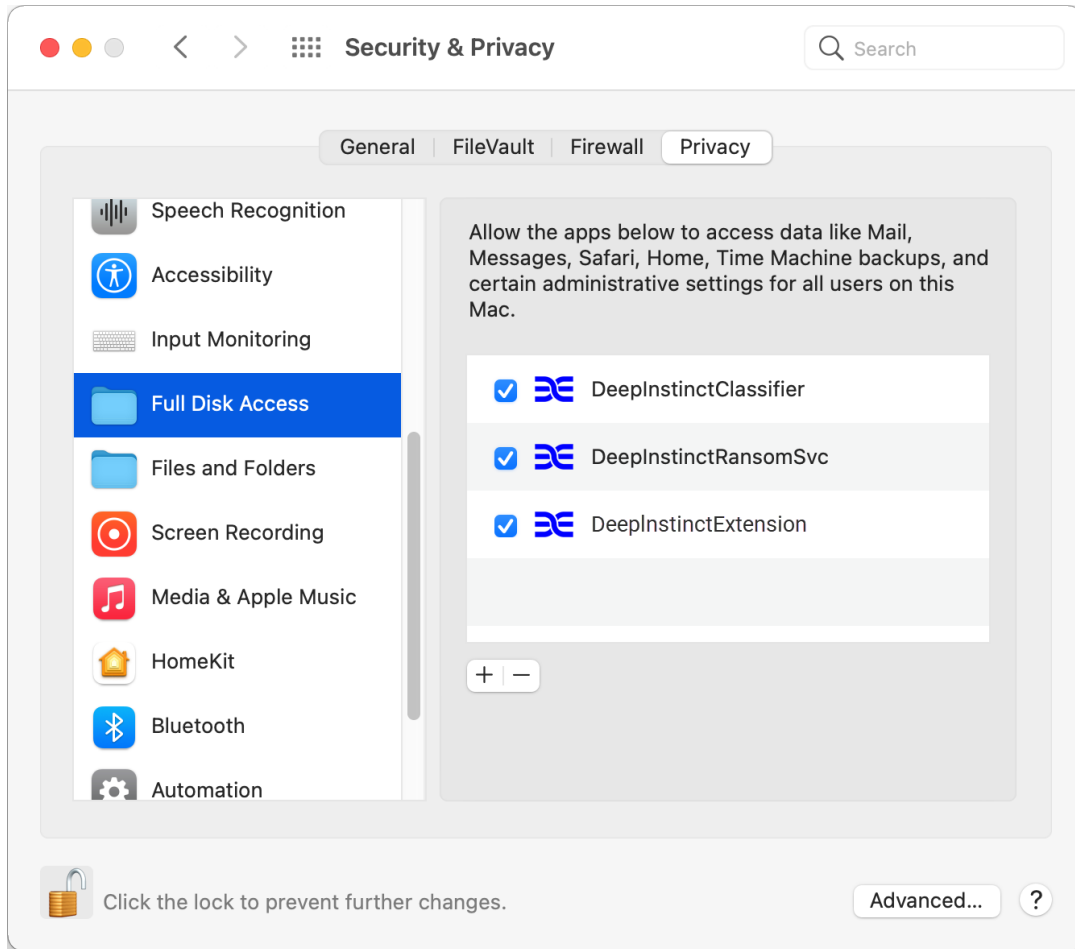
- e. Select all instances of **DeepInstinctUtility** and click **OK** to permit Deep Instinct to load the required system extensions.
13. Deep Instinct may need to perform network filtering. If permission is required, the **Filter Network Content** message opens and click **Allow**.




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



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

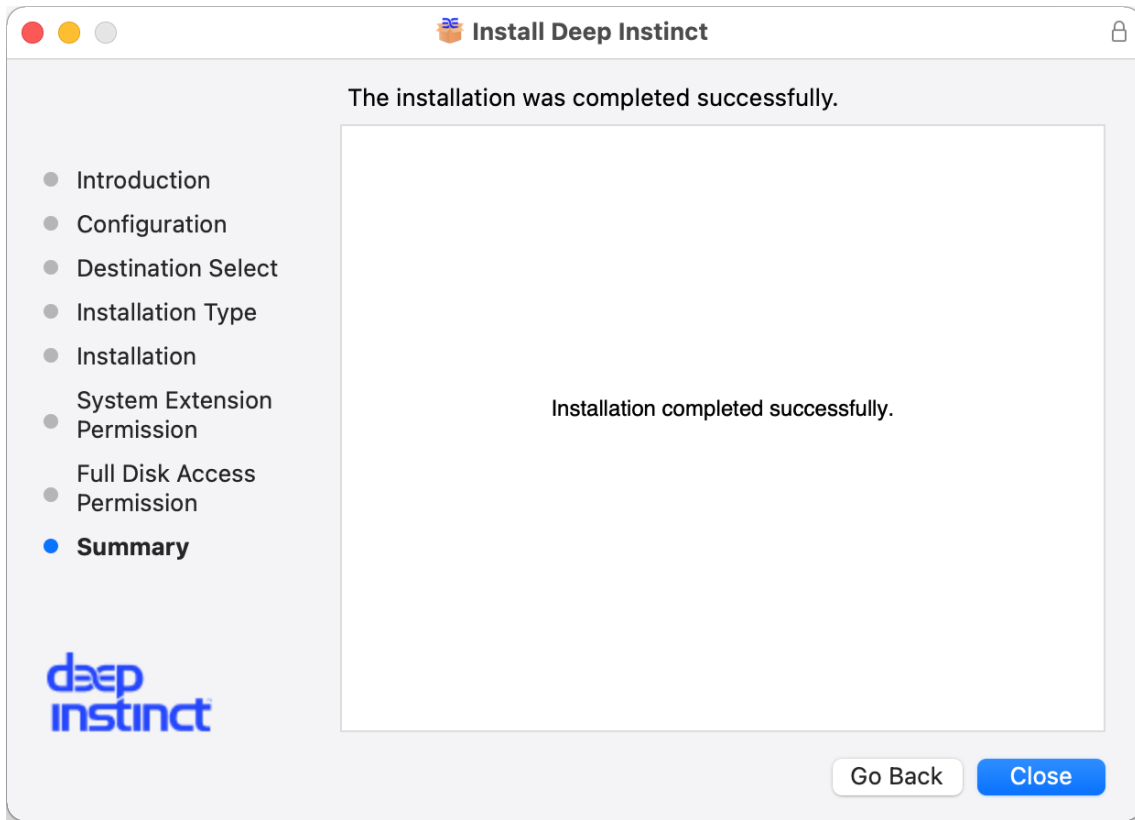


- b. Select **DeepInstinctClassifier**, **DeepInstinctRansomSvc**, and **DeepInstinctExtension**.
- c. Enable Full Disk Access Permission for each user.
- d. Go back to the Installation Wizard.

 **NOTE**

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](#).

15. A message appears after the installation completes successfully.



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

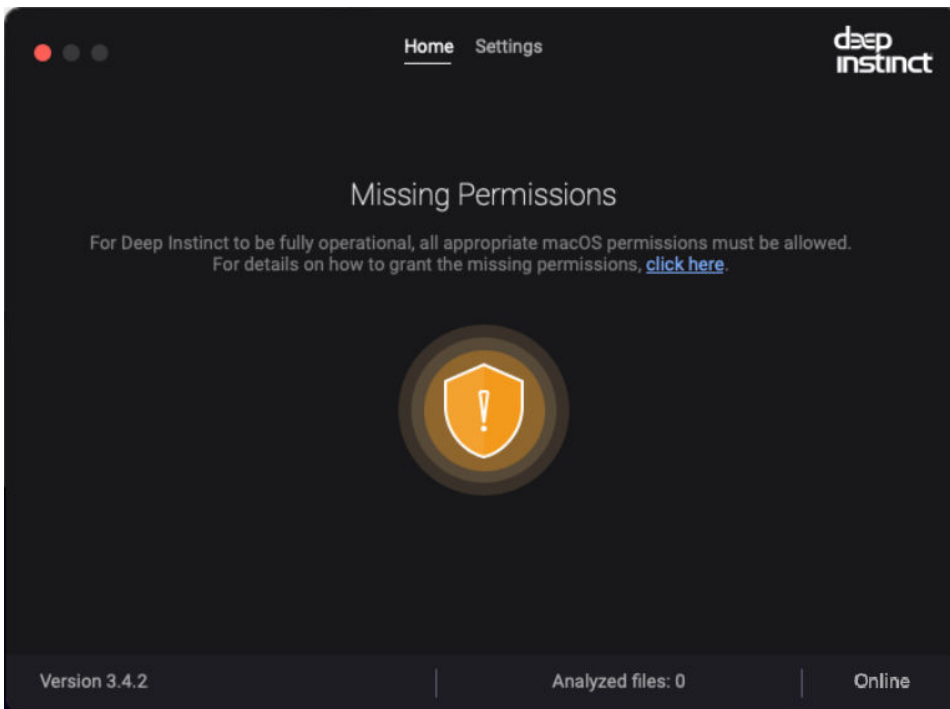
- **Network Content Filtering Permission**

- 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, .



NOTE

If the **Missing Permission** screen is not displayed, click the icon with the 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

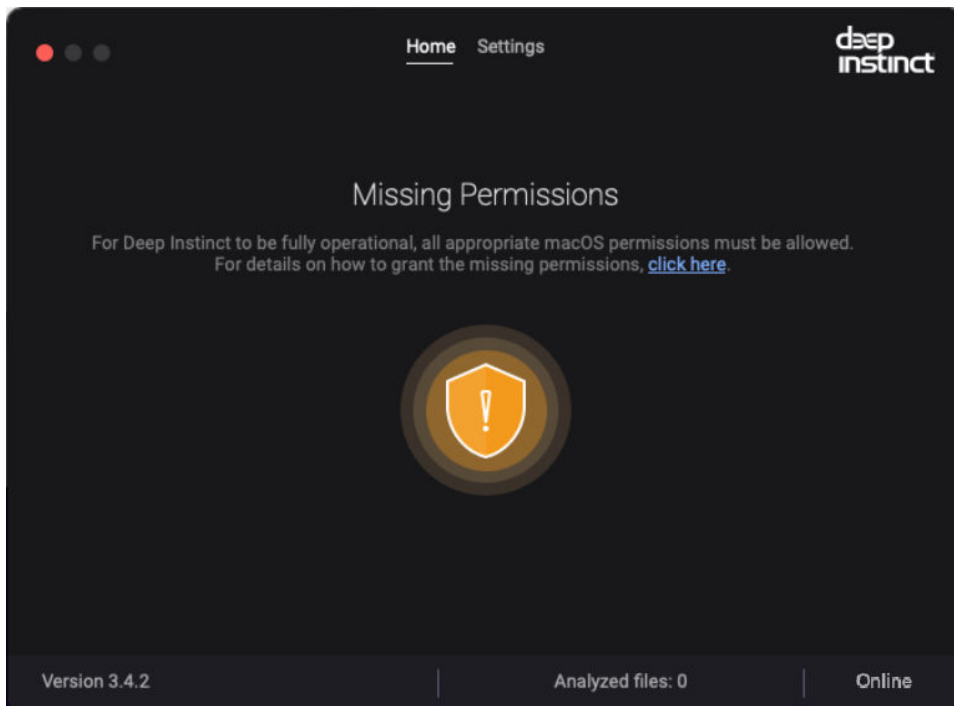
To enable missing permissions



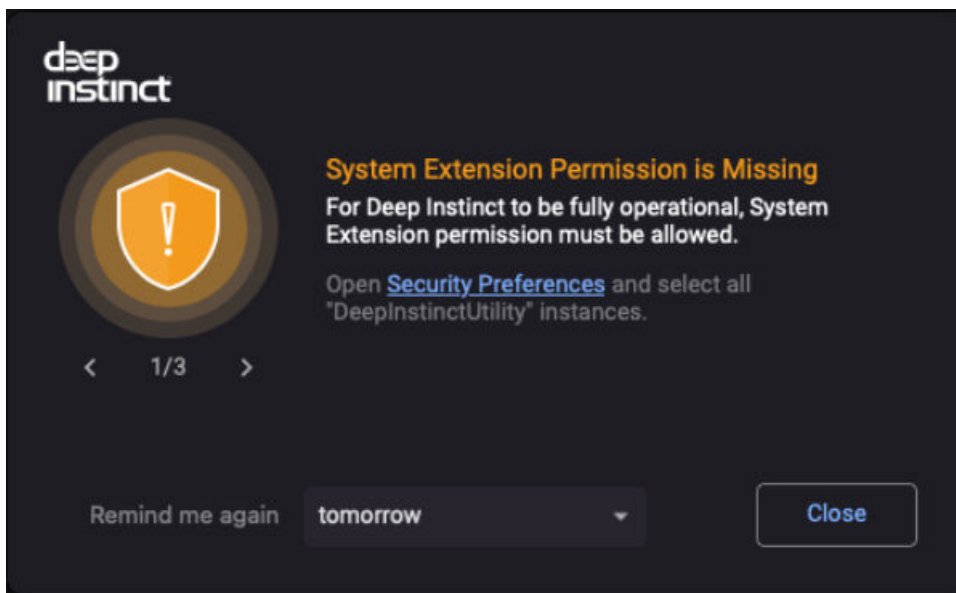
NOTE

If the **Missing Permission** screen is not displayed, click the icon with the yellow indicator .

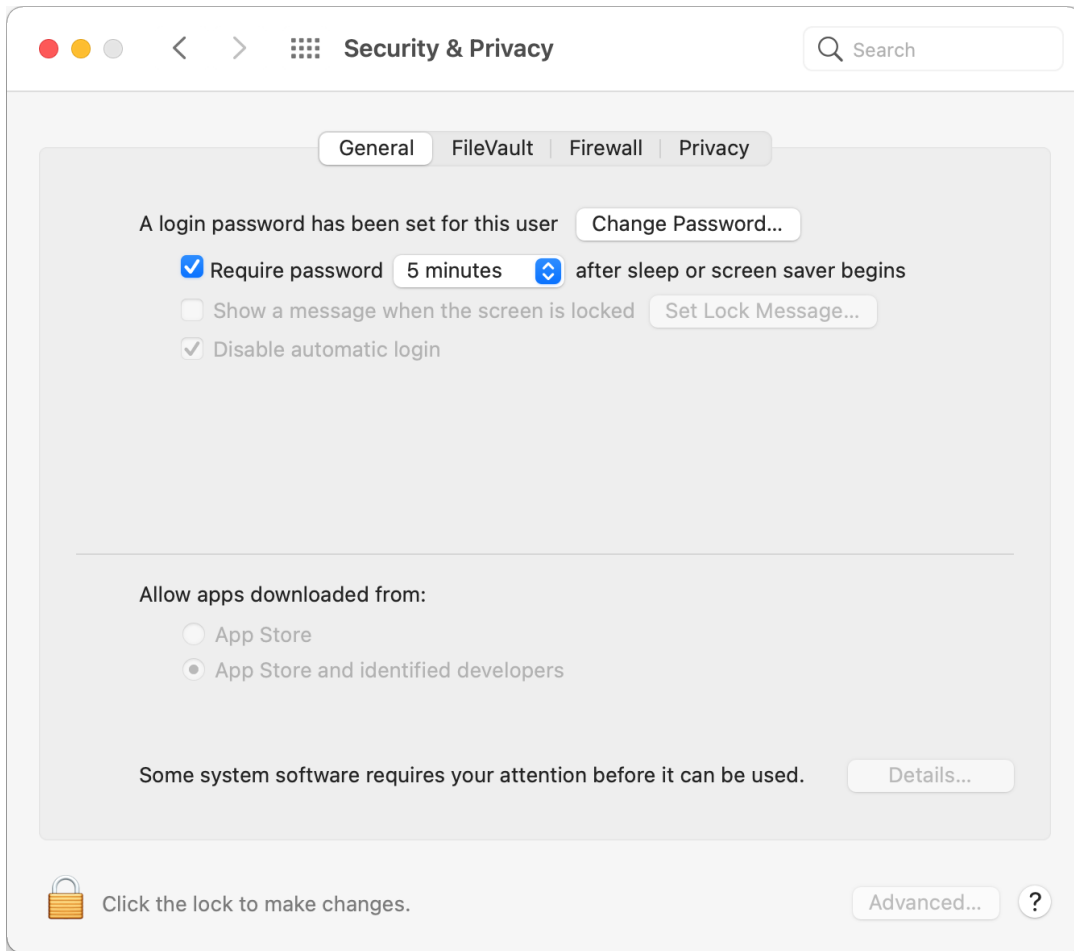
1. In the **Missing Permissions** screen, click on the **click here** link.




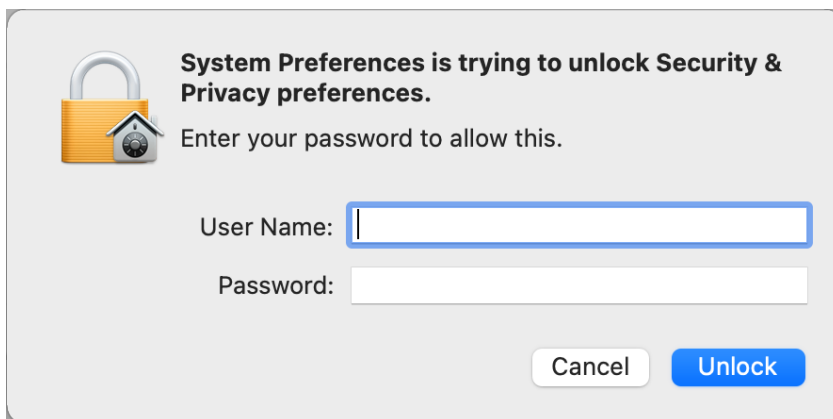
2. If you are missing the **System Extension Permissions**, a message requesting to enable them is displayed (there may be additional messages for other missing permissions as well).



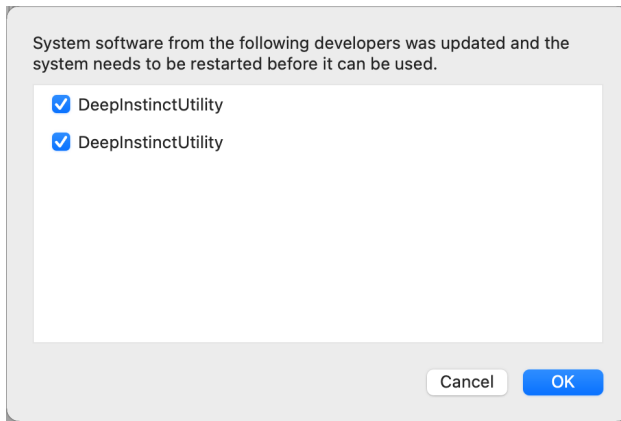
3. Click the **Security Preferences** link. The **Security & Privacy** screen appears.



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



5. Click **Unlock** → Details to continue.




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

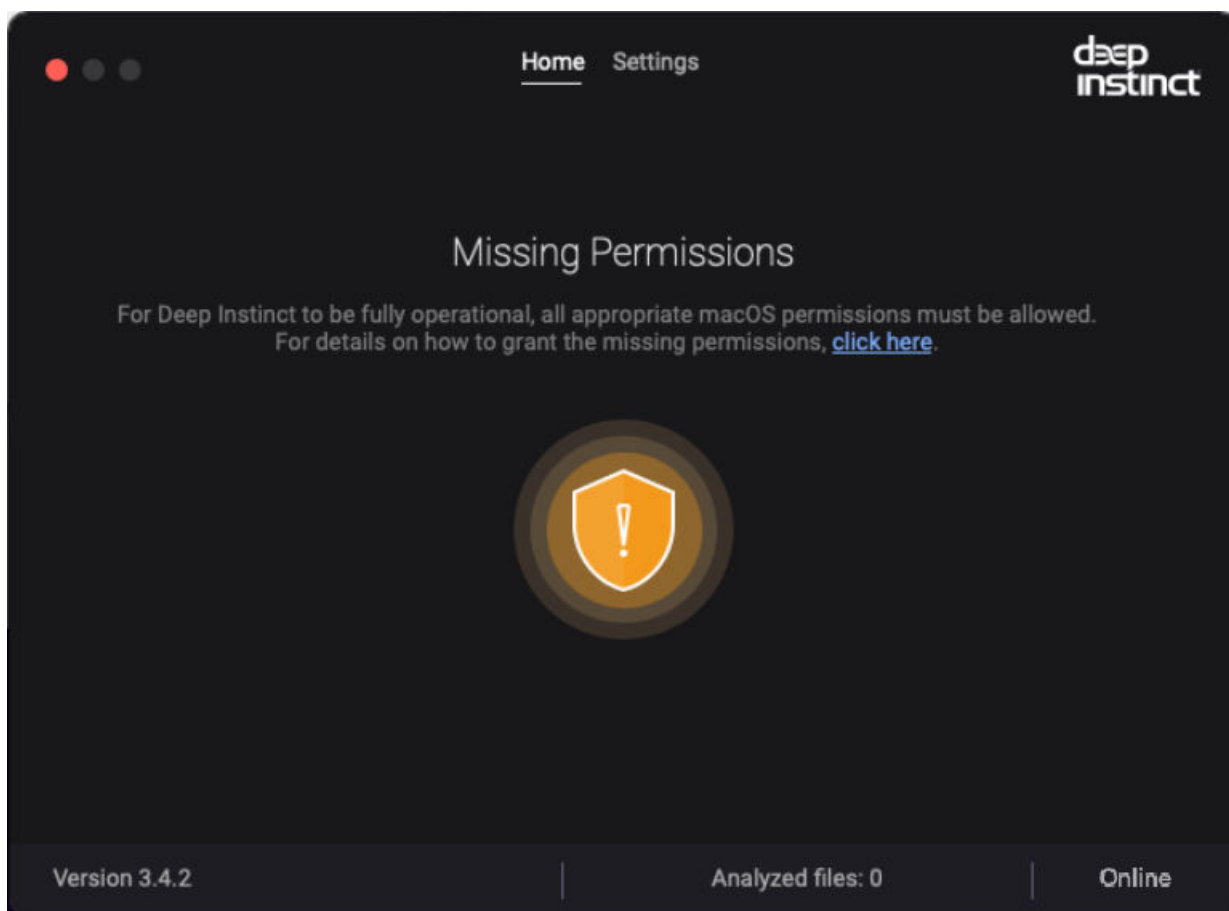
To enable missing permission



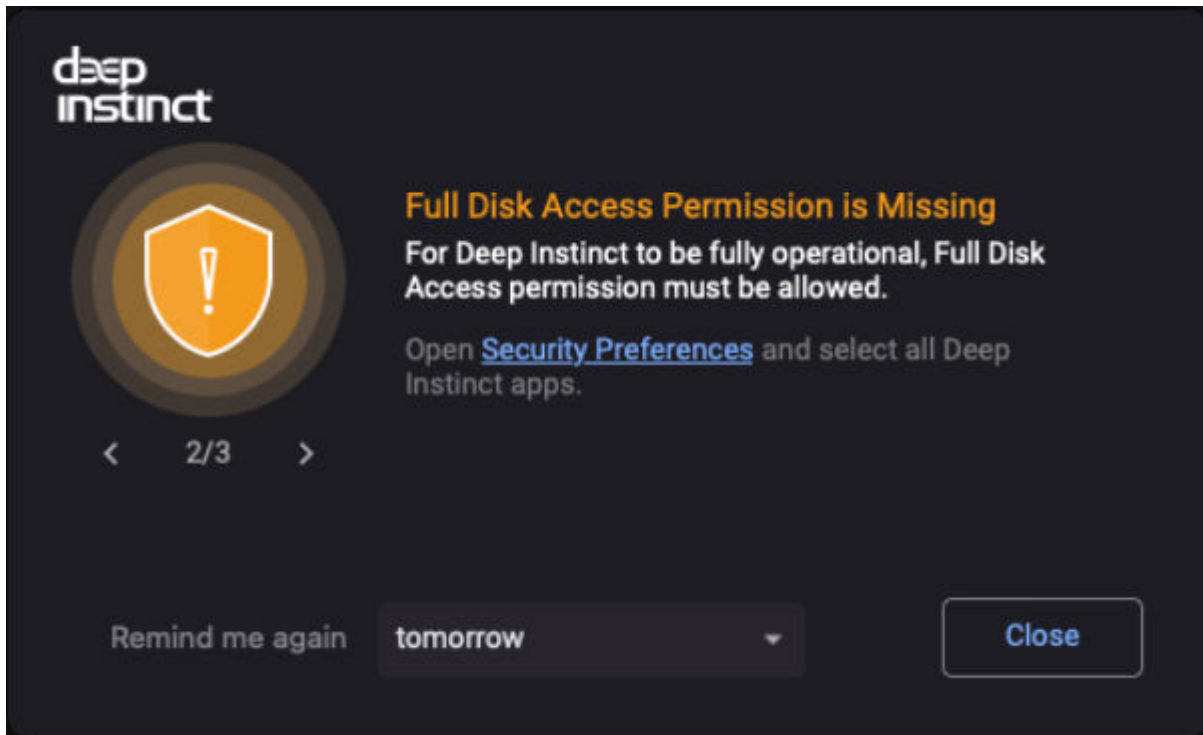
NOTE

If the **Missing Permission** screen is not displayed, click the icon with the yellow indicator .

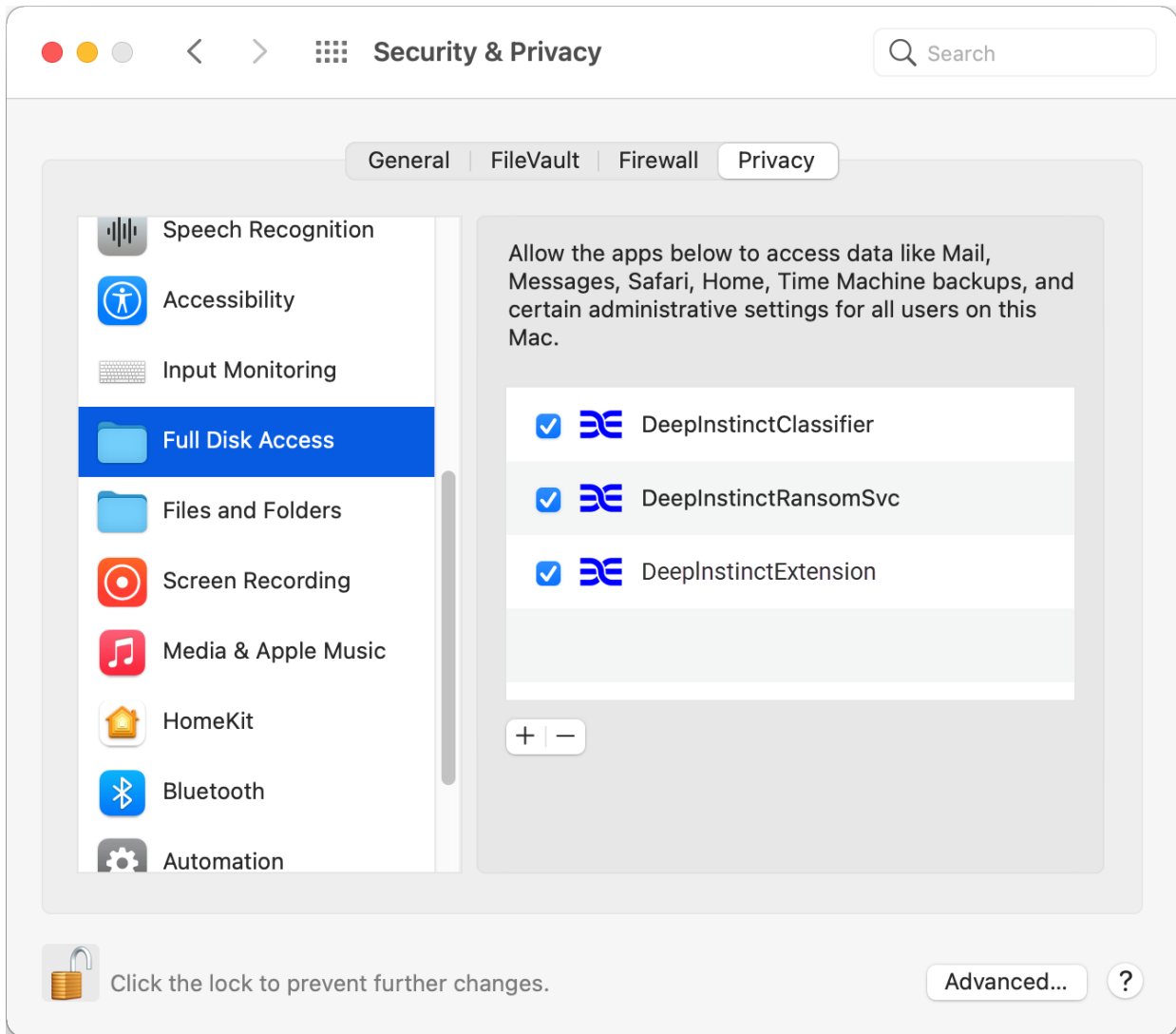
1. In the **Missing Permissions** screen, click on the **click here** link.



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

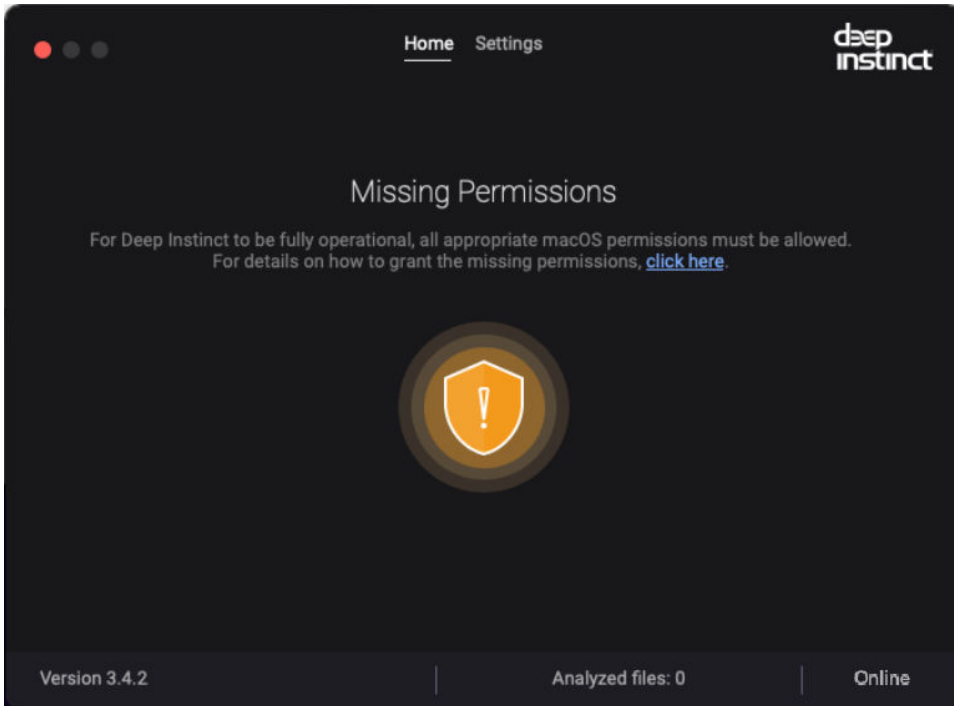
To enable missing permission



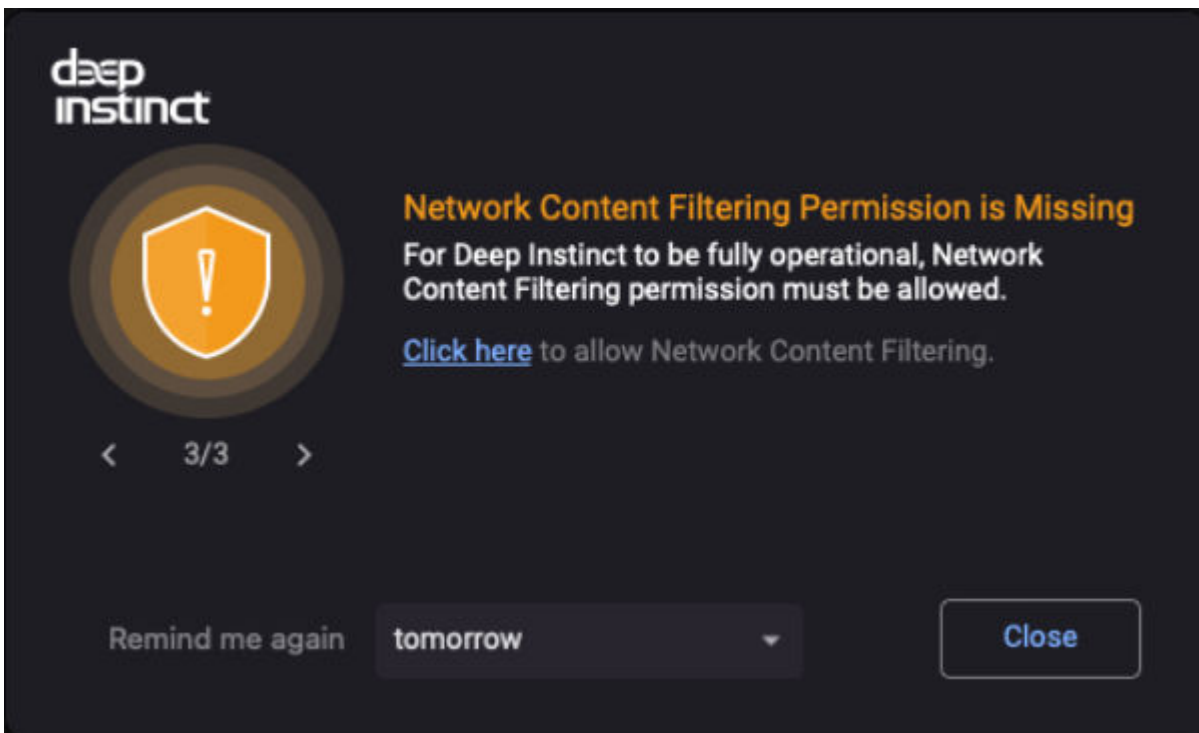
NOTE

If the **Missing Permission** screen is not displayed, click the icon with the yellow indicator .

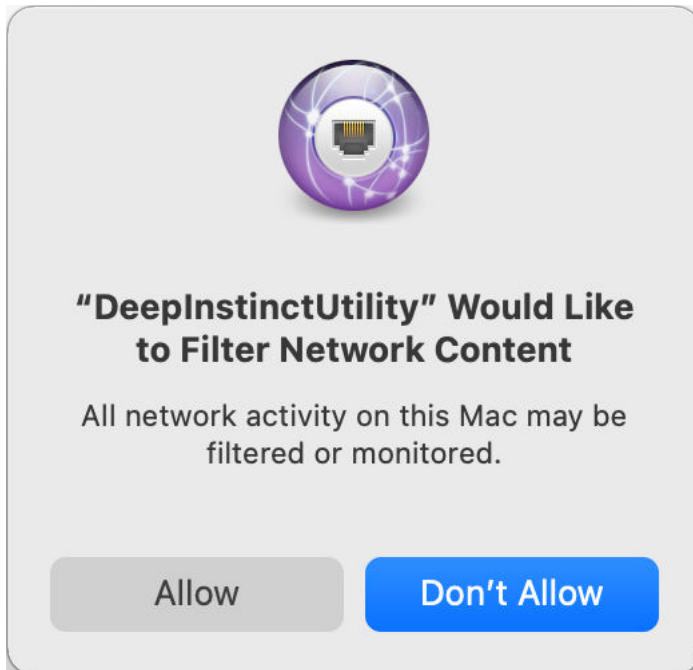
1. In the **Missing Permissions** screen, click on the **click here** link.




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.



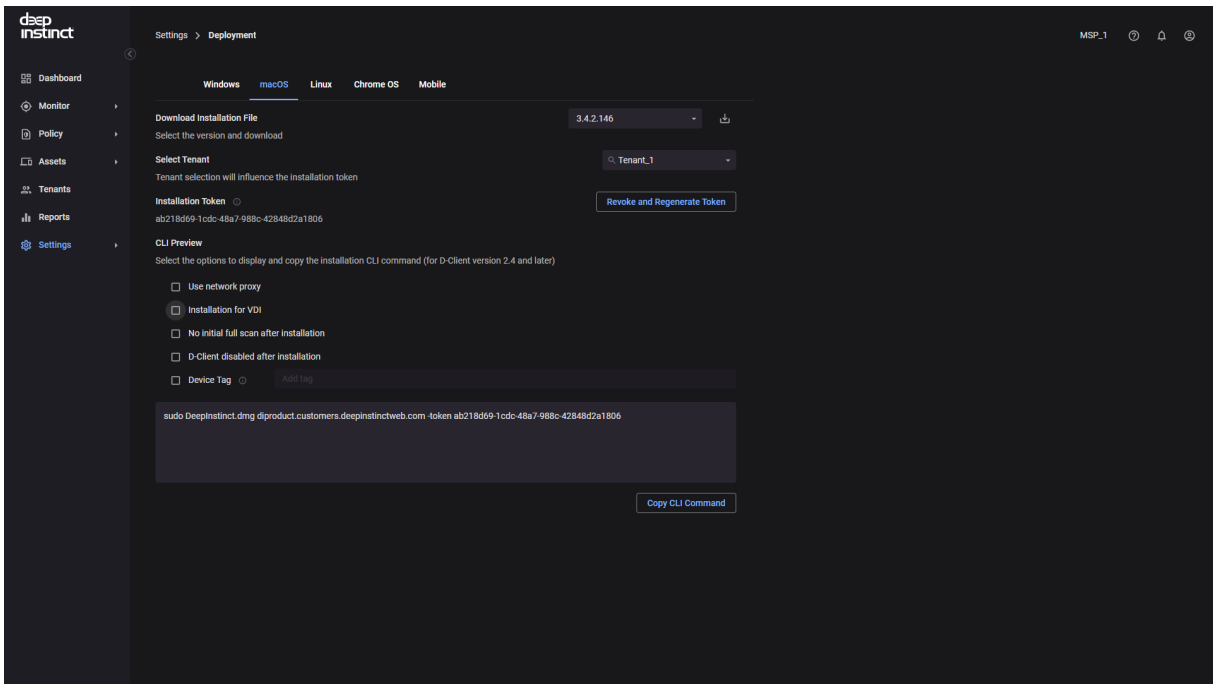
4. Click **Allow**. After a few minutes the permissions are enabled and the D-Client icon changes to a normal state .


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](#) → [Deployment](#) → [MacOS](#).



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

 **WARNING**

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](#)

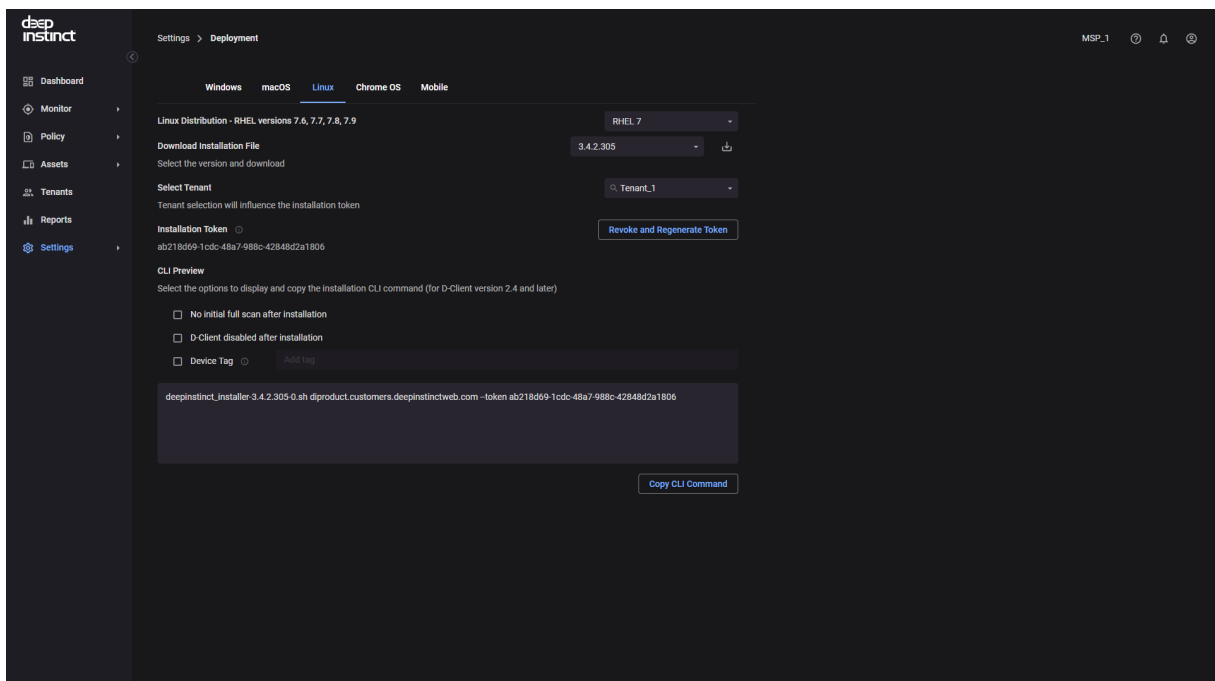
[Local deployment using the Installation CLI command](#)

4.4.1. Linux deployment resources


The Linux D-Client installation package is available for download in the Management Console's [Settings](#) → [Deployment](#) → [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](#) → [Deployment](#) → [Linux](#).



3. Select the Linux distribution applicable to your device from the Linux Distribution drop-down box.


 **NOTICE**

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 drop-down 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](#) → [Deployment](#) → [Linux](#) screen. Refer to [Linux Deployment Resources](#) for details.

 **NOTICE**

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.
3. 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>	Installation file path
<installation file>	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>] [--only_validate_deps]
```

Where:

Command Element	Description	Comments
<path>	Installation file path	N/C
<installation file>	Installation file name	N/C
<server address>	FQDN for the Management Server (D-Appliance)	N/C
<installation token>	ID of the installation token as displayed in the Linux Deployment Resources screen.	N/C
<tag>	Adds a tag associated with the deployed devices. Use quotation marks to enter values with spaces or special characters.	<ul style="list-style-type: none"> ■ Optional ■ The Device Tag must comply to the following: <ul style="list-style-type: none"> ■ Maximum length is 256 characters ■ Device Tags are case sensitive ■ Valid characters: <ul style="list-style-type: none"> ■ Letters (a-z, A-Z) ■ Numbers (0-9) ■ Spaces representable in UTF-8 ■ Special characters: + - = . _ : / @ <p>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.</p>

Command Element	Description	Comments
<code>--nfs</code>	Starts the D-Client without performing the initial full scan.	Optional
<code>--mp</code>	Enables the use of a network proxy server, using the specified settings of the proxy server URL and port number.	Optional
<code><proxy url></code>	URL for the proxy server, including the scheme	N/C
<code><proxy port></code>	Port number to access the proxy server.	N/C
<code>--only_validate_deps</code>	Disables the automatic installation of the required packages. It validates whether the required packages have been installed. If a required package is missing, the installation of D-Client 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/deepinstinct_installer.sh
```

```
[sudo] password for user:
```

```
[user@localhost ~]# sudo /home/user/Downloads/deepinstinct_installer.sh customer.deepinstinctweb.com --token 12345678
```

```
Extracting installation files...
```

```
Redirecting to /bin/systemctl start DeepNetworkService.service Redirecting 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"

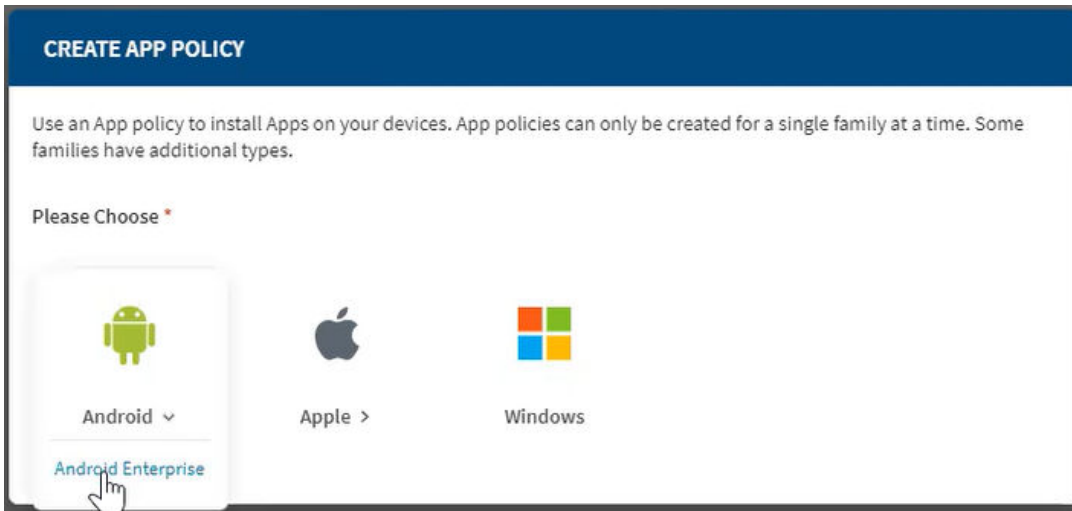
- Filename must be **devInfo.json**
- The file must be placed at the following location on the mobile device: **/sdcard/UPRR/**

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.




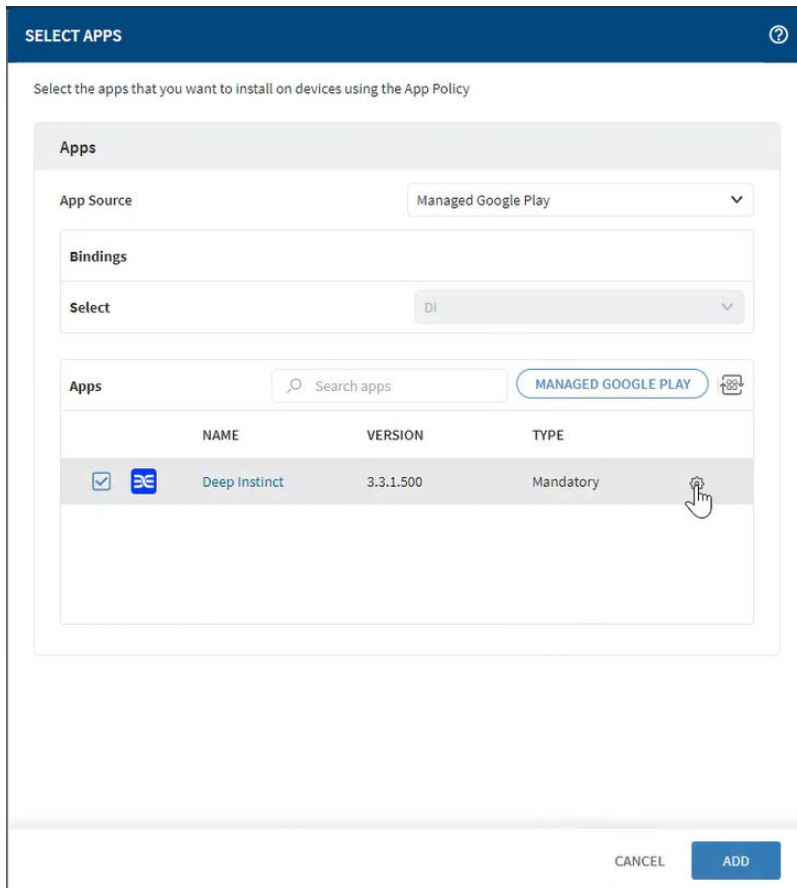
6. Click Android+Android Enterprise to create an App Policy for your Android device. The **CREATE APP POLICY** screen appears (**GENERAL** tab).

The screenshot shows the 'CREATE APP POLICY' interface with the 'GENERAL' tab selected. The form contains the following fields and values:


App Policy Name *	Policy Name
Description	Policy Description
Policy Status	n/a
Family	Android Plus
Type	Android Enterprise
Apps	0

At the bottom right of the form, there are three buttons: 'CANCEL', 'SAVE AND ASSIGN', and 'SAVE'. A question mark icon is visible in the top right corner of the header area.


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

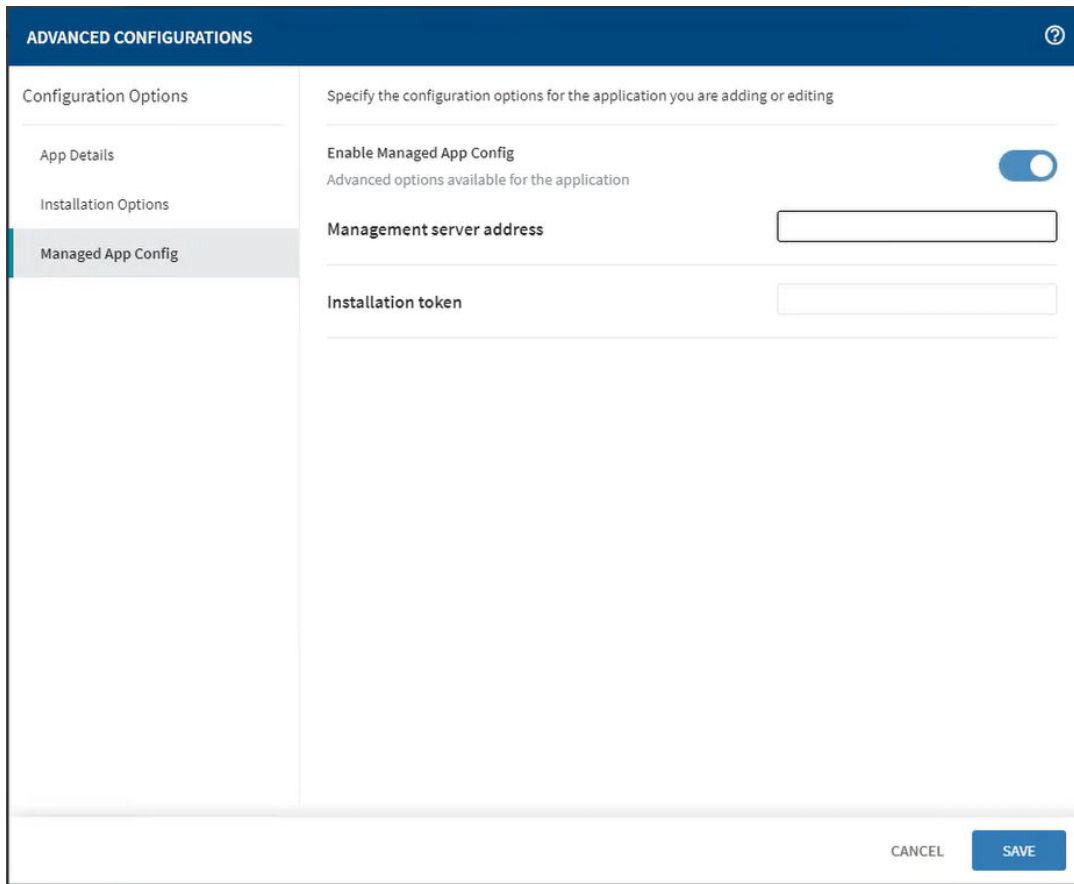


9. Select **MANAGED GOOGLE PLAY** from the App Source dropdown box.
10. Select your Managed Google Play Account from the Select dropdown box.

 **TIP**

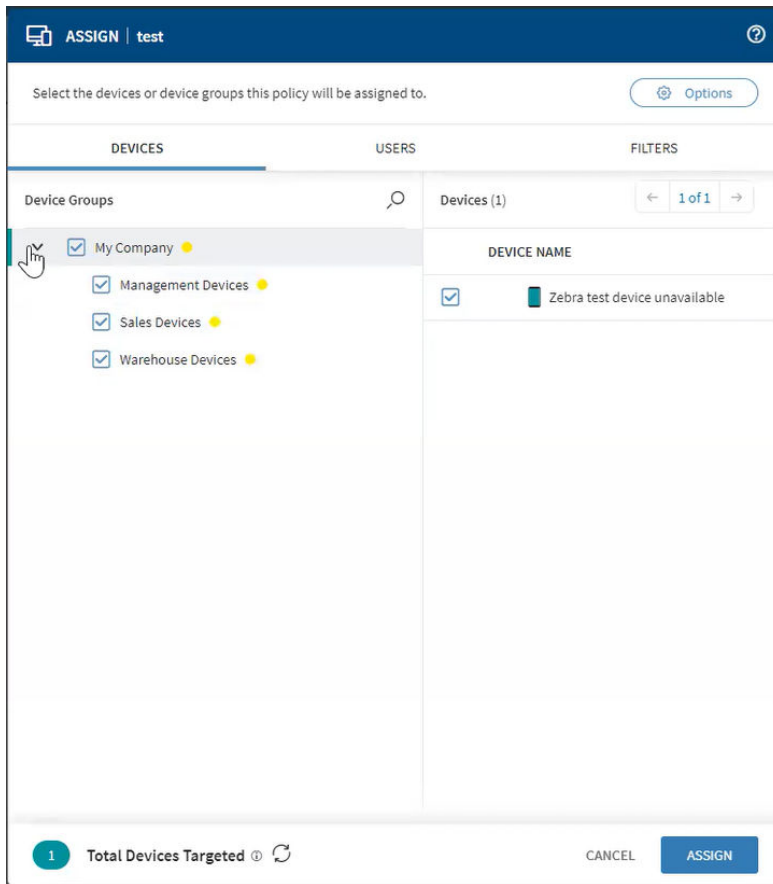
If Deep Instinct is not displayed in the Managed Apps list, click **MANAGED GOOGLE PLAY** and select the **Deep Instinct** app. Deep Instinct should now be displayed in the list.

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



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.



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:

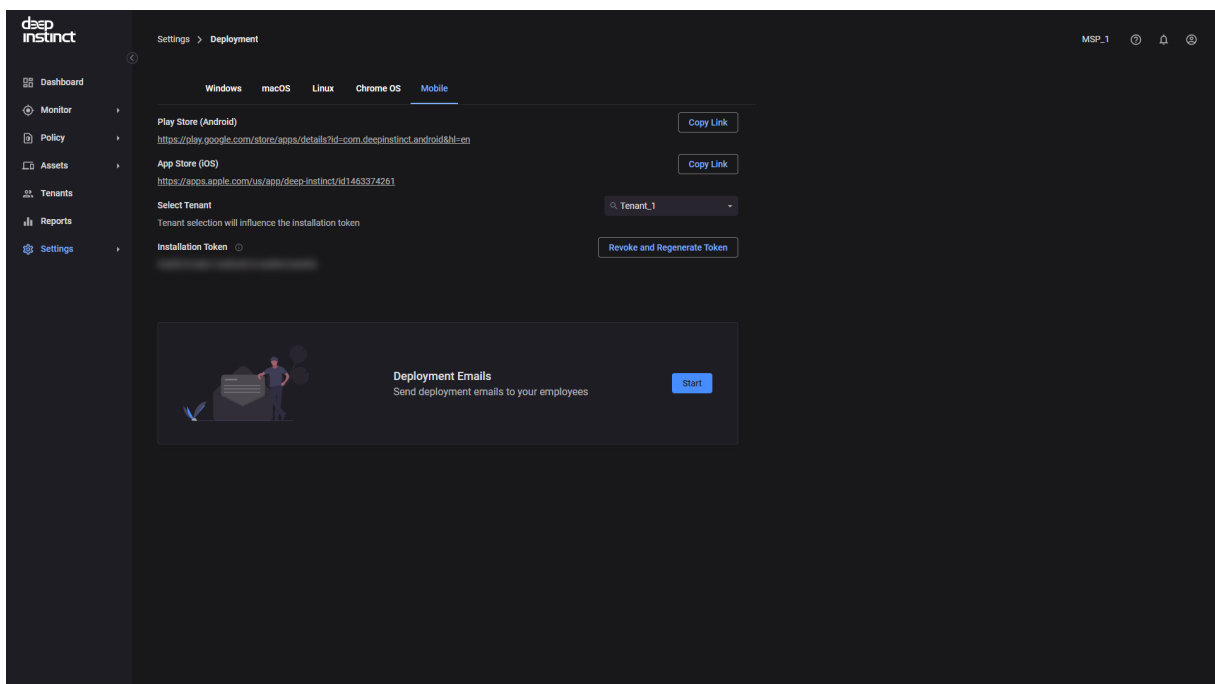
Make sure you have configured your **SMTP server account** required for the deployment on mobile devices and event notifications, The deployment of the D-Client uses a link sent by email from the Management Server. The SMTP Server may have been configured while running the Startup wizard. If not, configure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

4.5.2.1. Deployment Wizard

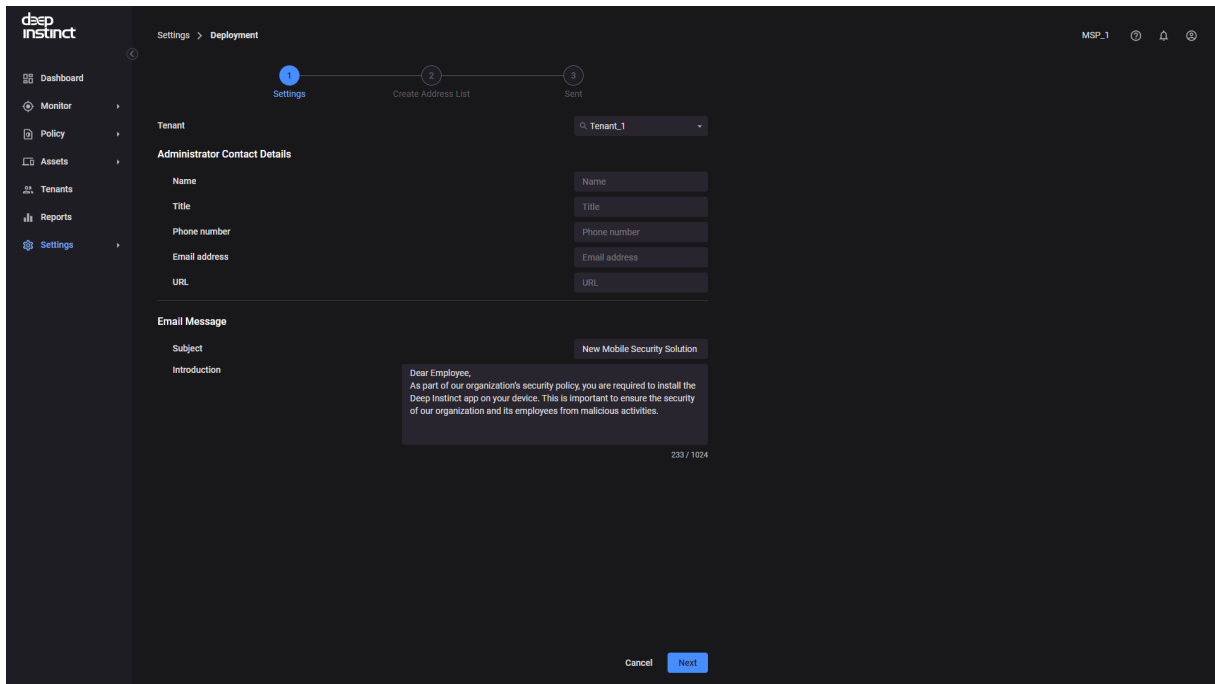
The Deployment Wizard generates a deployment email to the mobile devices which is then used to install the D-Client.

To run the Deployment wizard:

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



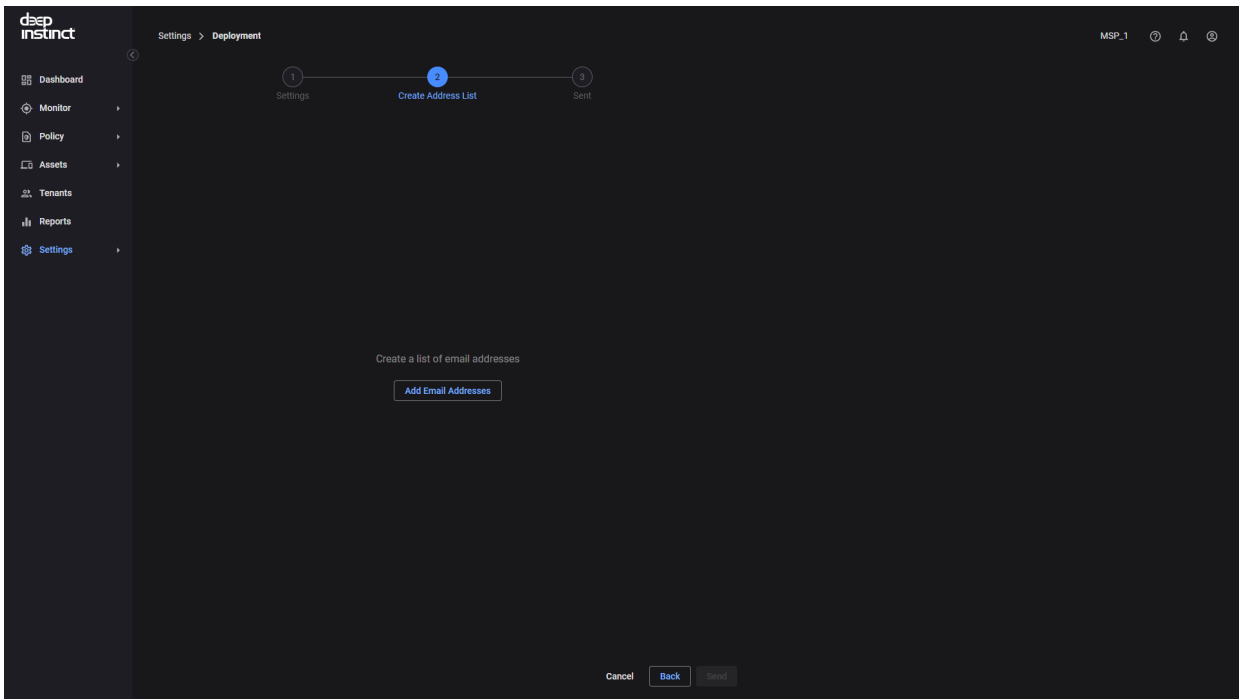
3. For deployments with MSP support — click the Select Tenant dropdown box and select the tenant associated with the deployment.
4. Click **Start** to start the Deployment wizard. The Settings page of the Deployment Emails screen appears.



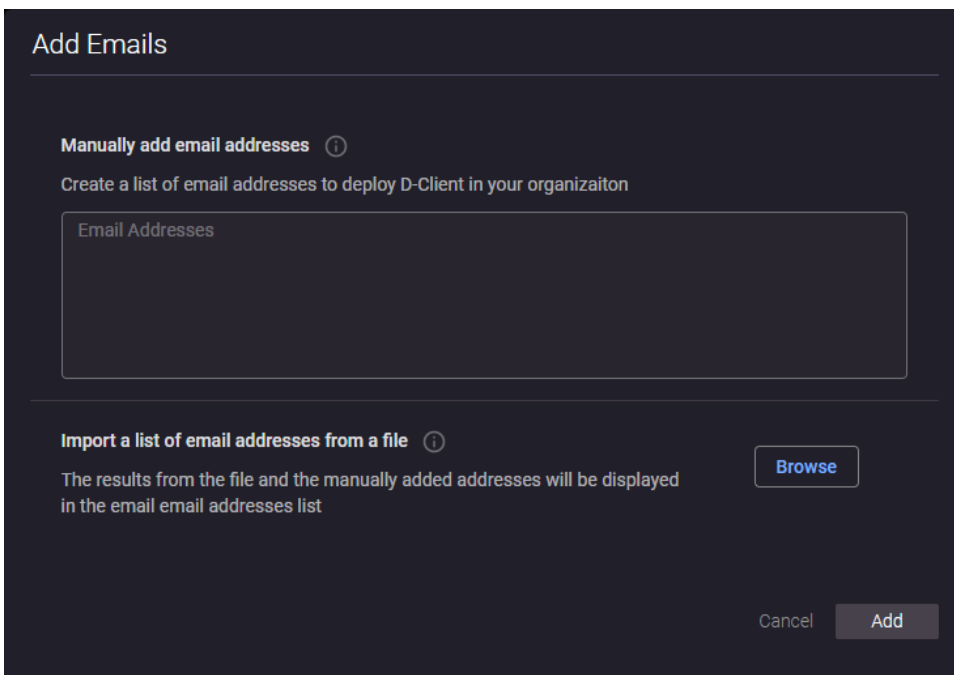
5. For deployments with MSP support — click the Select Tenant dropdown box and select the tenant associated with the deployment.
6. Enter the administrator’s contact information for the employees to contact, if they have any questions (e.g., name, title, phone number, email address and URL). Name and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



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



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 Address** — 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.



NOTE

To add more addresses, click **Add Email Addresses** from the table header.

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**.

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](#)

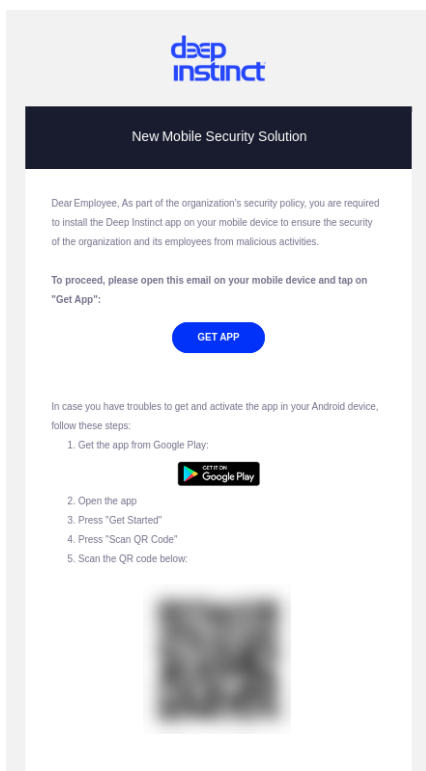
- Alternative Installation for iOS and iPadOS Devices

Email installation for Android devices

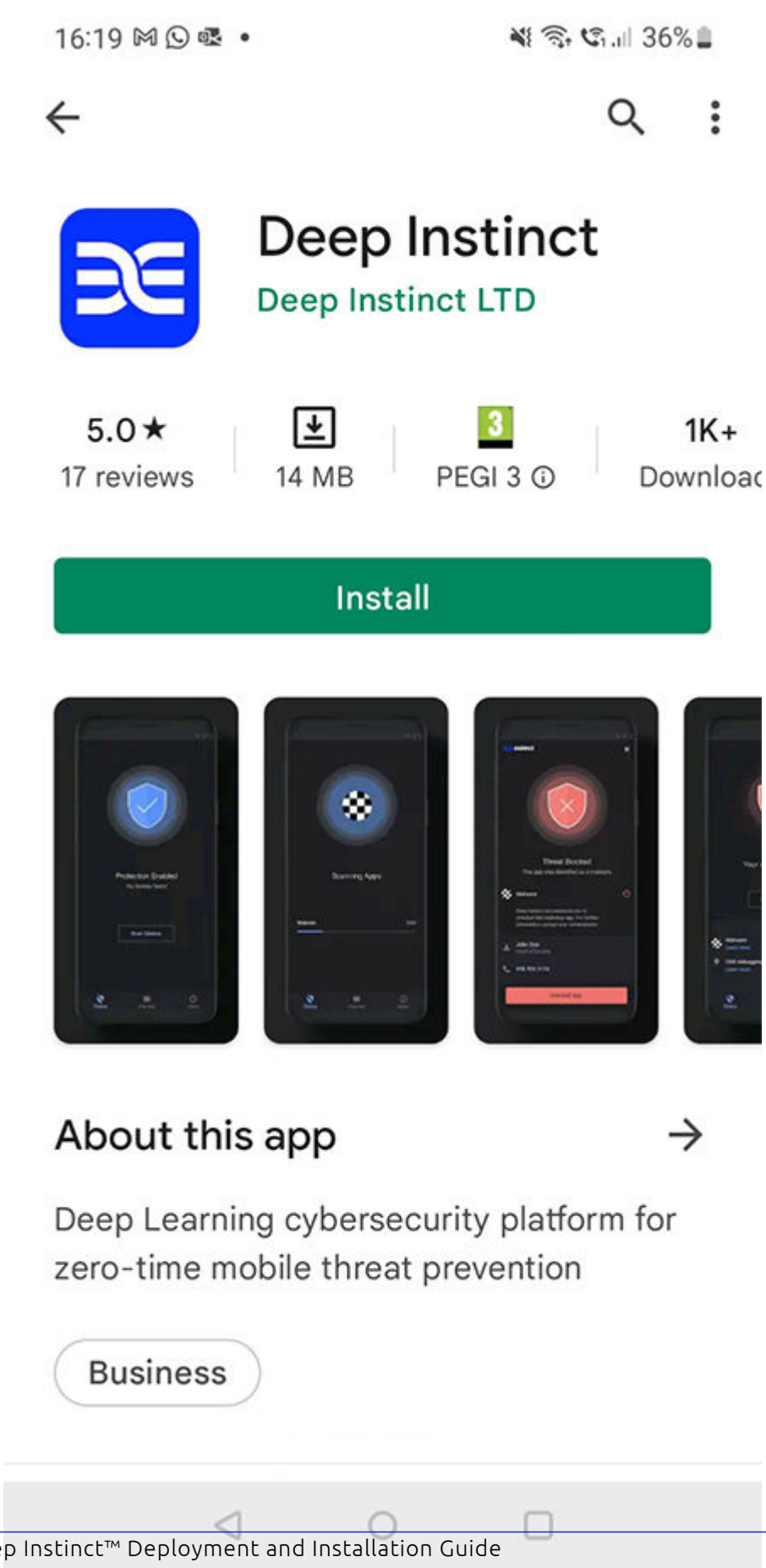
The email installation is the recommended method to install Deep Instinct D-Client on your Android device. However, if your device cannot receive emails or has limitations that prevent the installation by email, use the [alternative installation](#).

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

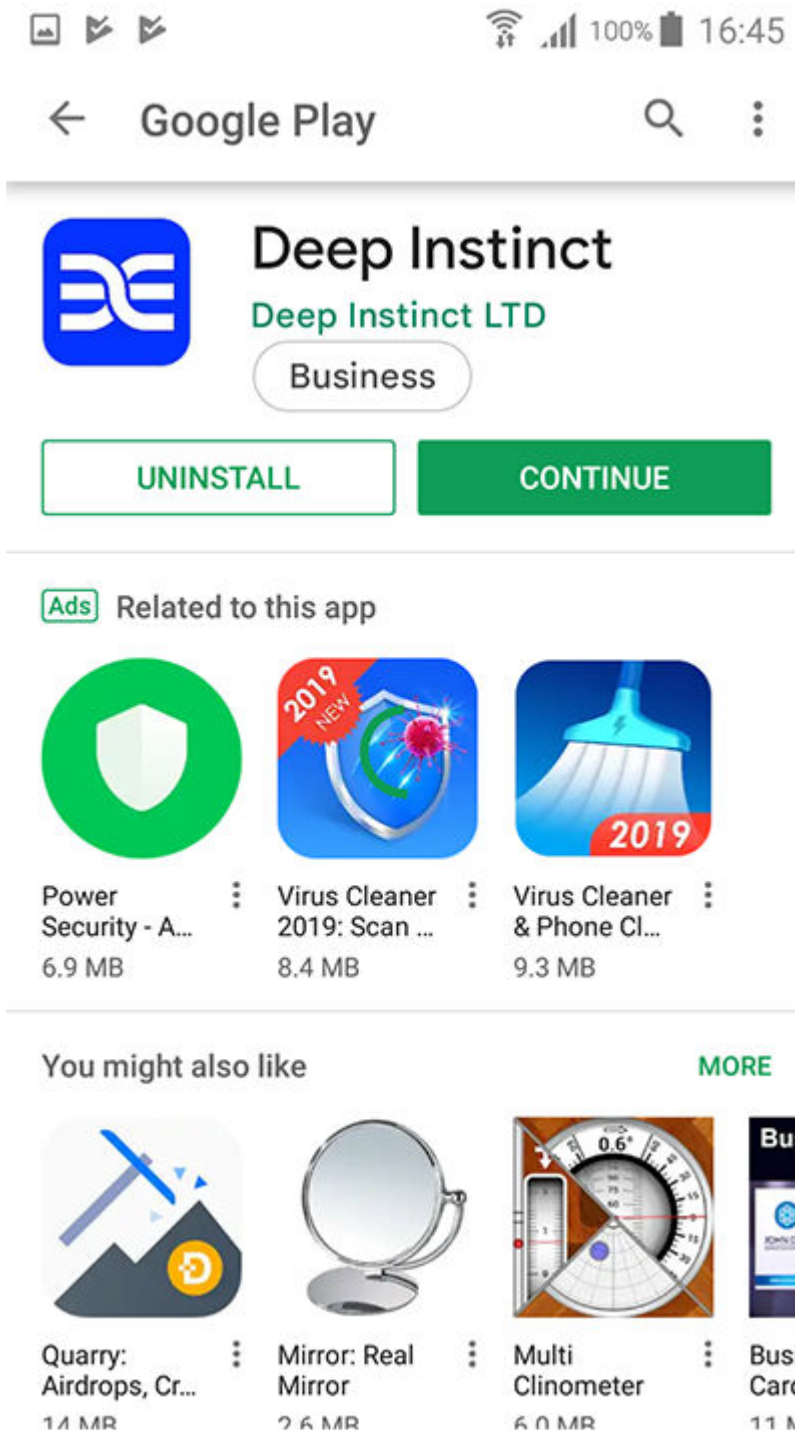
1. Open the installation email on the Android device and read the email.



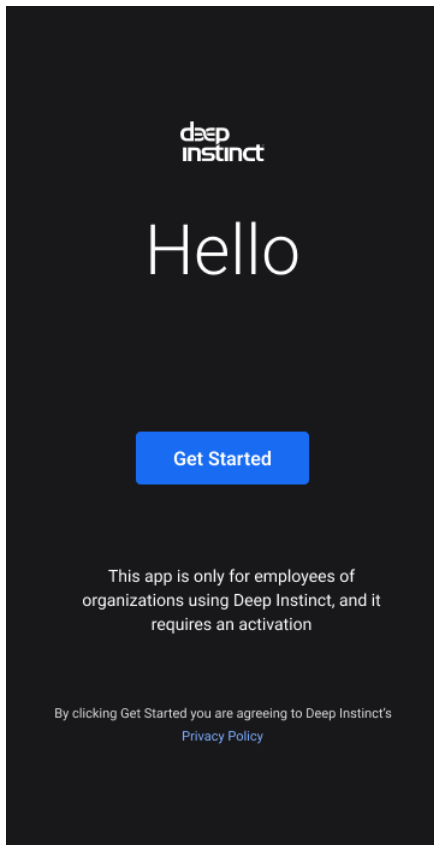
2. Tap Get App in the email to download and install Deep Instinct D-Client from Google Play. The Deep Instinct Agent installation screen opens.



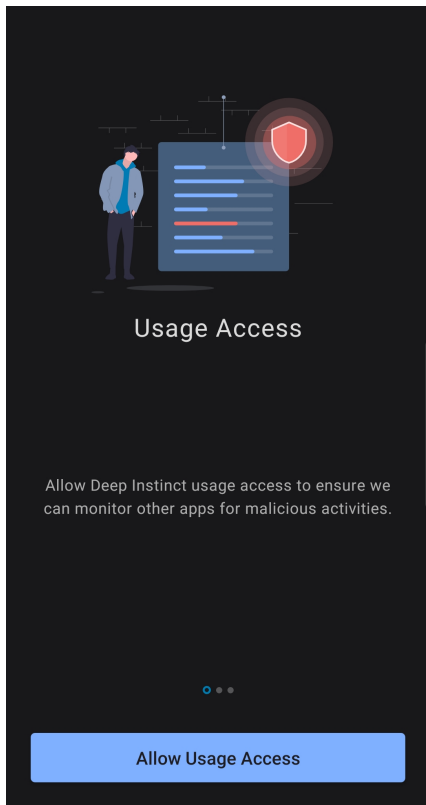
3. Tap INSTALL to install D-Client. A screen opens to indicate that Deep Instinct was installed.



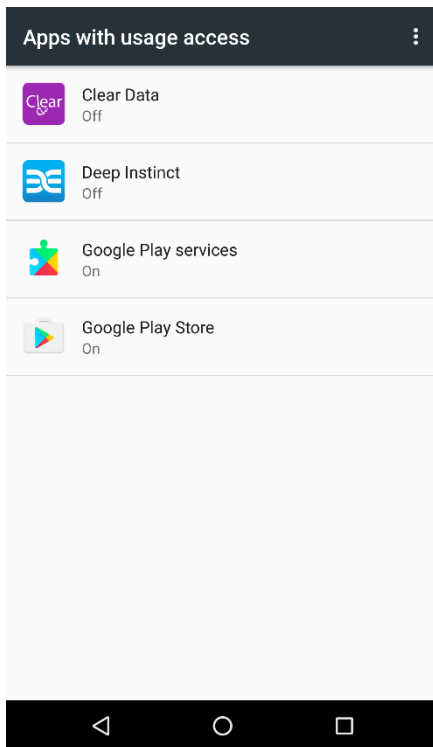
4. Tap CONTINUE to start D-Client. A screen opens to allow access to the privacy policy and to activate D-Client.



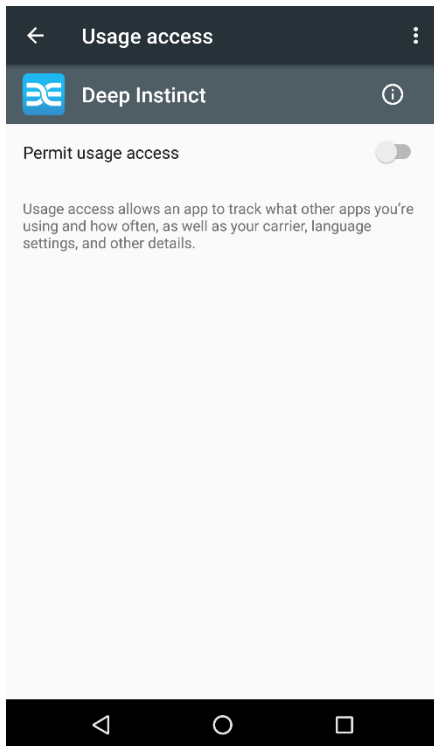
5. Tap Get Started. Deep Instinct D-Client is activated and scans your device.
6. In order to protect your device, specific permissions must be enabled. The order of the permission requests and some of the permissions, vary based on the operating system on your device.
7. Allow Usage Access to monitor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



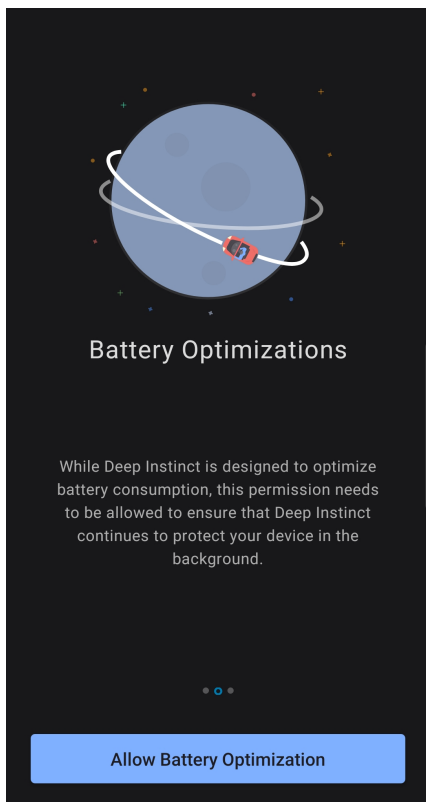
8. Tap Allow Usage Access and the Apps with usage access screen appears.



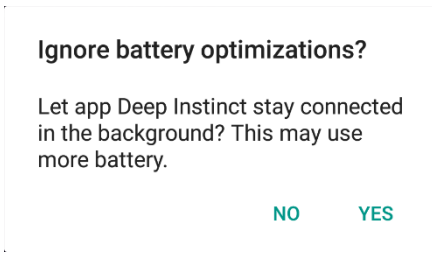
9. Tap Deep Instinct and the Usage access screen appears.



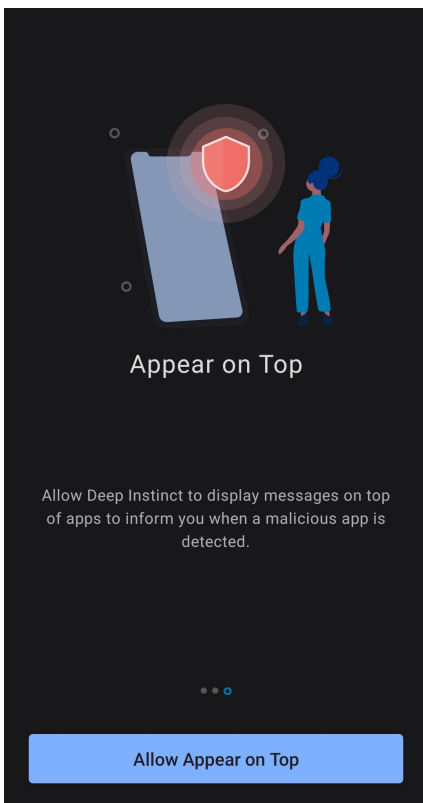
10. Tap the switch to permit usage access for Deep Instinct.
11. Enable Battery Optimizations permission to ensure continuous protection of your device.



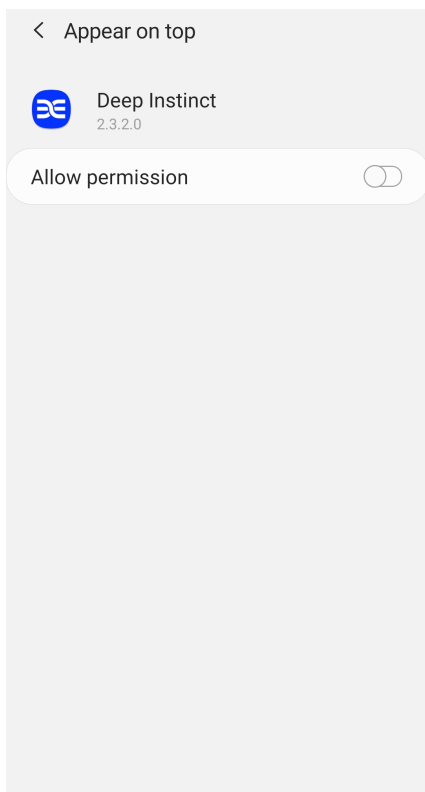
- To allow the Deep Instinct app to stay connected in the background, tap Allow Battery Optimization. A message appears.



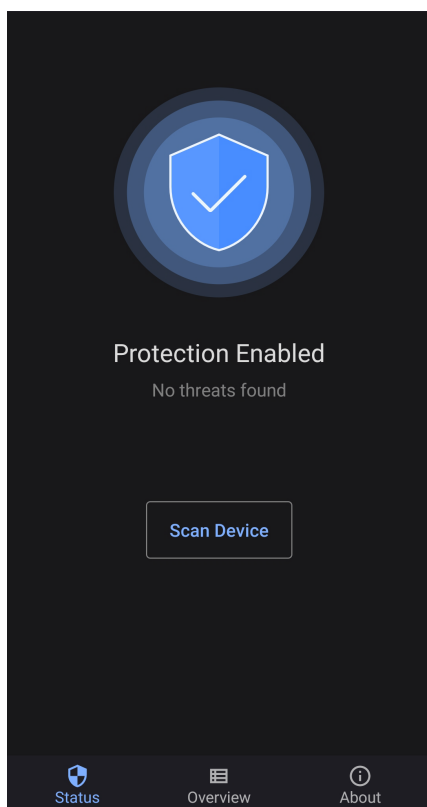
- Tap Yes to allow the Deep Instinct app to stay connected.
- For Android 10 — enable Appear on Top permission to display messages on top of apps when a malicious app is detected.



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



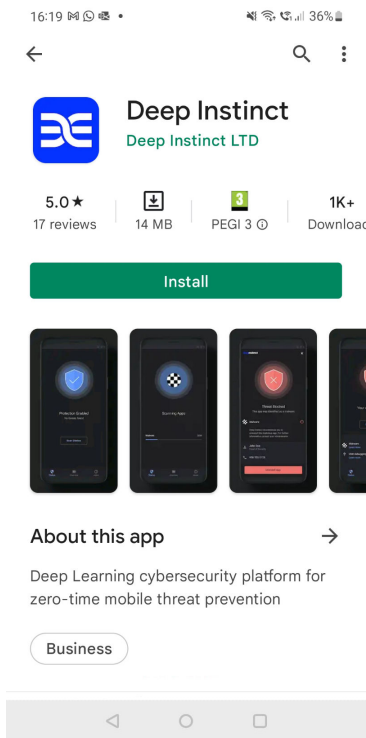
16. Tap the switch to allow this permission.
17. Once your device is scanned and no malicious file is detected, Deep Instinct informs you that no threats were found.



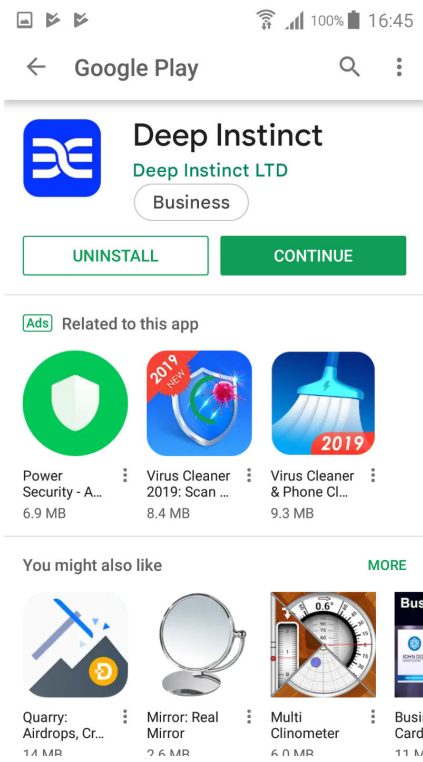
Alternative installation for Android devices

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:

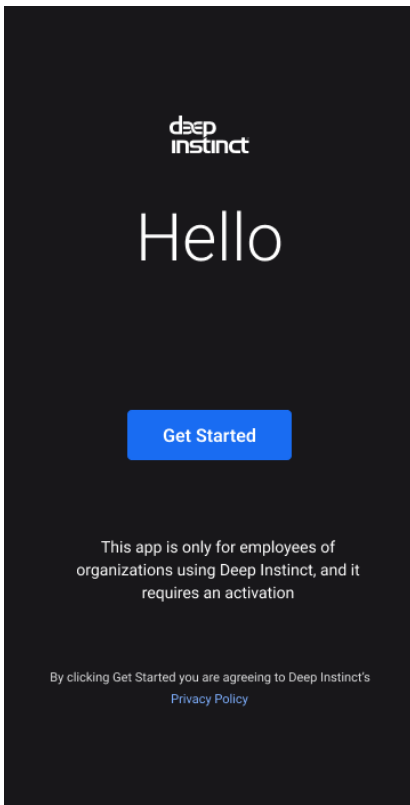
1. Go to **Google Play** and open the **Deep Instinct** app.



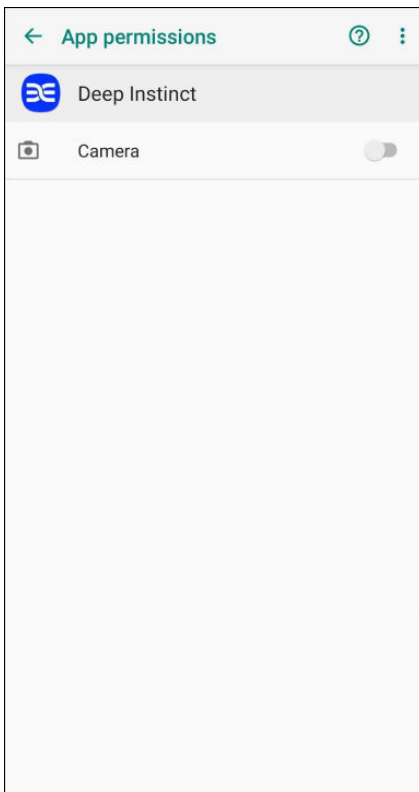
2. Tap Install to install D-Client. A screen opens to indicate that Deep Instinct was installed.



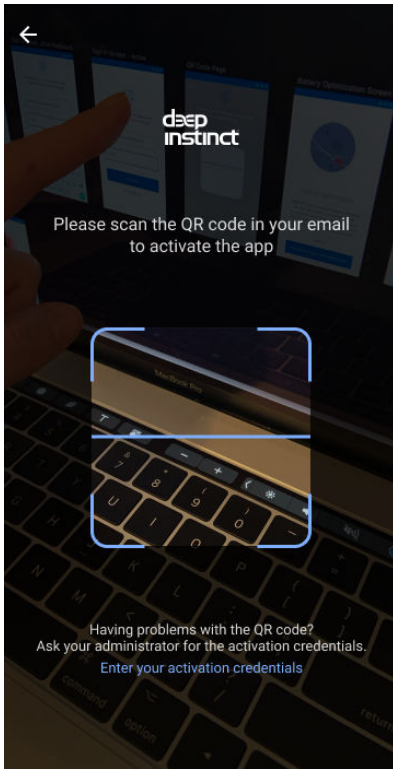
3. Tap Open to start D-Client. A screen opens to allow access to the privacy policy and to activate D-Client.



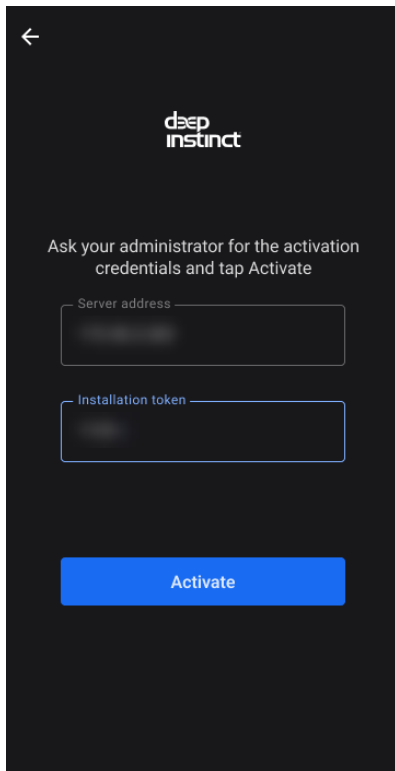
4. Tap Get Started and the App permissions screen opens.



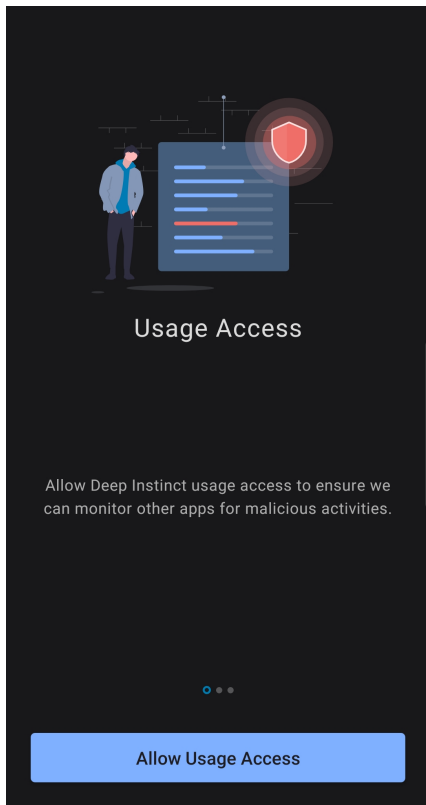
5. To use the QR Code to enter the information, tap the switch to permit camera usage. The QR Code Scanning screen opens and perform the following:



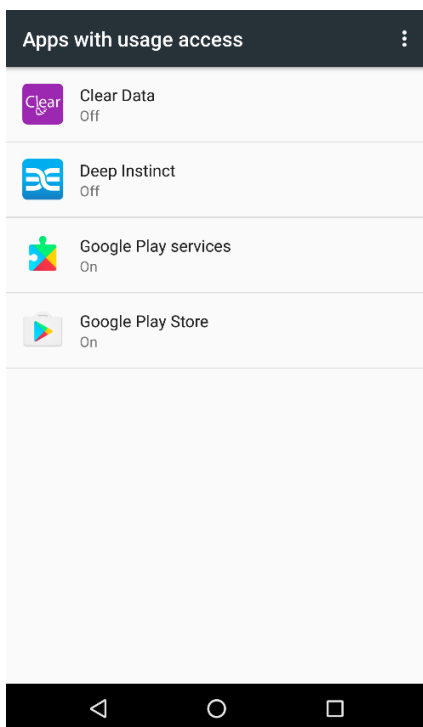
- a. Open the Installation email on another device.
 - b. With the camera on your Android device, scan the QR Code in the email.
6. To activate D-Client using your activation credentials, tap Enter your activation credentials. The Activation screen opens and perform the following:



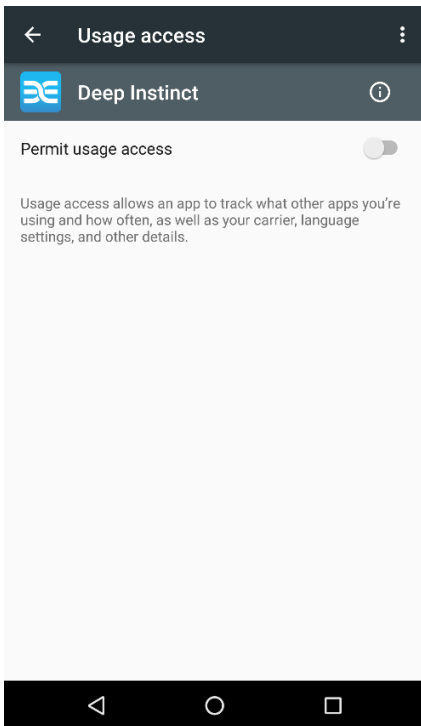
- a. Enter the Management server address and Installation token.
 - b. Tap **Activate**.
7. In order to protect your device, specific permissions must be enabled. The order of the permission requests and some of the permissions, varies based on the operating system on your device.
 8. Allow **Usage Access**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



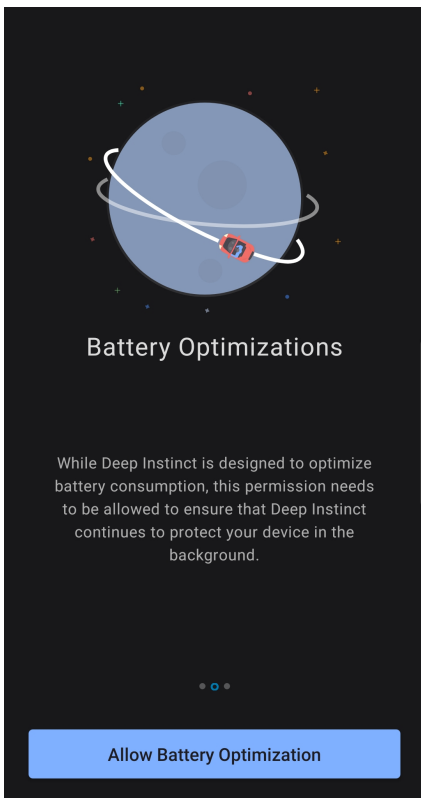
9. Tap **Allow Usage Access** and the Apps with usage access screen appears.



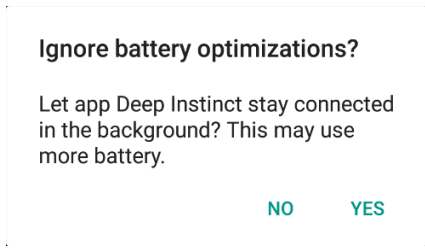
10. Tap **Deep Instinct** and the Usage access screen opens.



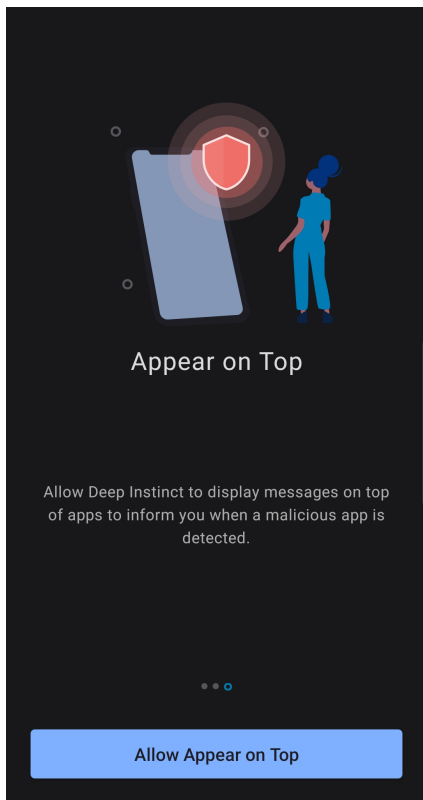
11. Tap the switch to permit usage access for Deep Instinct.
12. Enable Battery Optimizations permission to ensure continuous protection of your device.



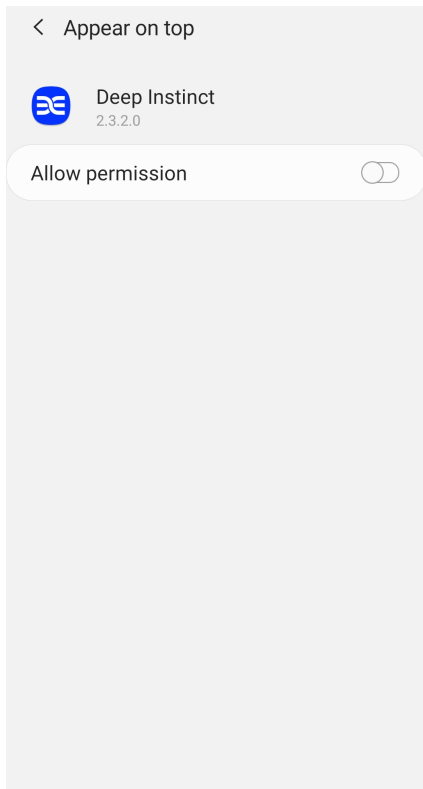
- To allow the Deep Instinct app to stay connected in the background, tap Allow Battery Optimization. A message appears.



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

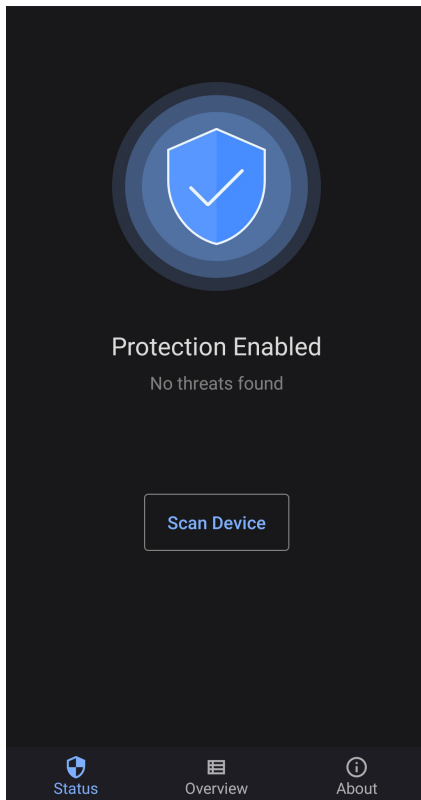


- Tap **Allow Appear on Top** and the Appear on top appears.



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.

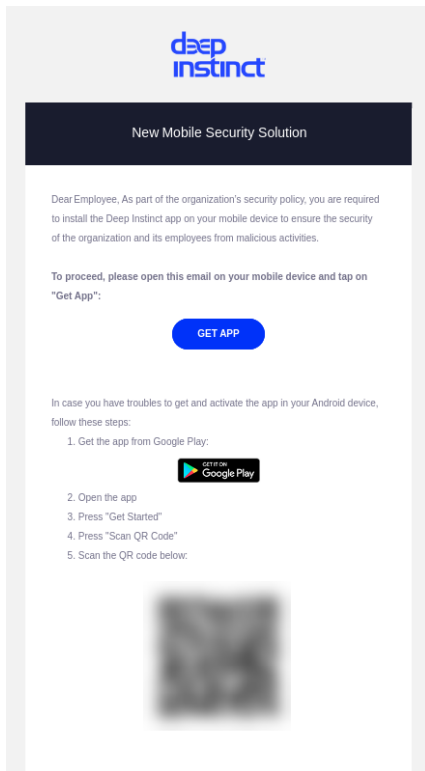


Email installation for Chrome OS devices

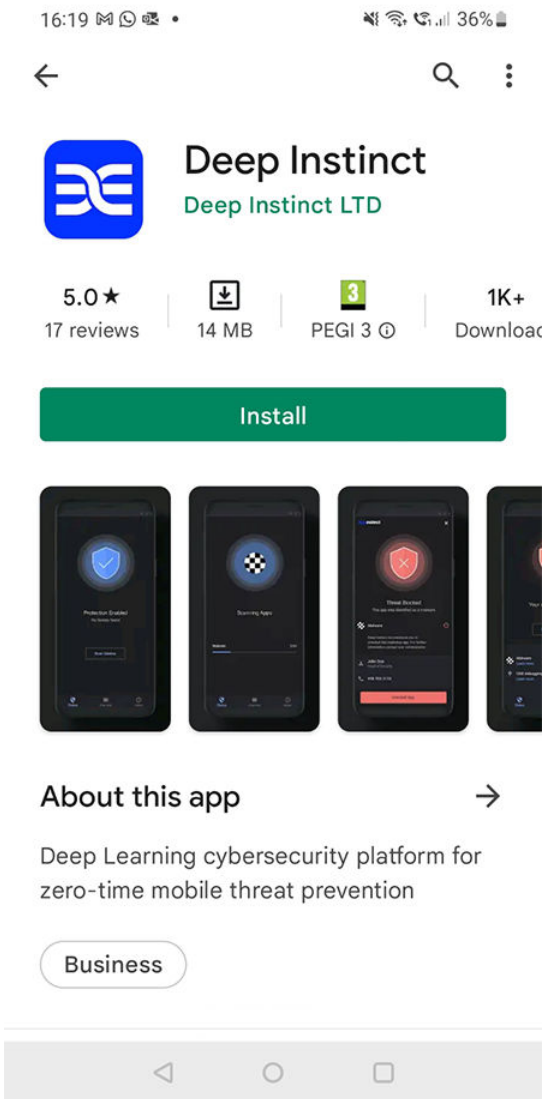
The email installation is the preferred method to install Deep Instinct D-Client on your Chrome OS device. If an email app has been installed (such as Gmail) in addition to the built-in app, use the installed email app to open the installation email. If the built-in email app will be used, a setting 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:

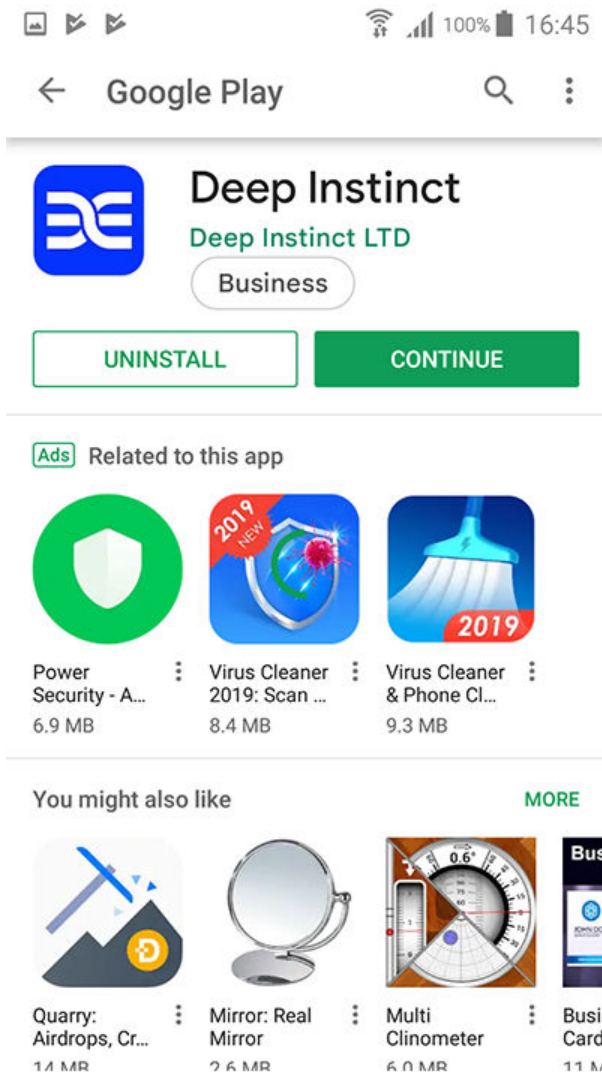
1. If an email app has been installed on the Chrome OS device, open the installation email on the device using the installed app. If the built-in email app will be used, follow the steps in



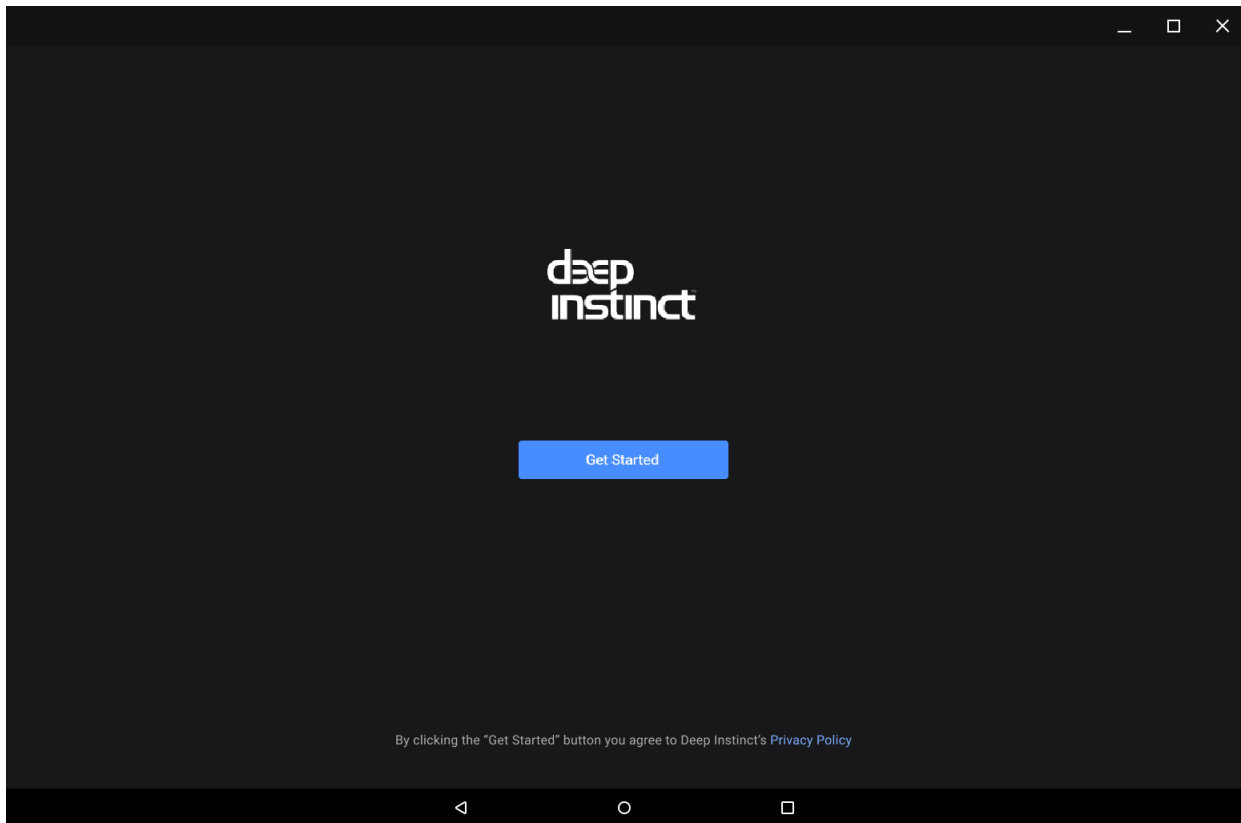
2. Click Click App in the email to download and install Deep Instinct D-Client from Google Play. The Deep Instinct Agent installation screen opens.



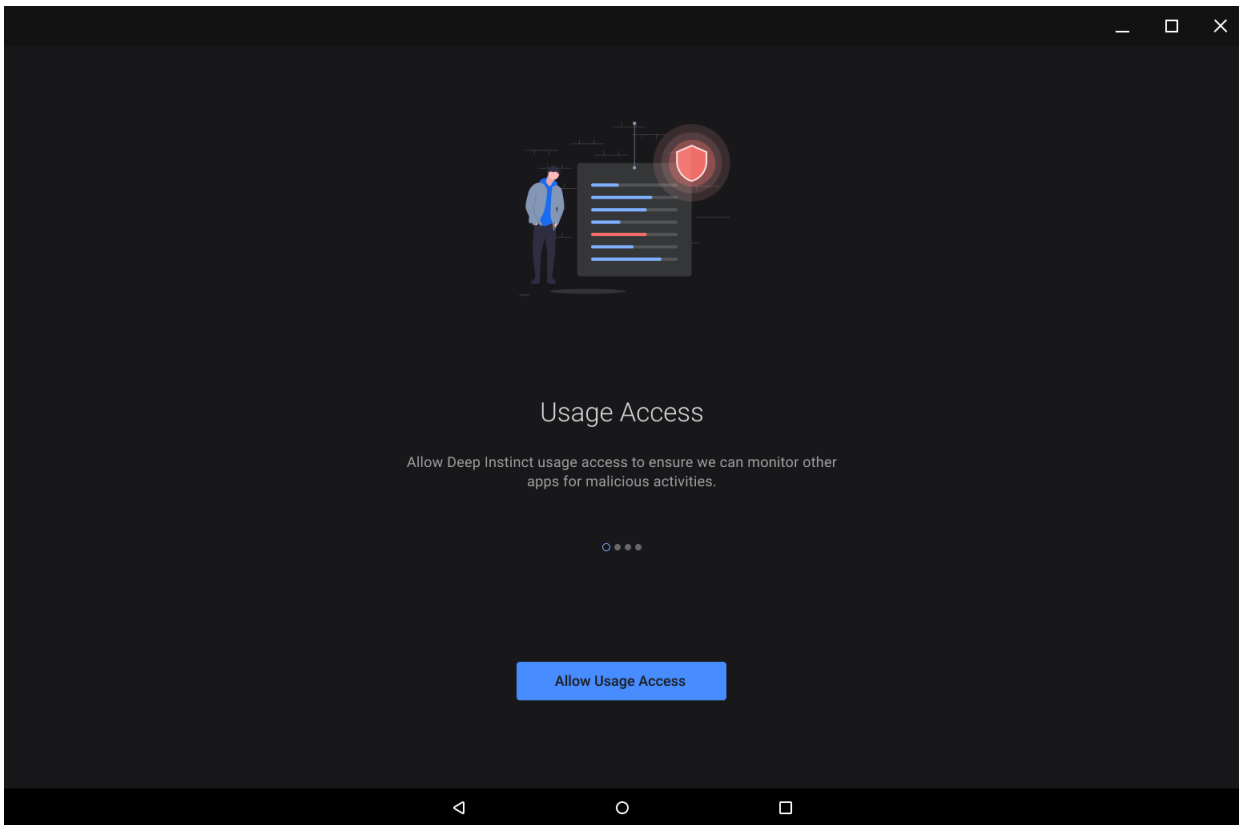
3. Click INSTALL to install D-Client. A screen opens to indicate that Deep Instinct was installed.



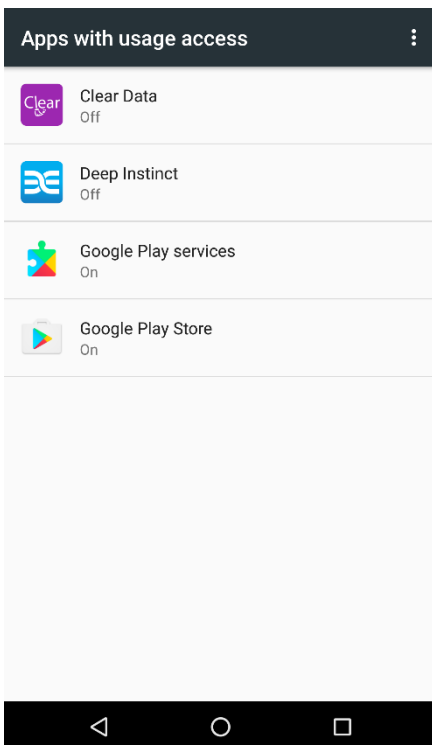
4. Click CONTINUE to start D-Client. A screen opens to allow access to the privacy policy and to activate D-Client.



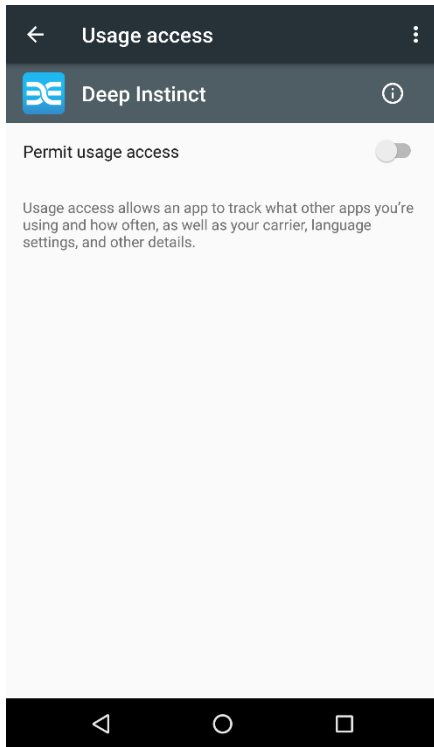
5. Click Get Started. Deep Instinct D-Client is activated and scans your device.
6. In order to protect your device, specific permissions must be enabled. The order of the permission requests and some of the permissions, vary based on the operating system on your device.
7. Allow Usage Access to monitor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



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



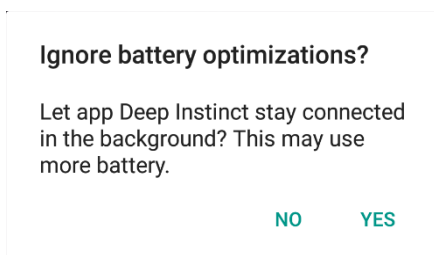
9. Click Deep Instinct and the Usage access screen appears.



10. Enable Permit usage access for Deep Instinct.

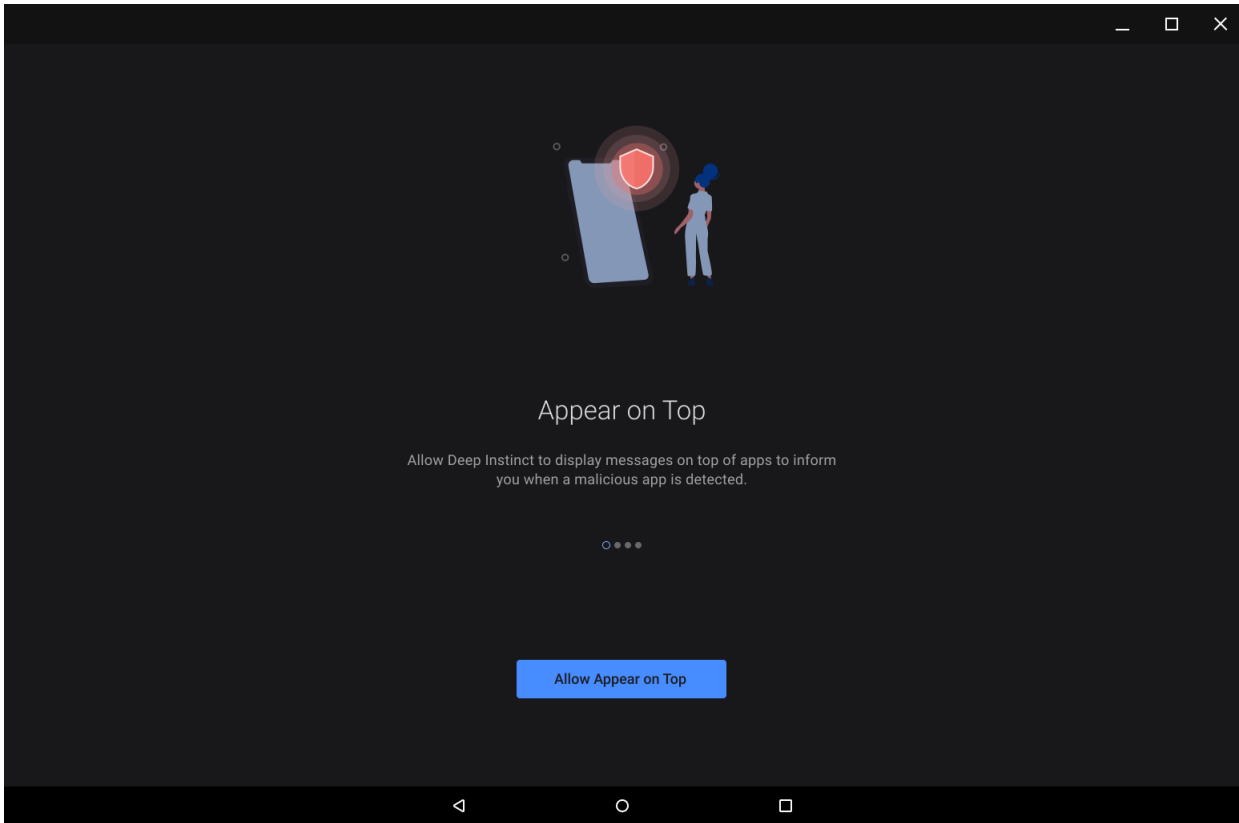
11. Click Allow Battery Optimization to ensure continuous protection of your device.

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

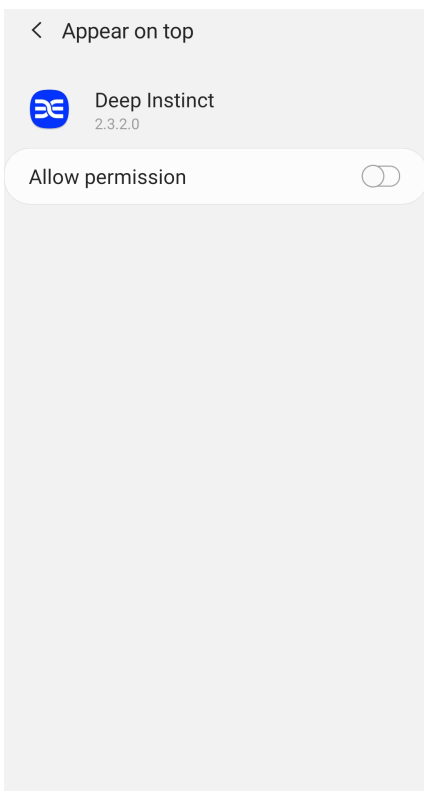


13. Click Yes to allow the Deep Instinct app to stay connected.

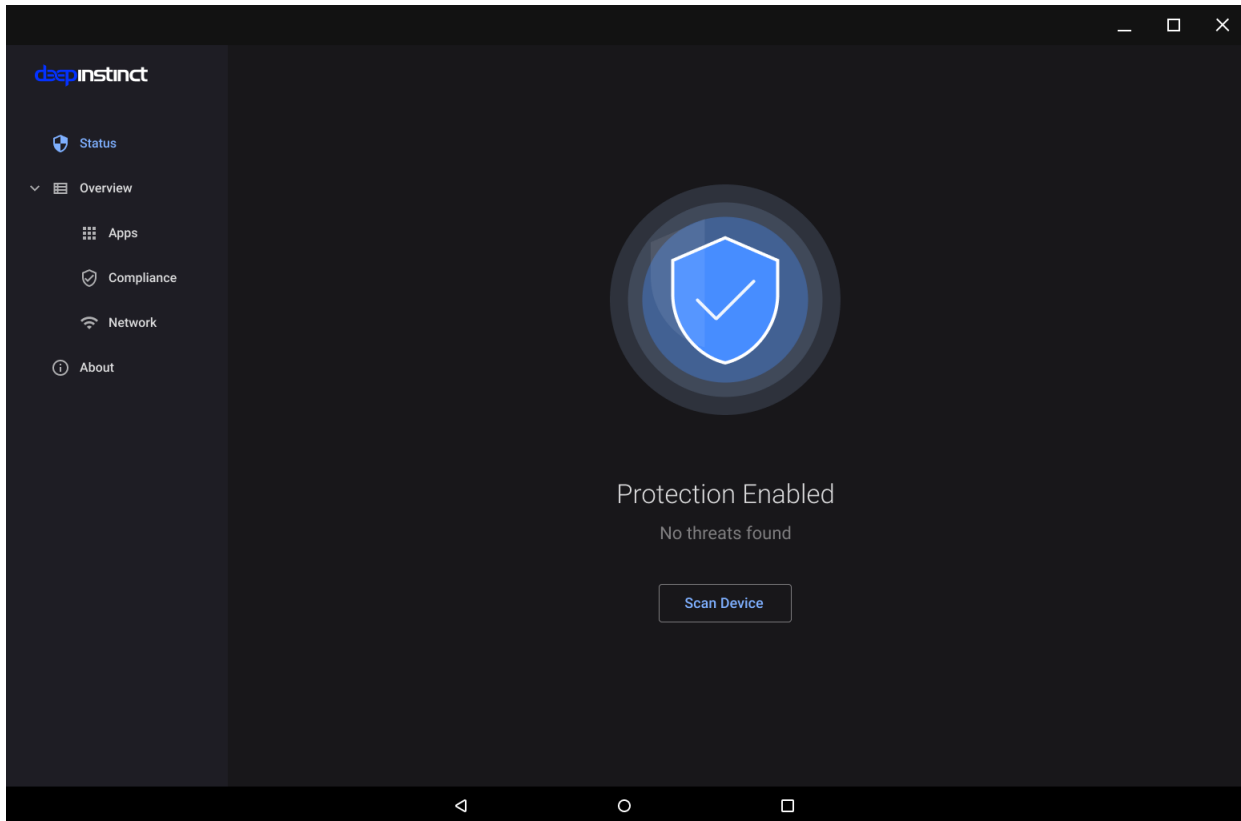
14. For Android 10 — enable Appear on Top permission to display messages on top of apps when a malicious app is detected.



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



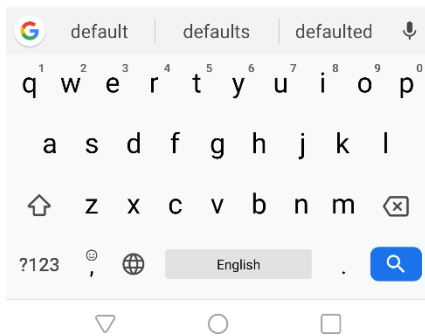
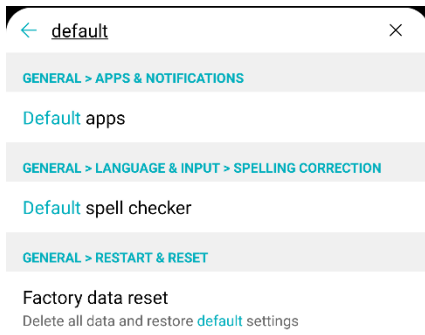
16. Enable the Allow Permission option.
17. Once your device is scanned and no malicious file is detected, Deep Instinct informs you that no threats were found.



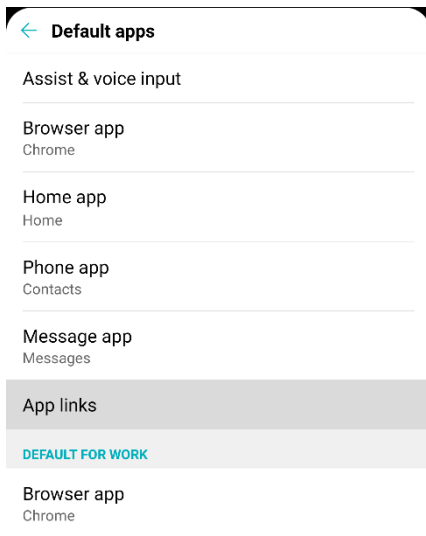
Installation prerequisite using Chrome OS built-in email app

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](#).

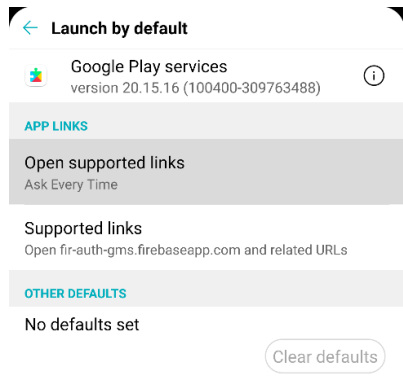


2. Search and go to “Default apps”.

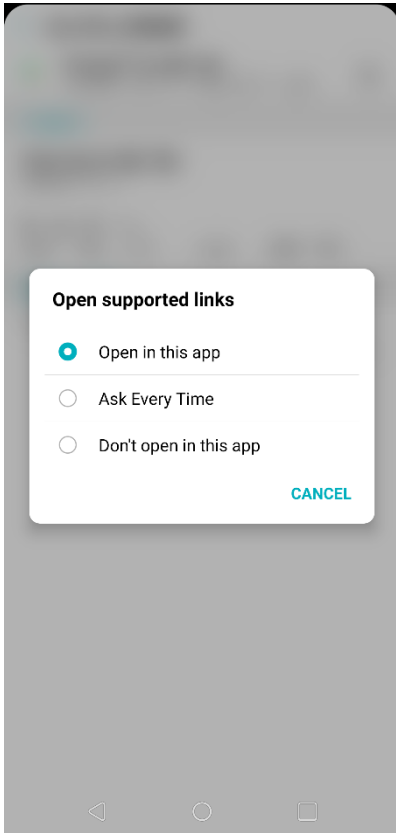


3. Click App links.

4. Click Google Play services.



5. Click Open supported links.



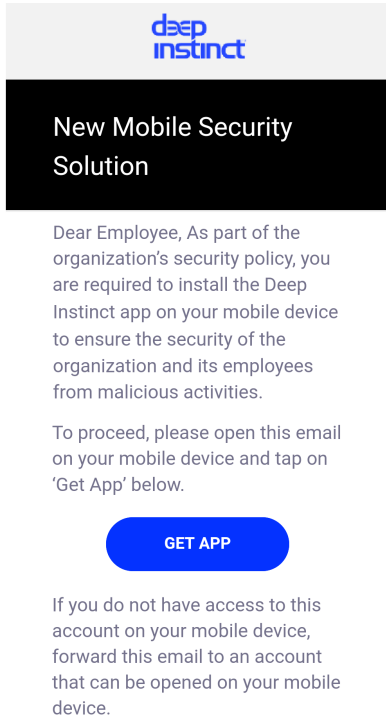
6. Select Open in this app.

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

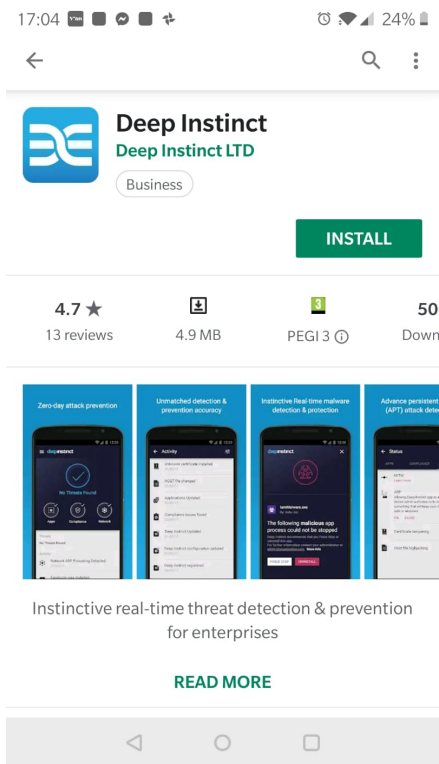
Email installation for iOS and iPadOS devices

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

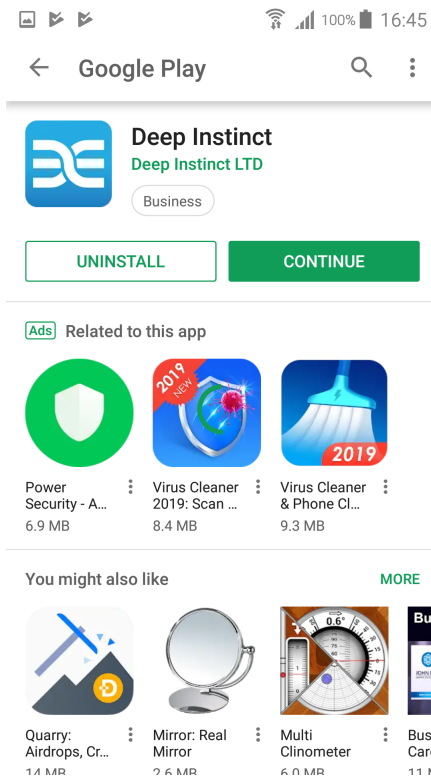
1. Open the installation email on the iOS or iPadOS device and read the email.



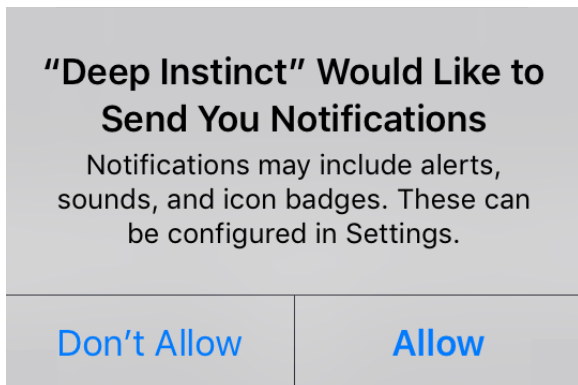
2. Tap Get App in the email to download and install Deep Instinct D-Client from App Store. The Deep Instinct Agent installation screen opens.



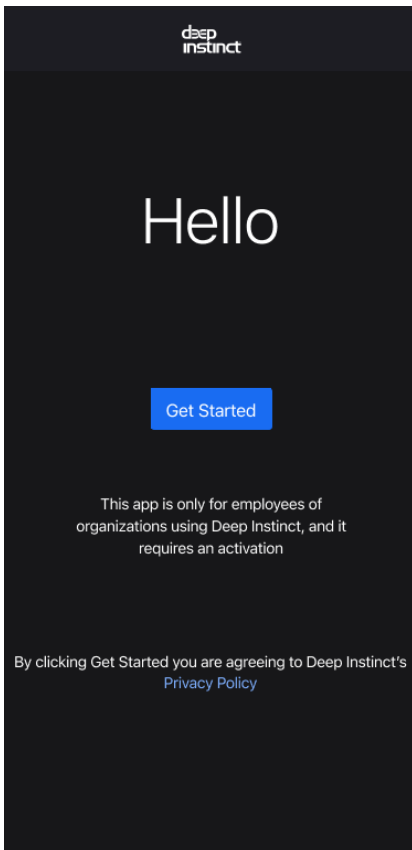
3. Tap GET to install D-Client. A screen opens to indicate that Deep Instinct was installed.



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

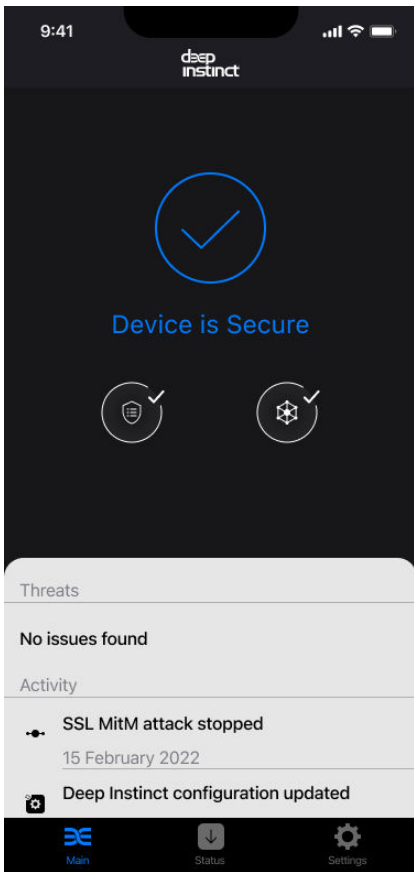


To allow the Deep Instinct app to display security notifications, tap Allow. A screen opens to allow access to the privacy policy and to activate D-Client.



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

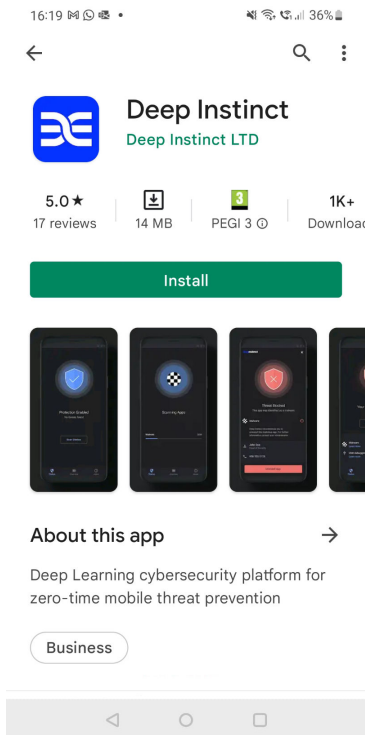
Once your device is scanned and no problems were detected, Deep Instinct informs you that your device is secure.



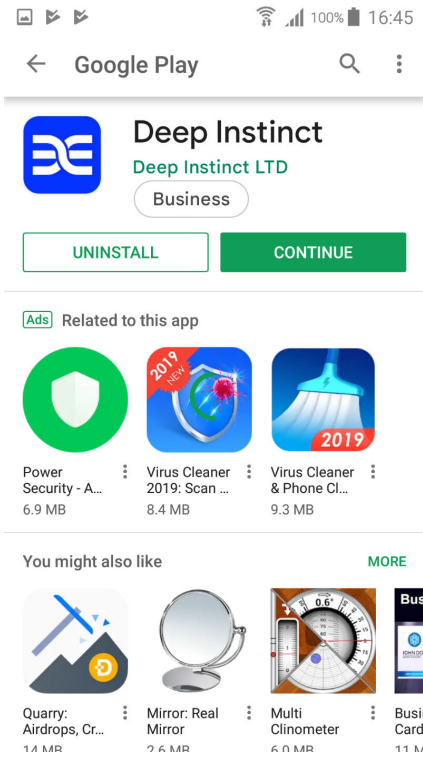
Alternative installation for iOS and iPadOS devices

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:

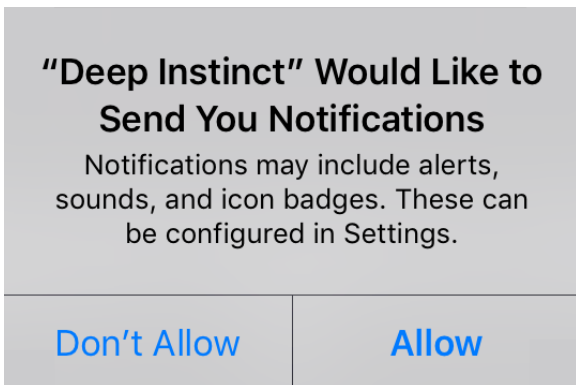
1. Go to App Store and open the Deep Instinct app.



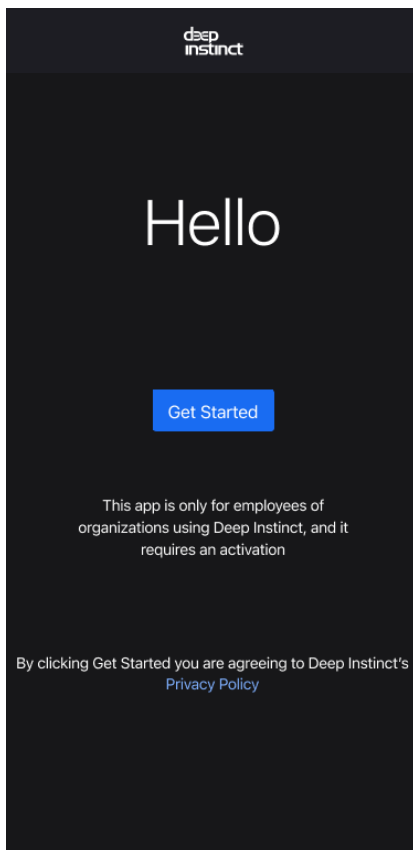
2. Tap GET to install D-Client. A screen opens to indicate that Deep Instinct was installed.



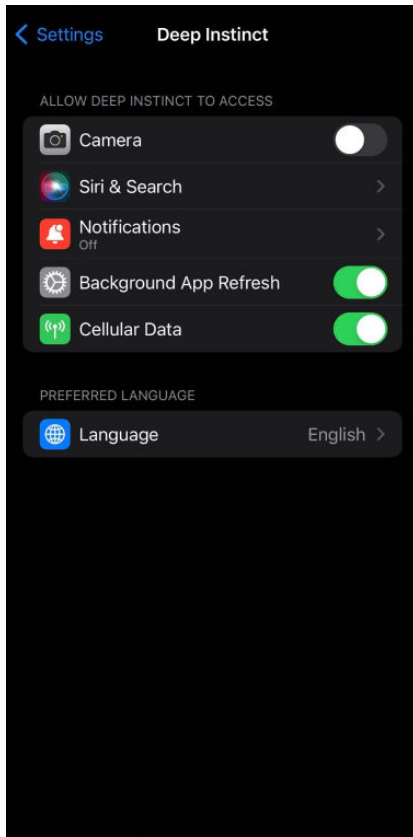
3. Tap OPEN to start D-Client. A notification message appears.



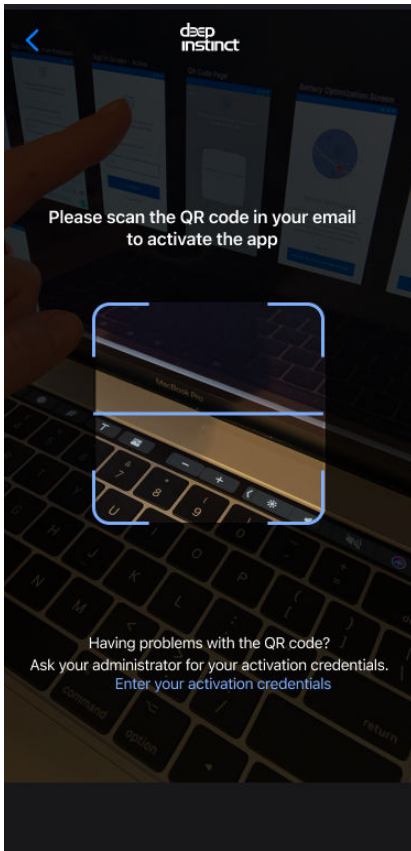
4. To allow the Deep Instinct app to display security notifications, tap Allow. A screen opens to allow access to the privacy policy and to activate D-Client.



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

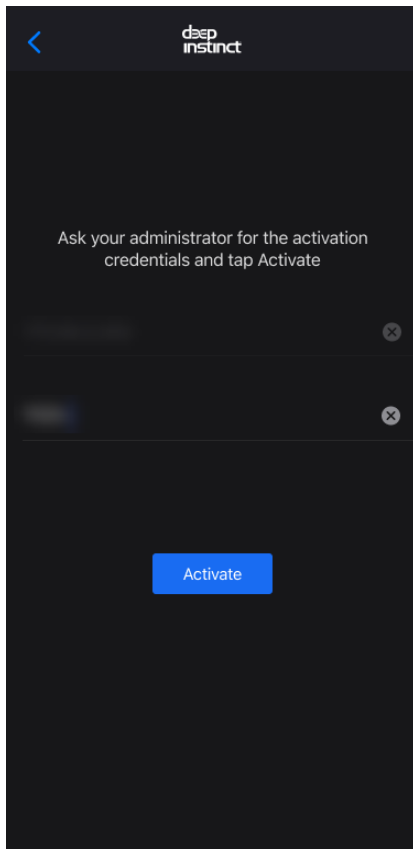


6. To use the QR Code to enter the information, tap the switch to permit camera usage. The QR Code Scanning screen opens.

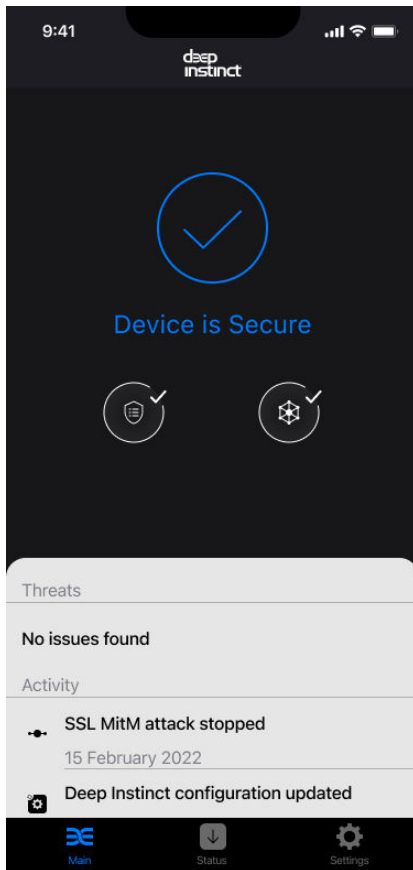


Perform the following:

- 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>	FQDN for the Management Server (D-Appliance)	N/C
<token>	ID of the installation token, as displayed in the Linux Deployment Resources screen.	N/C
PROXY_URL	Enables the use of a network proxy server, using the specified settings of the proxy server URL and port number.	Optional
<proxy url>	URL for the proxy server, including the scheme.	N/C
<proxy port>	Port number to access the proxy server.	<ul style="list-style-type: none"> Optional — only relevant with REST API integration Do not use with CERT or PRIVATE_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 PRIVATE_KEY	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_certificate>	Single line base64 encoded string of the certificate file.	N/C
<base64_key>	Single line base64 encoded string of the private key associated with the certificate.	N/C


Command Parameter	Description	Comments
<service port>	Port number used for integration using ICAP or REST API.	Typically, ICAP uses port number 1344 and REST API port number 443.
<Exposed port>	Port number used for integration using ICAP or REST API: <1344> OR <443>	Typically, ICAP uses port number 1344 and REST API port number 443.
NUM_THREADS_PER_WORKER:	Used for configuring the number of Gunicorn (Python web server) threads for the worker processes handling the REST API requests: NUM_THREADS_PER_WORKER = 4*Number of CPUs	<ul style="list-style-type: none"> 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 “DISABLE_WORKER_THREADING” parameter.
DISABLE_WORKER_THREADING	Disables the worker threading: <ul style="list-style-type: none"> DISABLE_WORKER_THREADING = true when threading is disabled DISABLE_WORKER_THREADING = false when threading is enabled 	<ul style="list-style-type: none"> 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_WORKERS :	Enables configuring the number of workers	<ul style="list-style-type: none"> Applies to REST integration only Optional — can be manually added to the command Default (without this parameter) = 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

- 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.
- Once your container is registered with the Management Server and the configurations files have been downloaded, you can proceed to send files for scanning.



NOTE

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:

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

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

```
mkdir dipa-pkg
```

- 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.

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

```
cd dipa-pkg
```

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

```
docker build -t agentless --network=none
```

- 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
```

- 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>	FQDN for the Management Server (D-Appliance)	N/C

Command Parameter	Description	Comments
<token>	ID of the installation token, as displayed in the Linux Deployment Resources screen.	N/C
PROXY_URL	Enables the use of a network proxy server, using the specified settings of the proxy server URL and port number.	Optional
<proxy url>	URL for the proxy server, including the scheme.	N/C
<proxy port>	Port number to access the proxy server.	<ul style="list-style-type: none"> Optional — only relevant with REST API integration Do not use with CERT or PRIVATE_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 PRIVATE_KEY	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_cert>	Single line base64 encoded string of the certificate file.	N/C
<base64_key>	Single line base64 encoded string of the private key associated with the certificate.	N/C
<service port>	Port number used for integration using ICAP or REST API.	Typically, ICAP uses port number 1344 and REST API port number 443.


Command Parameter	Description	Comments
<Exposed port>	<p>Port number used for integration using ICAP or REST API:</p> <p><1344></p> <p>OR</p> <p><443></p>	<p>Typically, ICAP uses port number 1344 and REST API port number 443.</p>
NUM_THREADS_PER_WORKER:	<p>Used for configuring the number of Gunicorn (Python web server) threads for the worker processes handling the REST API requests:</p> <p>NUM_THREADS_PER_WORKER = 4*Number of CPUs</p>	<ul style="list-style-type: none"> 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 “DISABLE_WORKER_THREADING” parameter.
DISABLE_WORKER_THREADING	<p>Disables the worker threading:</p> <ul style="list-style-type: none"> DISABLE_WORKER_THREADING = true when threading is disabled DISABLE_WORKER_THREADING = false when threading is enabled 	<ul style="list-style-type: none"> 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_WORKERS:	Enables configuring the number of workers	<ul style="list-style-type: none"> 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.



NOTE

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.



NOTE

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: Malware
X-Infection-Found	<p>Contains the description of the threat that was found in the content. If multiple threats were found, only the first one is returned.</p> <p>The value is a semicolon separated list with three parameters.</p> <p>Type:</p> <p>0: Infection was found.</p> <p>2: Container violation was found.</p> <p>Resolution:</p> <p>0: Suspicious content was not repaired.</p> <p>Threat: Threat name</p>	<p>X-Infection-Found: Type=0; Resolution=0; Threat=EICAR Test String</p> <p>X-Infection-Found: Type=2; Resolution=0; Threat=Encrypted Archive;</p>
X-Violations-Count	Contains the number of the reported violations	0
X-Violation<number>-FileName	Name of the file that was blocked	eicar.zip
X-Violation<number>-ThreatName	A name describing the threat	Malware
X-Violation<number>-ProblemID	Currently 0 returned for all threats	0

Header Name	Description	Example
X-Violation<num-ber>-ResolutionID	0: File was not repaired 1: File was 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:

```
curl -k https://localhost/scan/binary/
-H "Content-Type: application/octet-stream" \
--data-binary @eicar.exe
```

Where:

Entry	Description
https://localhost/scan/binary	URL to which the request is sent
-H "Content-Type: application/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	Description	Example Value	Comments
verdict	File scan verdict	Malicious	<p>In case the verdict is a failure verdict (Unsupported, Timeout, Classification Failed) some fields, like severity, file_type, scan_duration, may not be available.</p> <p>Supported values:</p> <ul style="list-style-type: none"> ■ Malicious ■ Benign ■ Unsupported File Type ■ Unsupported File Size ■ Classification Failed ■ Timeout
submit_time_in_milliseconds	Local time on the Application Security Connector when the request was submitted	1589284291800	N/C

Field	Description	Example Value	Comments
severity	<p>Threat severity</p> <p>This is not included in the response for benign files.</p>	VERY_HIGH	<p>Possible values:</p> <ul style="list-style-type: none"> ▪ VERY_LOW ▪ LOW ▪ MODERATE ▪ HIGH ▪ VERY_HIGH
scan_duration_in_microseconds	<p>Time in microseconds to complete the classification</p>	17159	
malware_family	<p>Deep Classification of the file. If multiple exist, the primary is returned.</p> <p>This is not included in the response for non-PE or benign files.</p>	BACKDOOR	<p>Possible values:</p> <ul style="list-style-type: none"> ▪ RANSOMWARE ▪ BACKDOOR ▪ DROPPER ▪ PUA ▪ SPYWARE ▪ VIRUS ▪ WORM

Field	Description	Example Value	Comments
file_type	File format of the scanned file	PE64FileType	<p>Possible values:</p> <ul style="list-style-type: none"> ▪ Other ▪ Macho32FileType ▪ Macho64FileType ▪ MachoFATFileType ▪ XarFileType ▪ TarFileType ▪ PDFFileType ▪ DMGFileType ▪ RTFFFileType ▪ TTFFileType ▪ OTFFFileType ▪ OfficeFileType ▪ ZipFileType ▪ SevenZipFileType ▪ EICARType ▪ RARFileType ▪ PE32FileType ▪ PE64FileType ▪ PEFileType ▪ SWFFFileType ▪ TIFFFFileType

Field	Description	Example Value	Comments
			<ul style="list-style-type: none"> ■ JarFileType ■ OOXMLFileType ■ OLEInOOXMLFileType ■ GzipFileType
file_size_in_bytes	Size of the scanned file	2465280	
file_hash	Sha256 hash of the malicious/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 container, and not the malicious file	1e0faca8e6847e1b0fe 7c2a7131254027cc38 e8489840bf9e5355ef3 b00c836b	
event_description	An explanation of the event	Office file identified as malicious	

Field	Description	Example Value	Comments
additional_office_data	<p>List of values for different components in the document.</p> <p>1 means the document contains this component</p>	<pre>{ "vba": 1, "swf": 0, "load_external_object": 0, "dde": 0, "xl4_macros": 0, "activex": 0} </pre>	<p>When the value is 1, the document contains the following:</p> <ul style="list-style-type: none"> ■ VBA: VBA macro ■ SWF: Adobe Flash object ■ Reference to an external object (RELS) ■ DDE object ■ XL4 macros (old type of macros) ■ Embedded ActiveX 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-
balb526cbe4a1bc57ba178f25f20e18eba438b6d96361b337a30ee7c",
"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.

- **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:

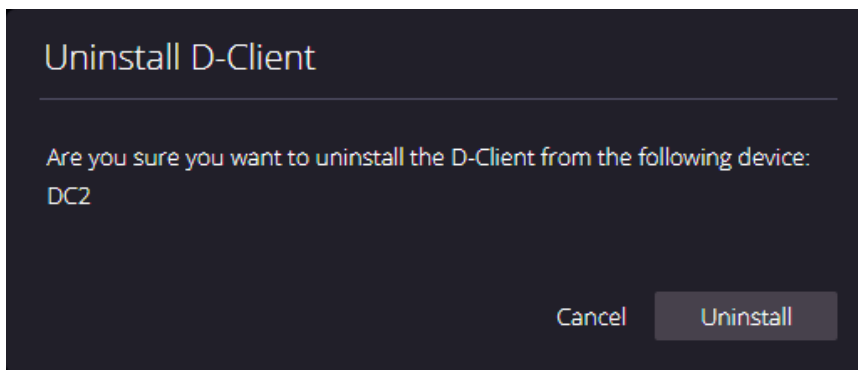
- As the default, uninstalled devices are not displayed in the Device List. However, the Device List can display these devices, by displaying devices with an Uninstalled status.
- On Windows and macOS devices, the D-Client is uninstalled.
- When the Android D-Client is remotely uninstalled using the 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:

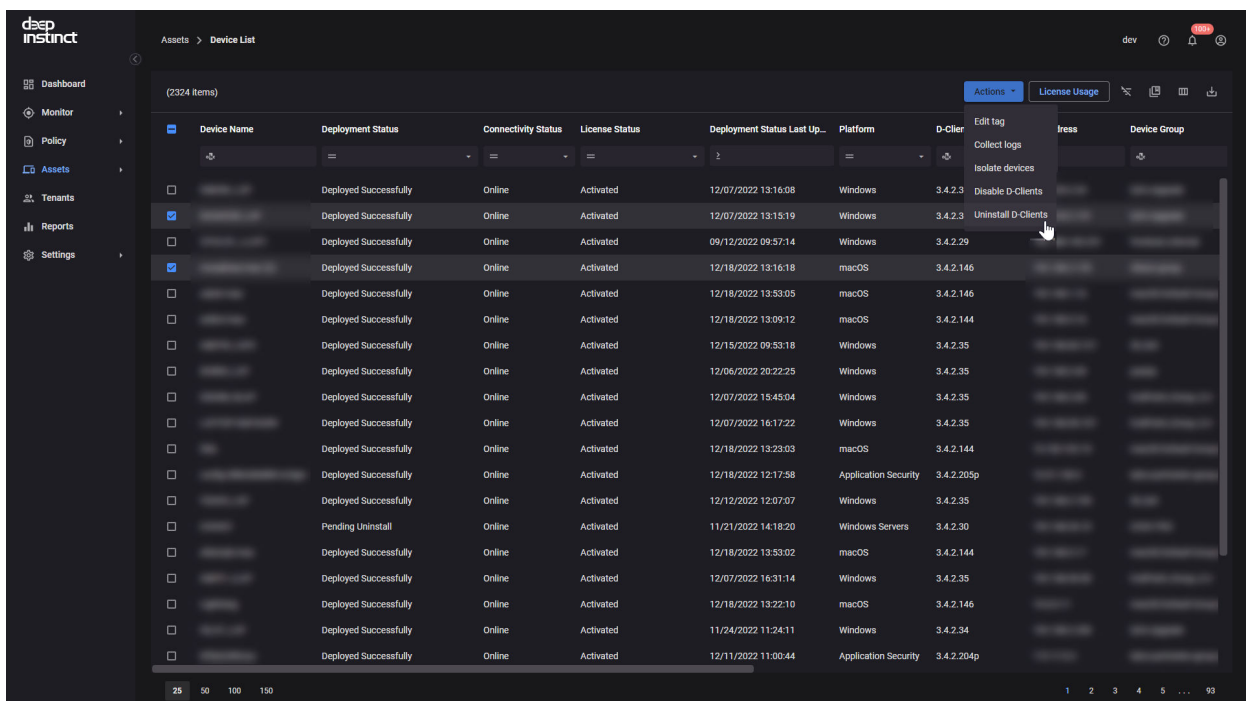
1. Select **Assets** → **Device List** Device List from the Management Console Navigation pane.
2. Right-click the device, on which the D-Client is installed and then select **Uninstall D-Client**. A confirmation dialog appears. dialog box opens to confirm your request.



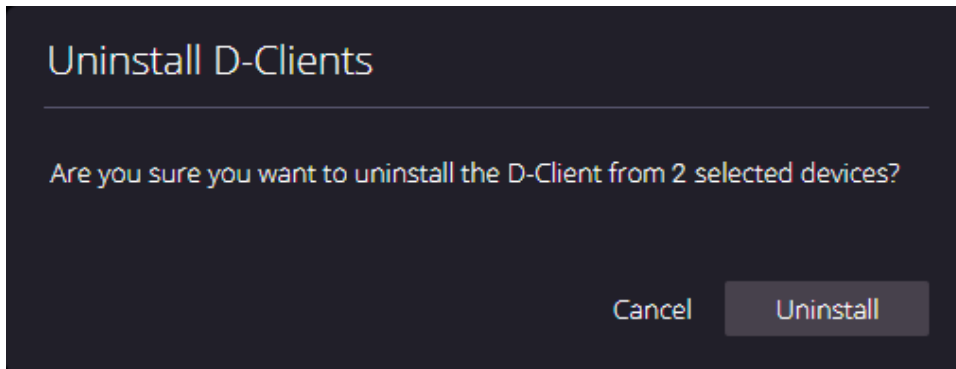
3. Click **Uninstall**. The Deployment Status for the device changes to **Pending Uninstall** and the device is instructed to uninstall the D-Client. After the D-Client is uninstalled, the status changes to **Uninstalled**.

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

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



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.



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.

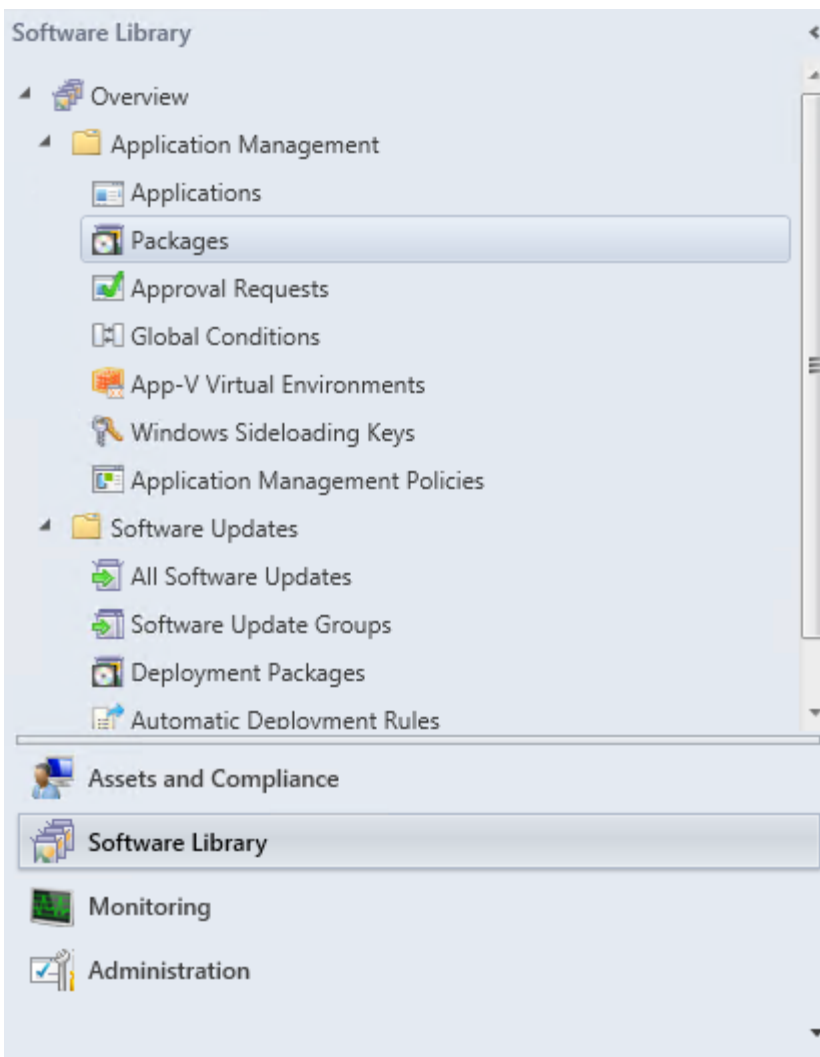
The D-Client uninstall process using SCCM requires the following:

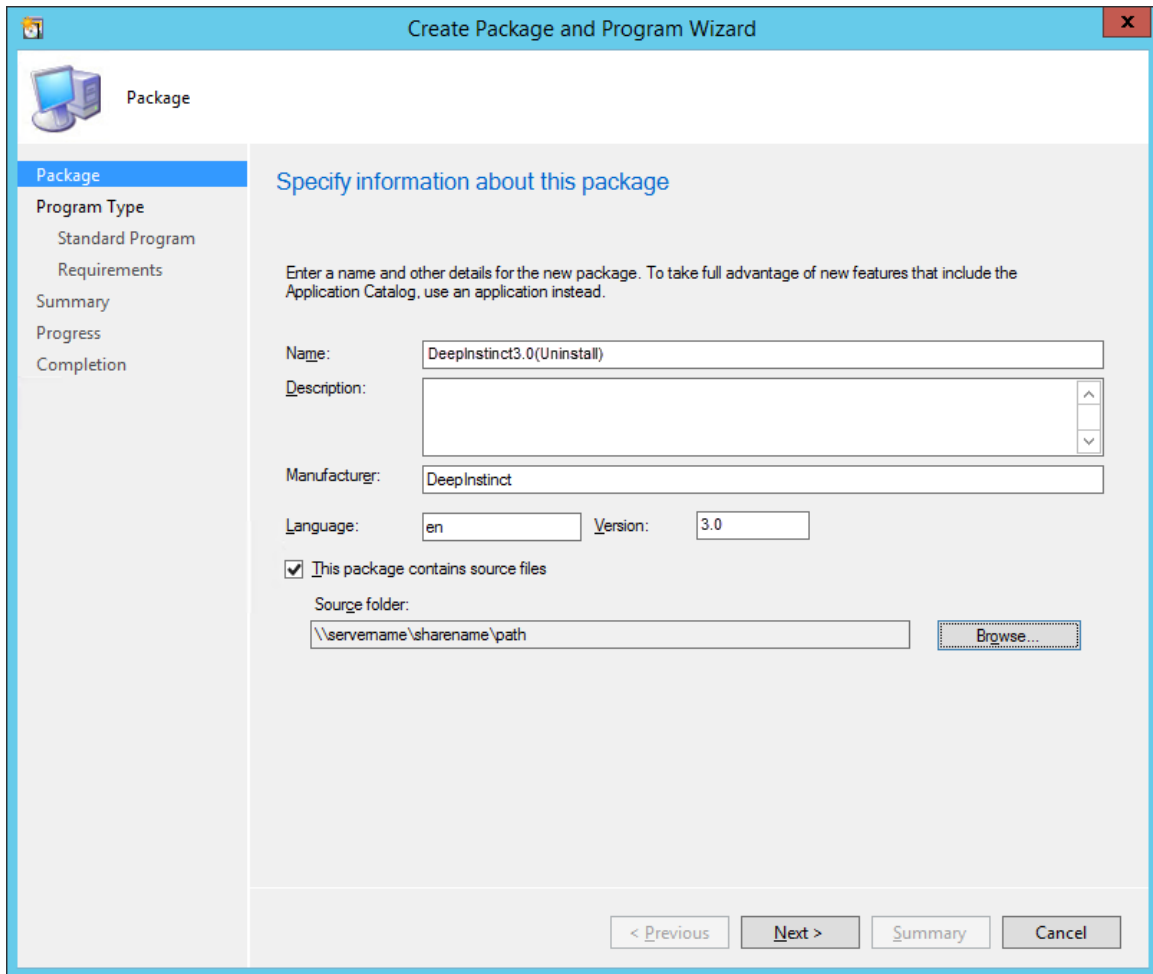
- Deep Instinct Windows EXE installation file. File may be downloaded from the [Windows Deployment Resources](#) screen.
- [Create a package to uninstall D-Clients](#)
- [Deploy the D-Client uninstall package](#)

Creating a Package to Uninstall D-Clients

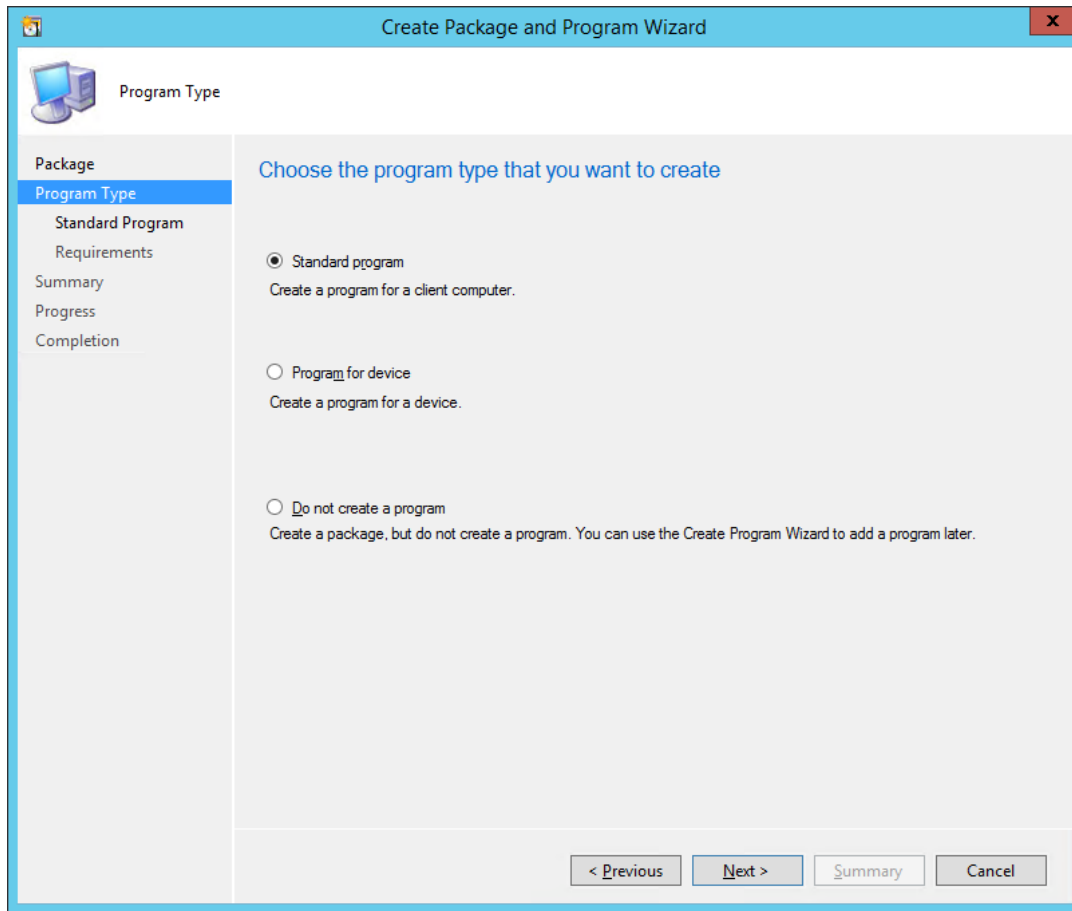
To create a package to uninstall D-Clients:

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:

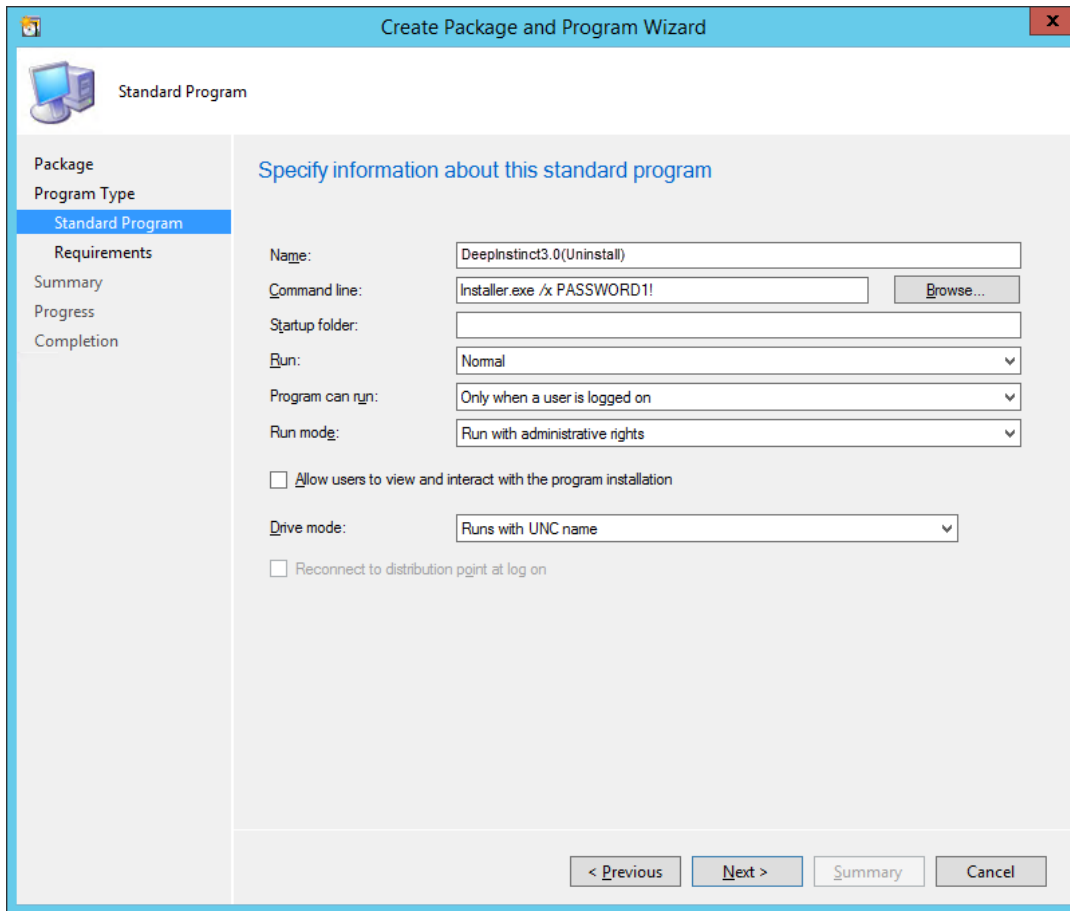




- a. Enter the name of the package.
- b. As an option, enter the description, manufacturer, language, and/or version of the package. It is recommended to enter the version number for version control.
- c. Select This package contains source files.
- d. Click **Browse**. Go to the folder where the installation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



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



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

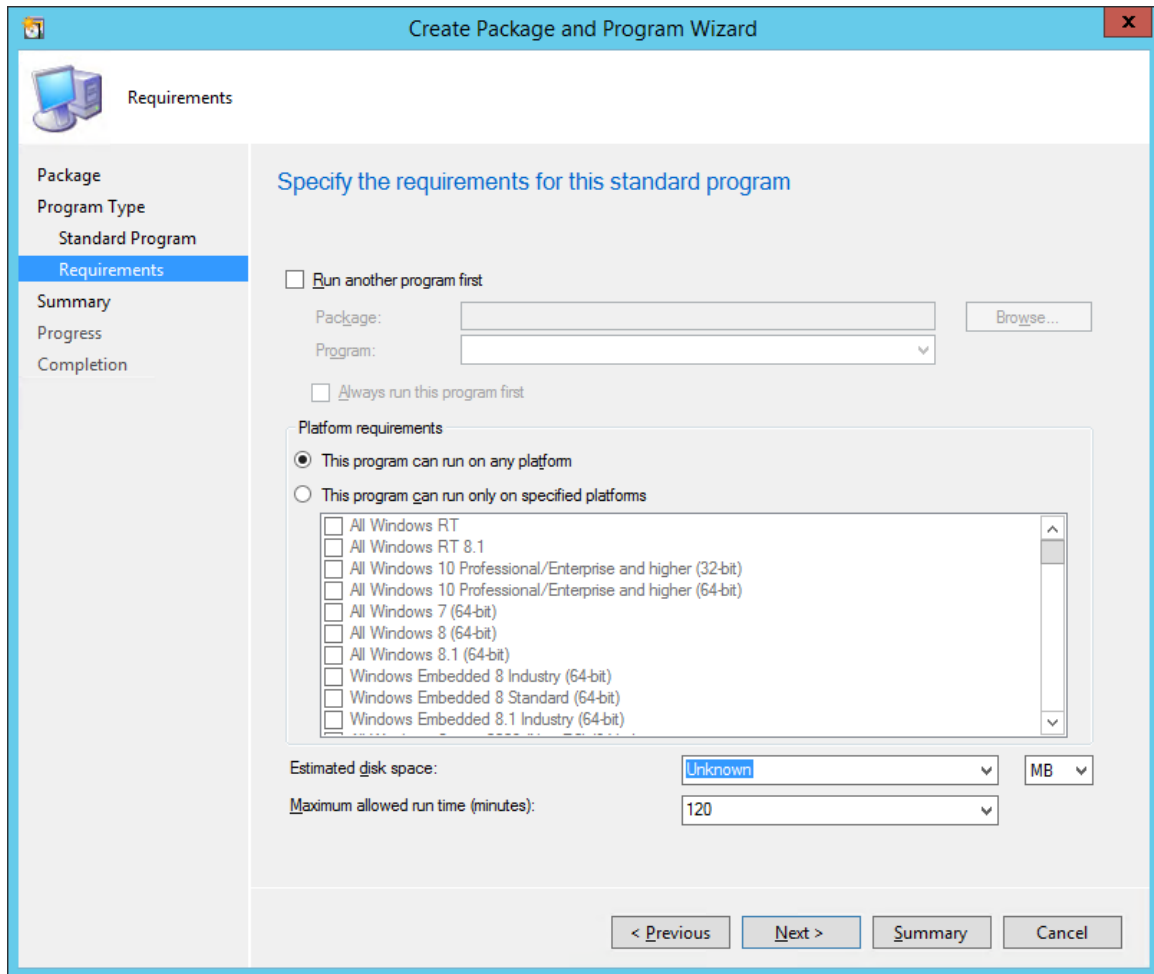
<installation file> /x <password>

Where:

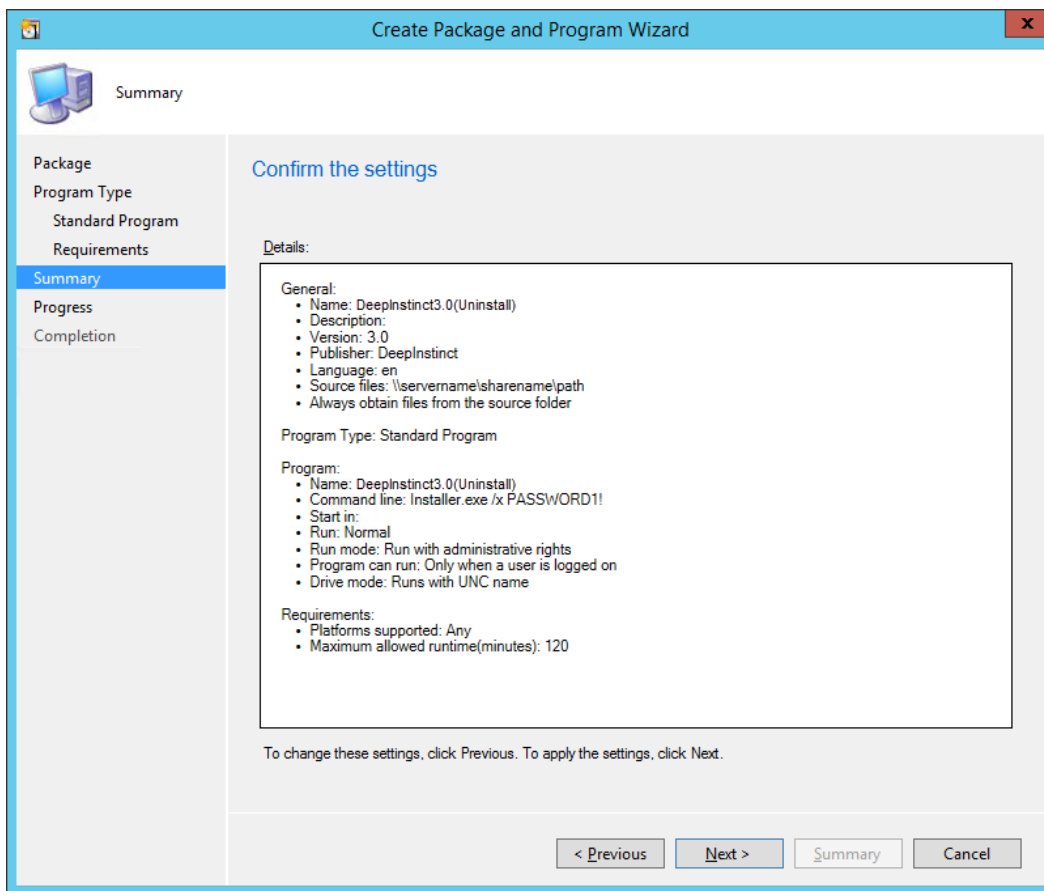
- **<installation file>** = File name for the appropriate installation file. To enter the path and file name, click Browse and select the file from the folder.
- **<password>** = Uninstall password, as defined in the relevant Windows Device policy. If the Windows devices were never in communications 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!`

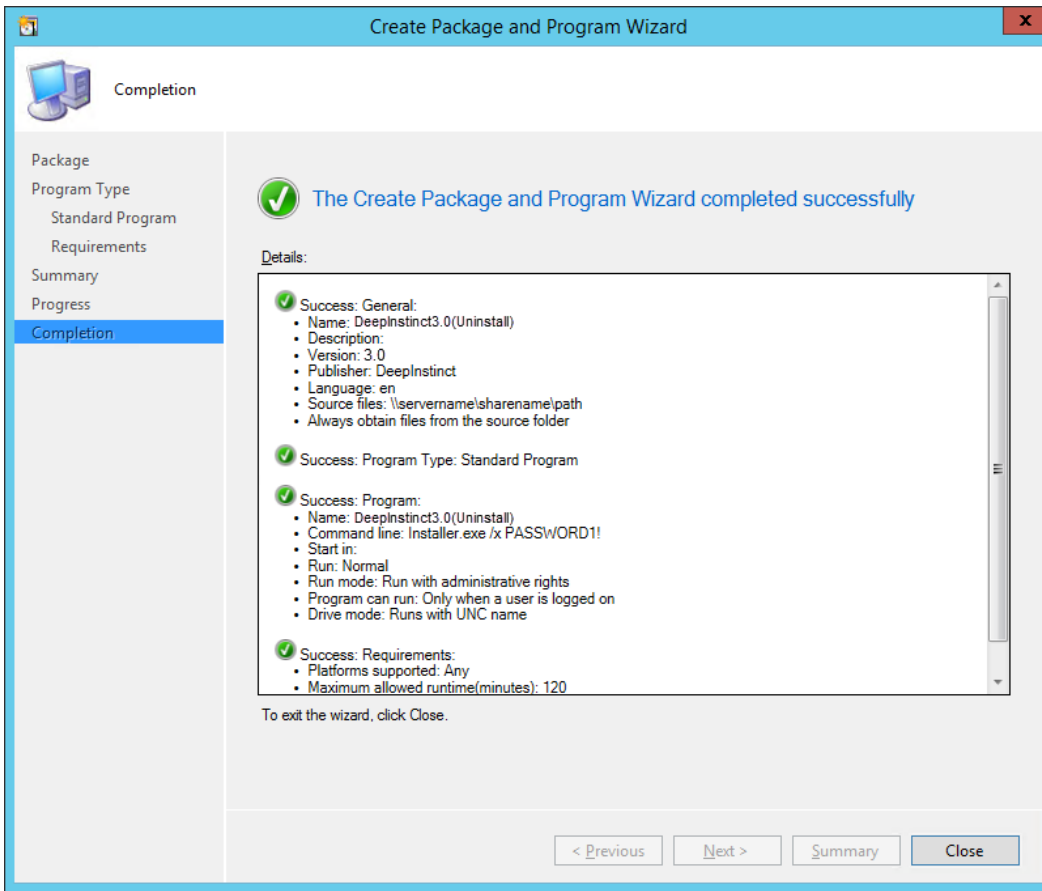
- c. Change Run Mode to **Run with administrative rights** and click **Next**.



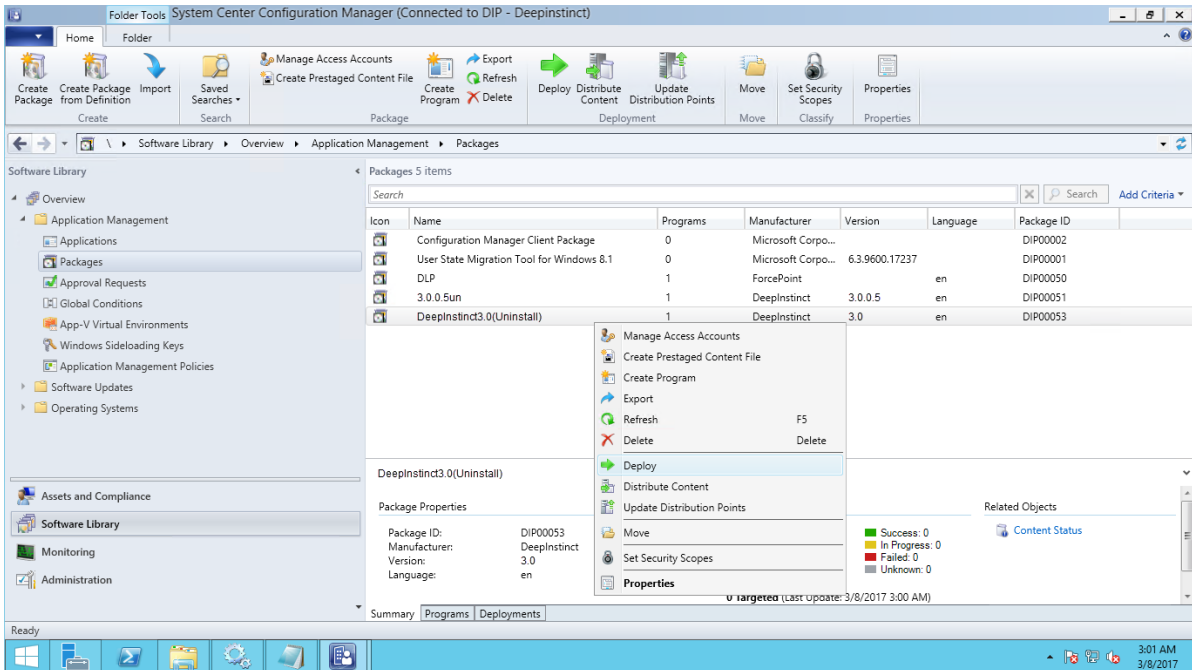
8. Click **Next** and a summary of the package settings are displayed.



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



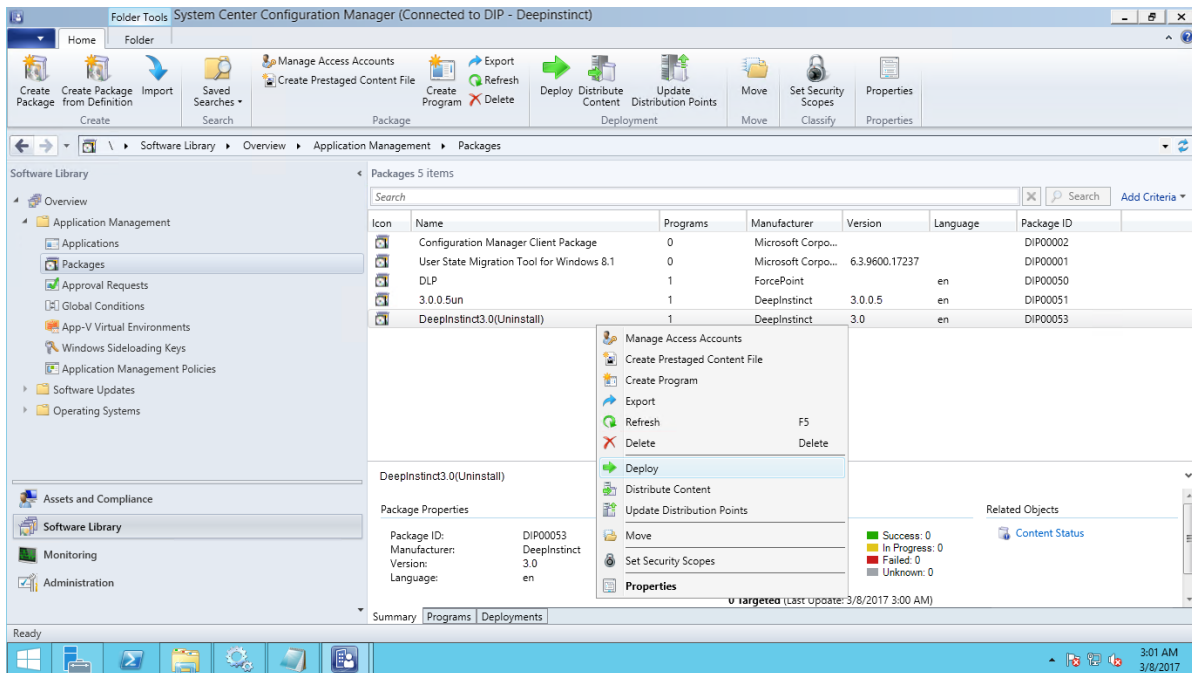
10. Click **Close** and the Deep Instinct package appears in the list of packages.



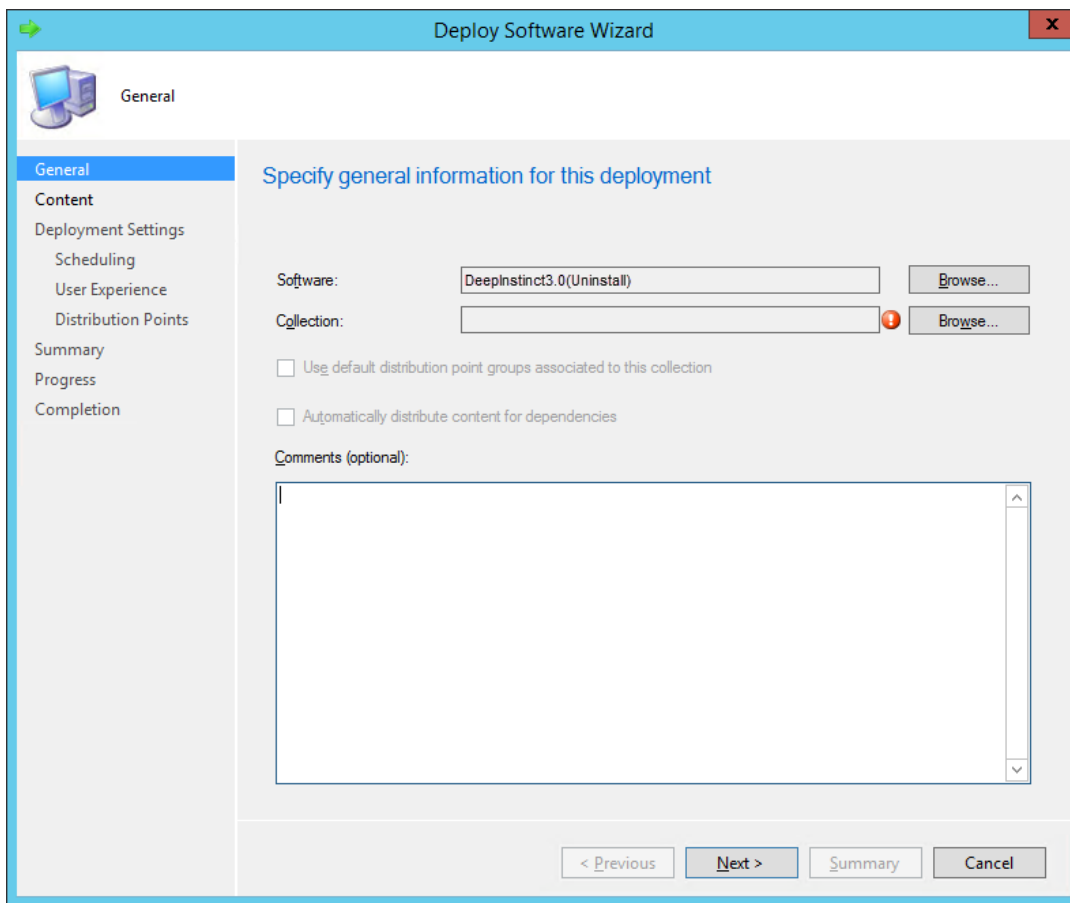
Deploying the D-Client Uninstall Package

To deploy the uninstall package using SCCM:

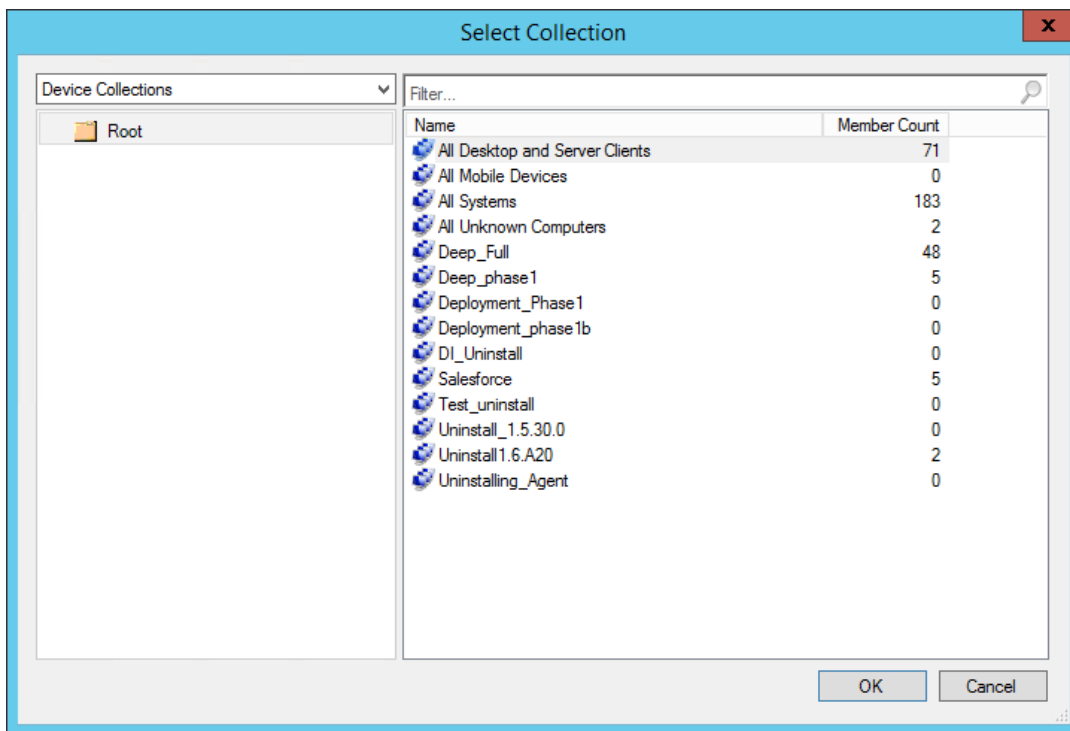
1. Start Microsoft System Center Configuration Manager.
2. In the Configuration Manager console, click [Software Library](#).
3. In the Software Library workspace, expand [Application Management](#).
4. Click [Packages](#) . The Packages list appears.



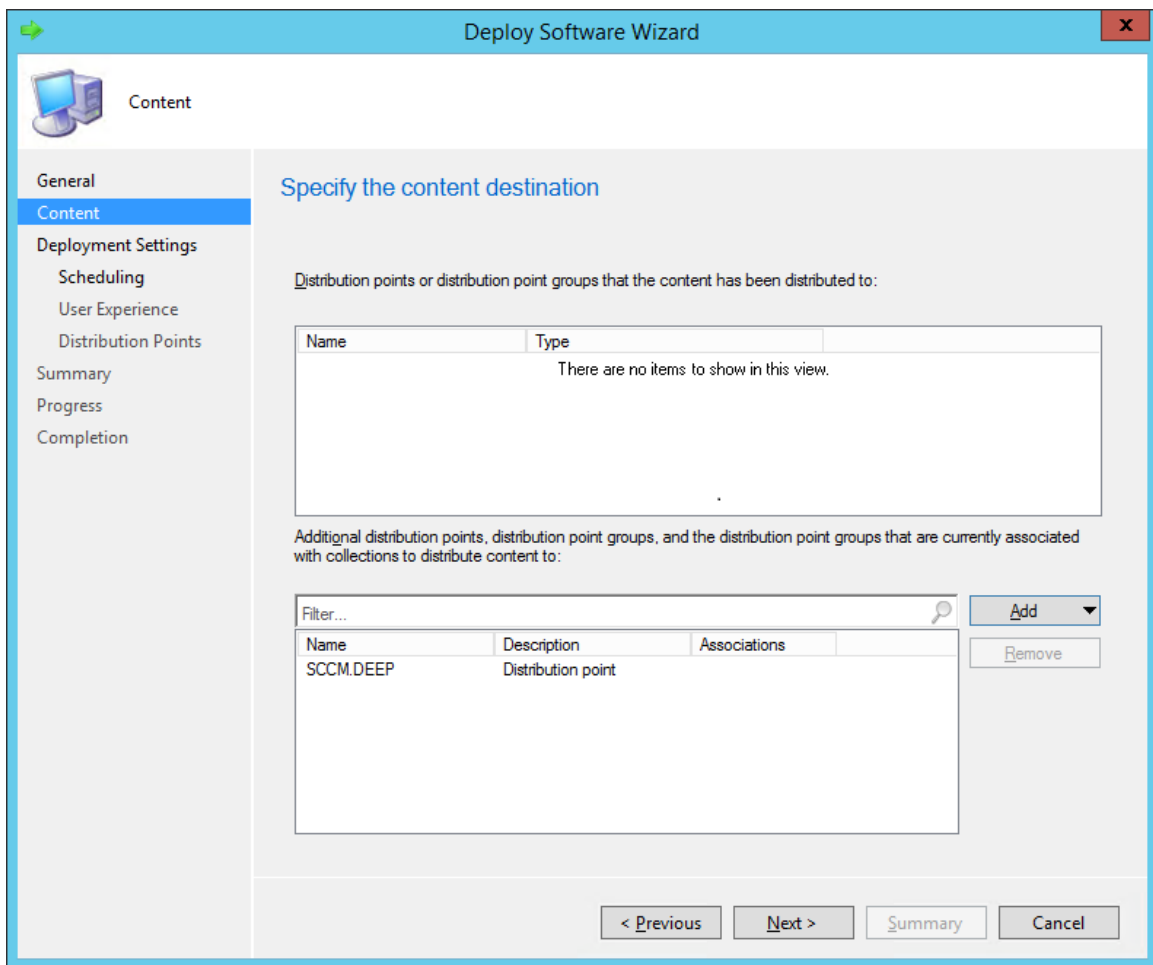
5. Right-click the Deep Instinct uninstall package and click [Deploy](#). The [Deploy Software Wizard](#) opens.



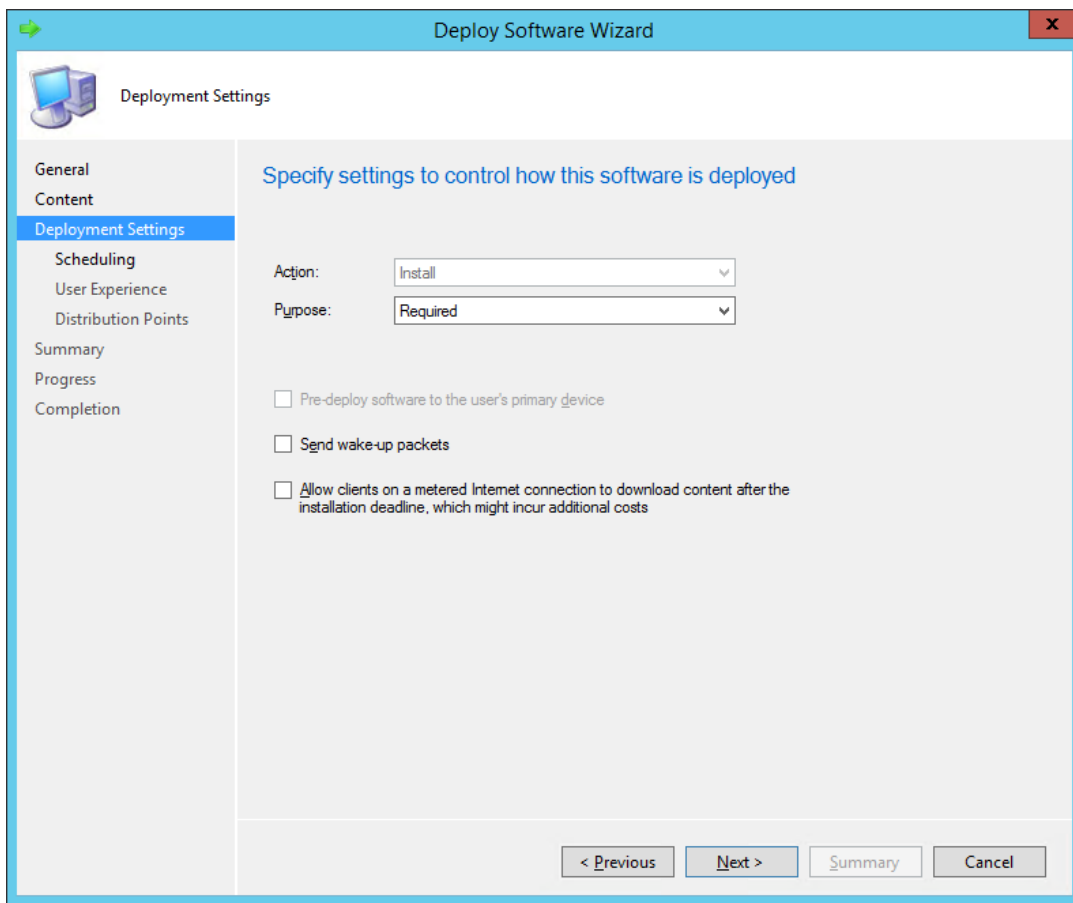
6. Click Browse. Select the Device Collection for uninstalling D-Clients and click OK.



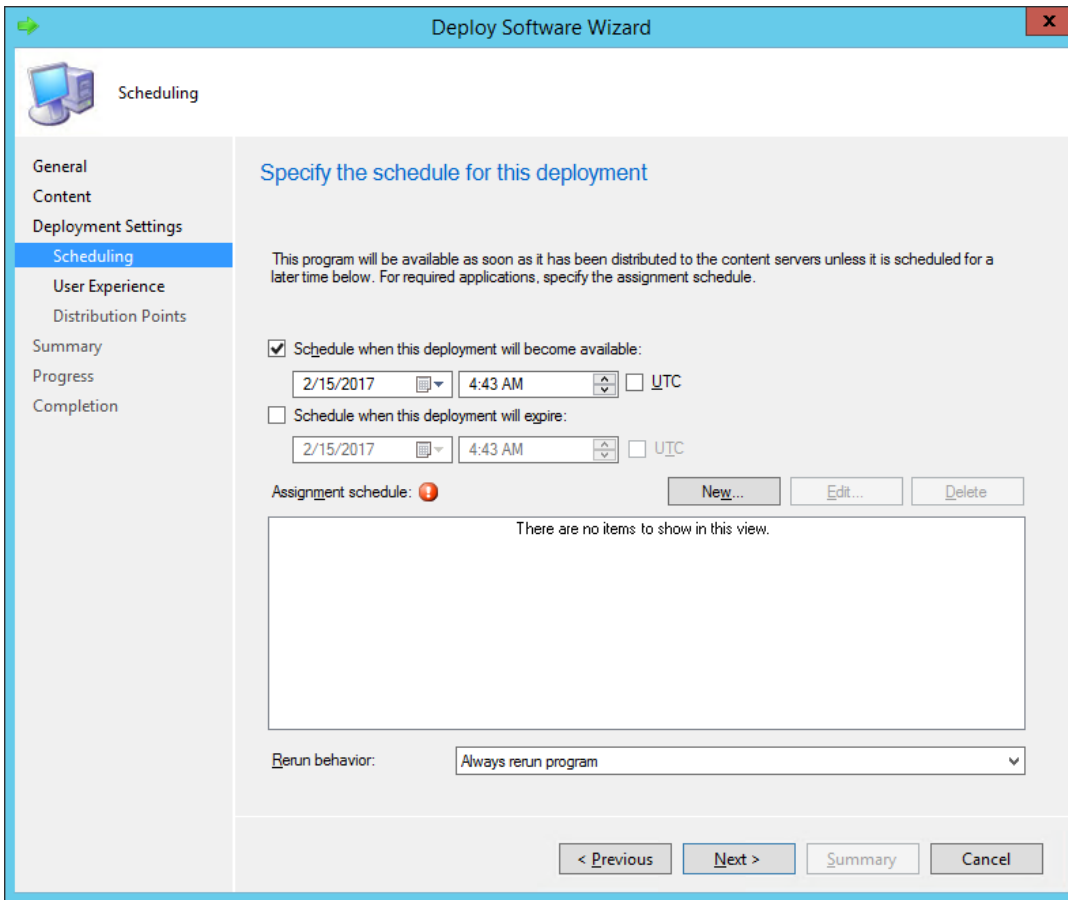
7. Click **Next** and then click Add+Distribution Point and select the distribution points for the content destination. This is typically the SCCM server.



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

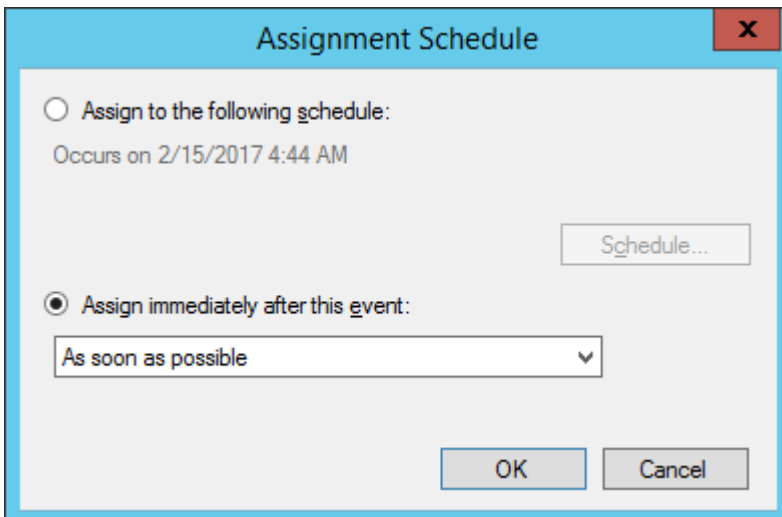


9. Click **Next** and the Scheduling dialog box opens.



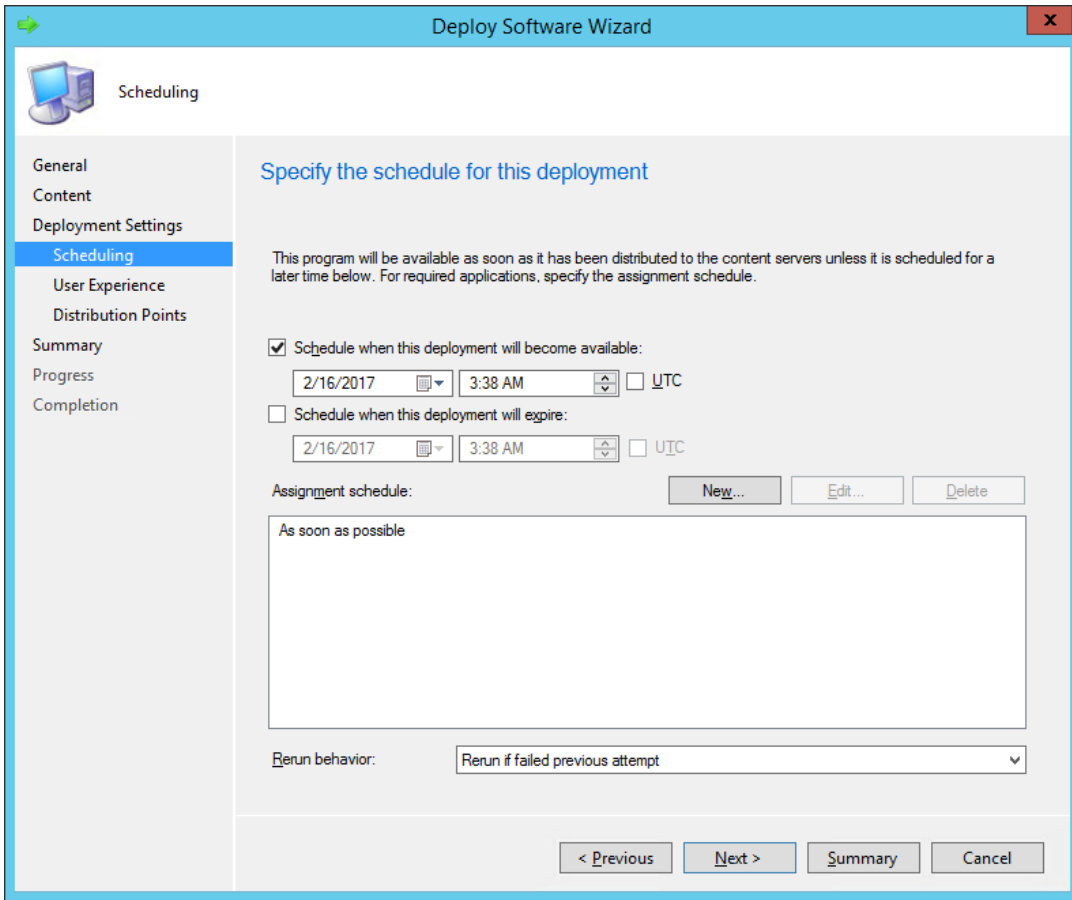
10. Select Schedule when this deployment will become available.

11. Click New and the Assignment Schedule dialog box opens.

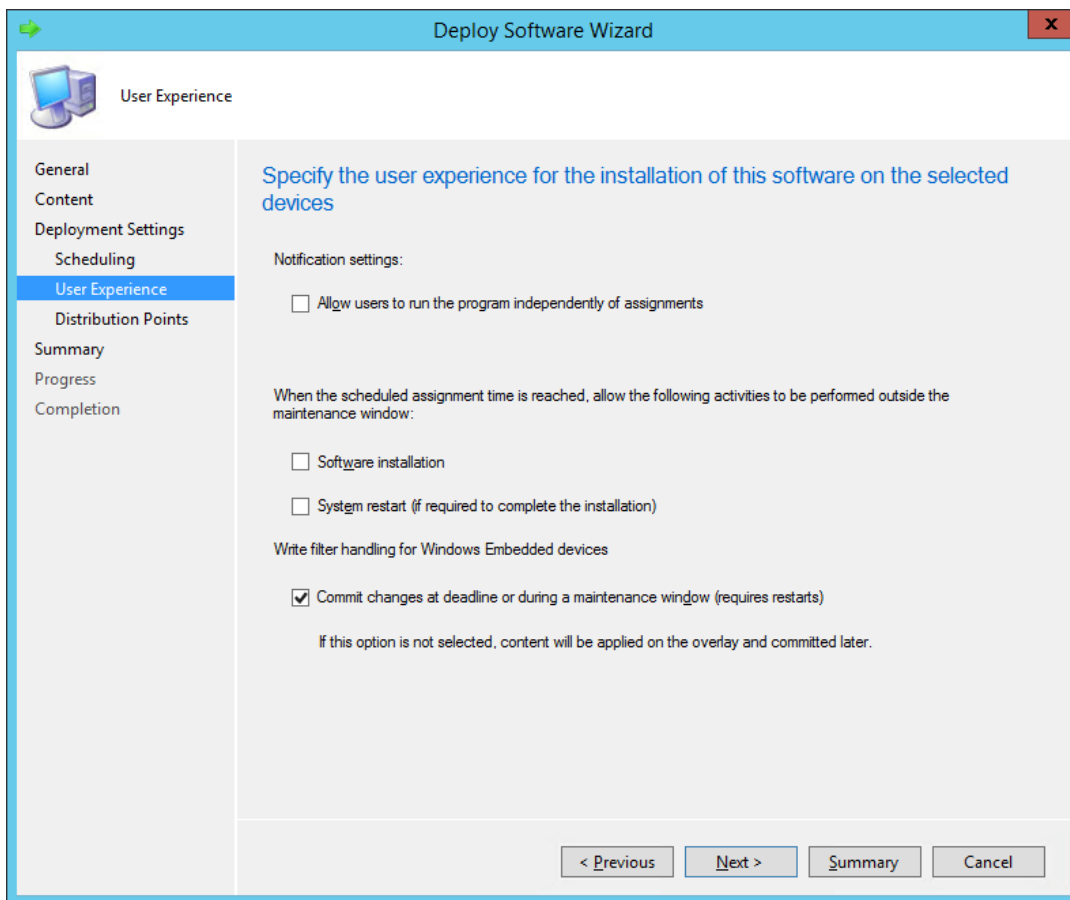


12. Select Assign immediately after this event and select As Soon As Possible from the dropdown box.

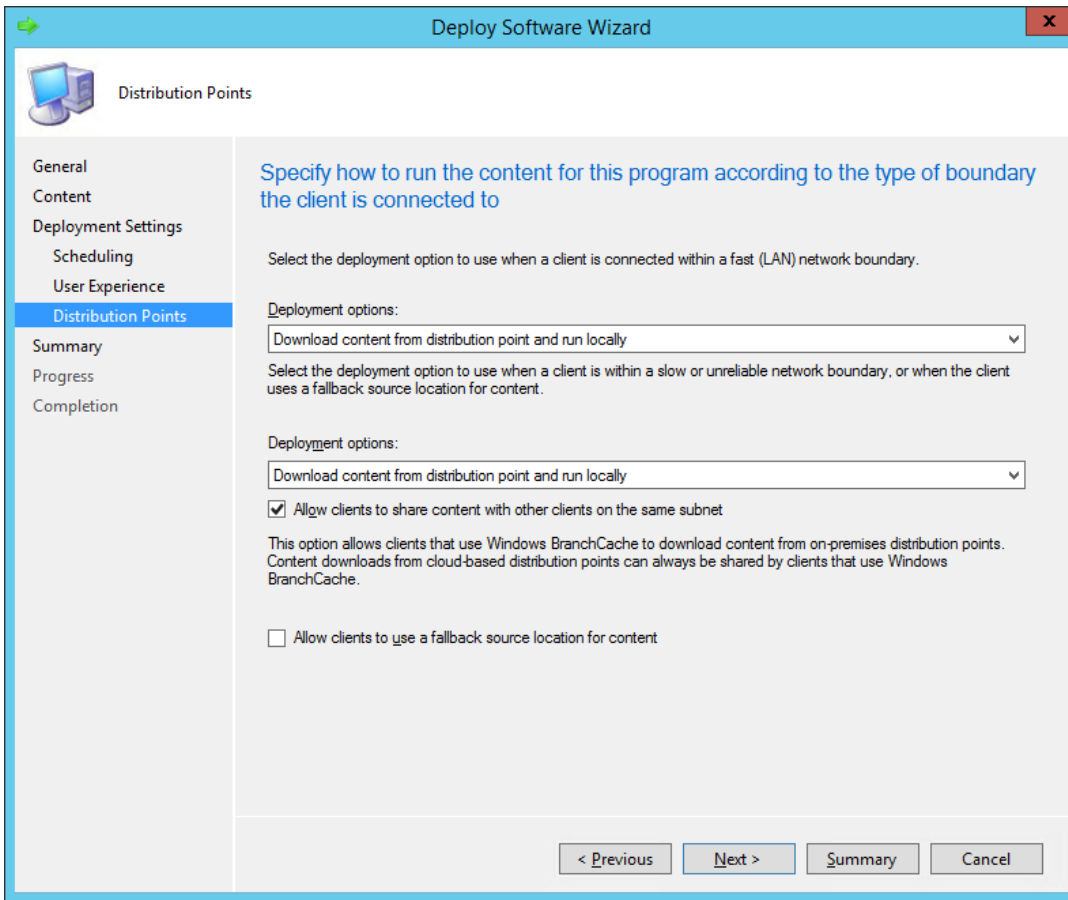
13. Click **OK** and As Soon As Possible is added to the assignment schedule.



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

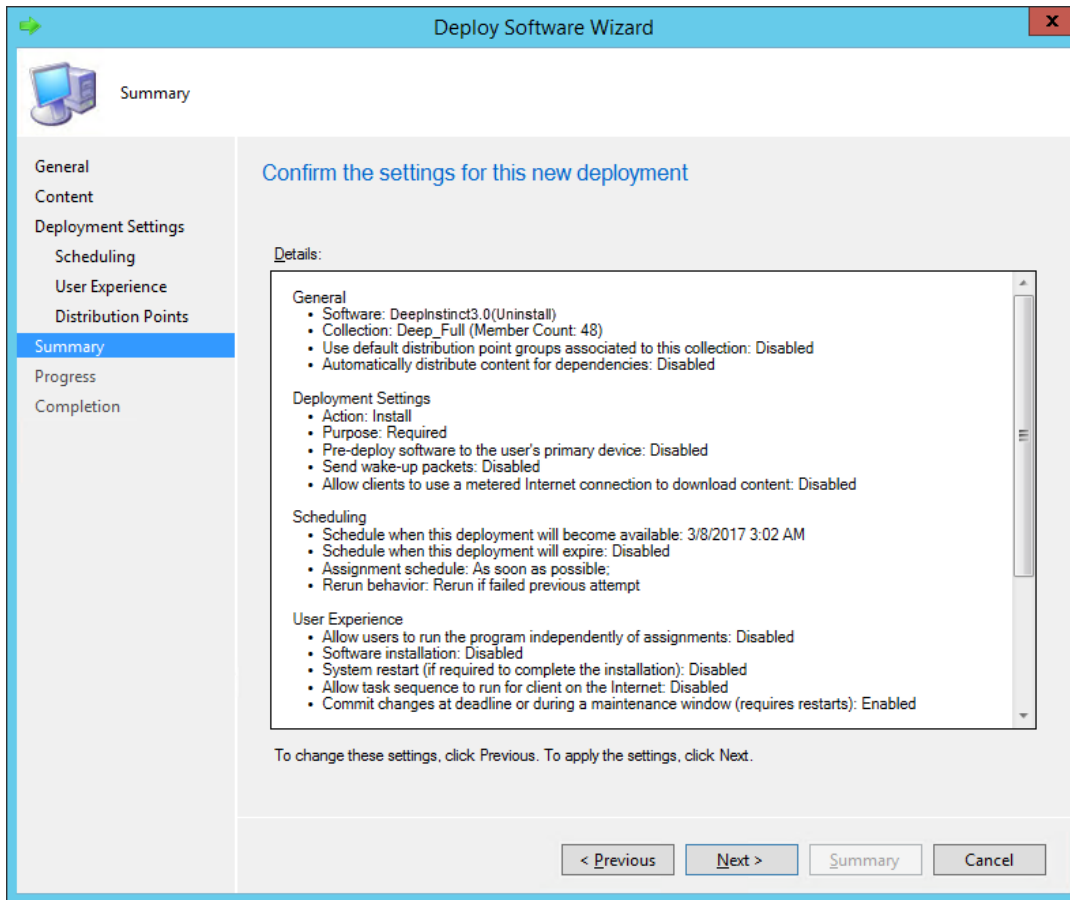


15. Click **Next** and the Distribution Points dialog box opens.

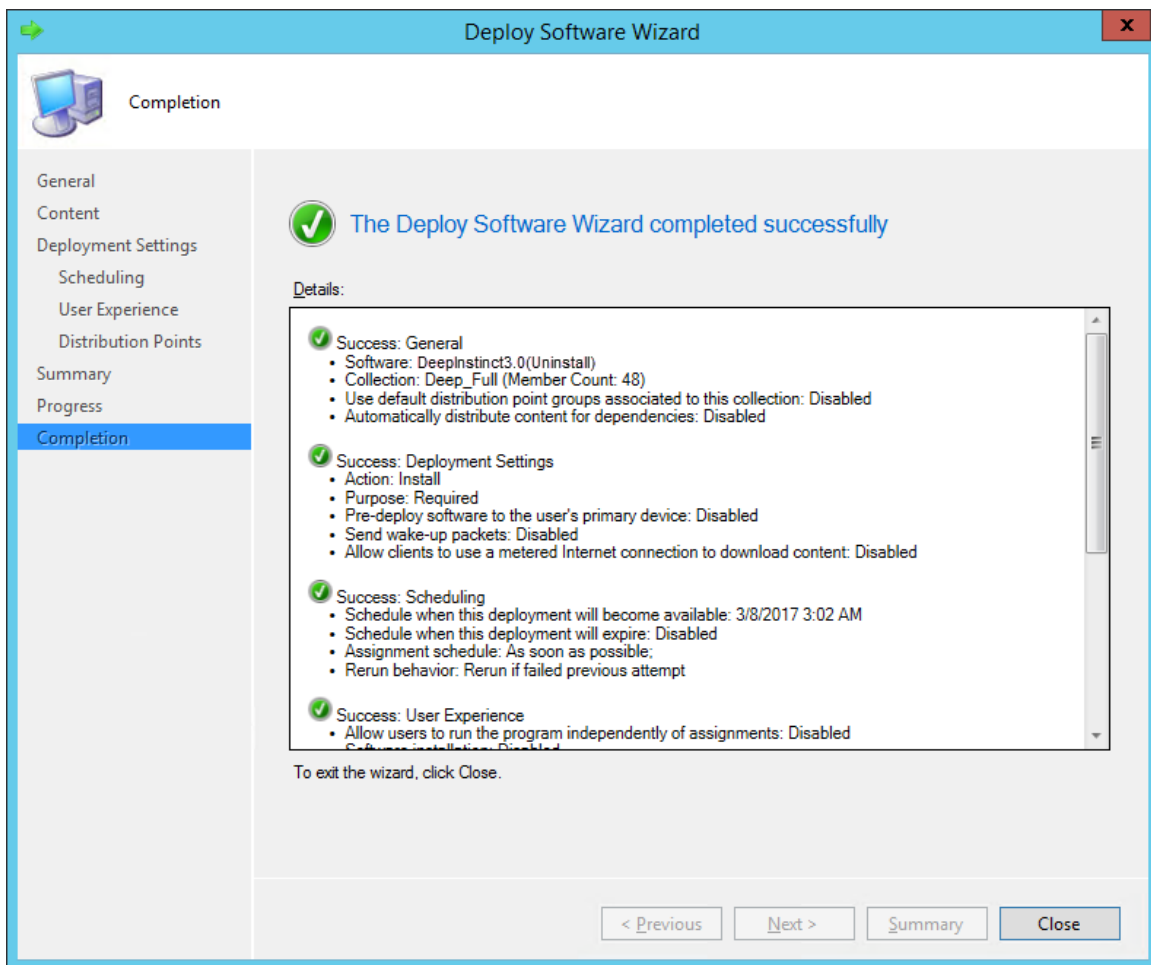


16. In both Deployment options lists, select Download Content From Distribution Point And Run Locally.

17. Click **Next** and a summary of the deployment settings are displayed.



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.

To create the uninstall batch file:

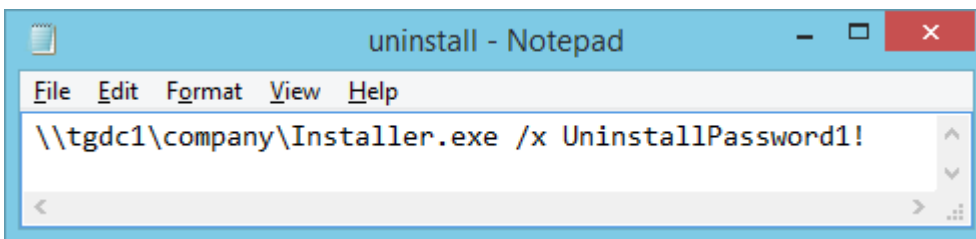
1. Save the installation file to a location where all the Windows devices have access.
2. Open the text editor.
3. Type the following command in the first line of the file:

<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. Command example



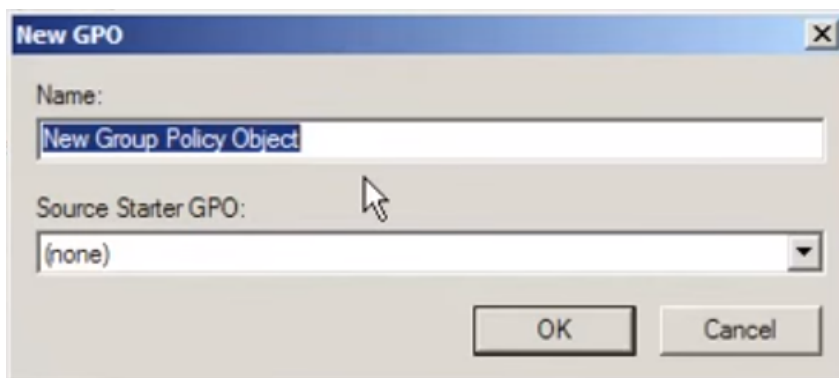
- **exe path** = \\tgc1\company\
- **installation file** = Installer.exe
- **password** = UninstallPassword1!

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.

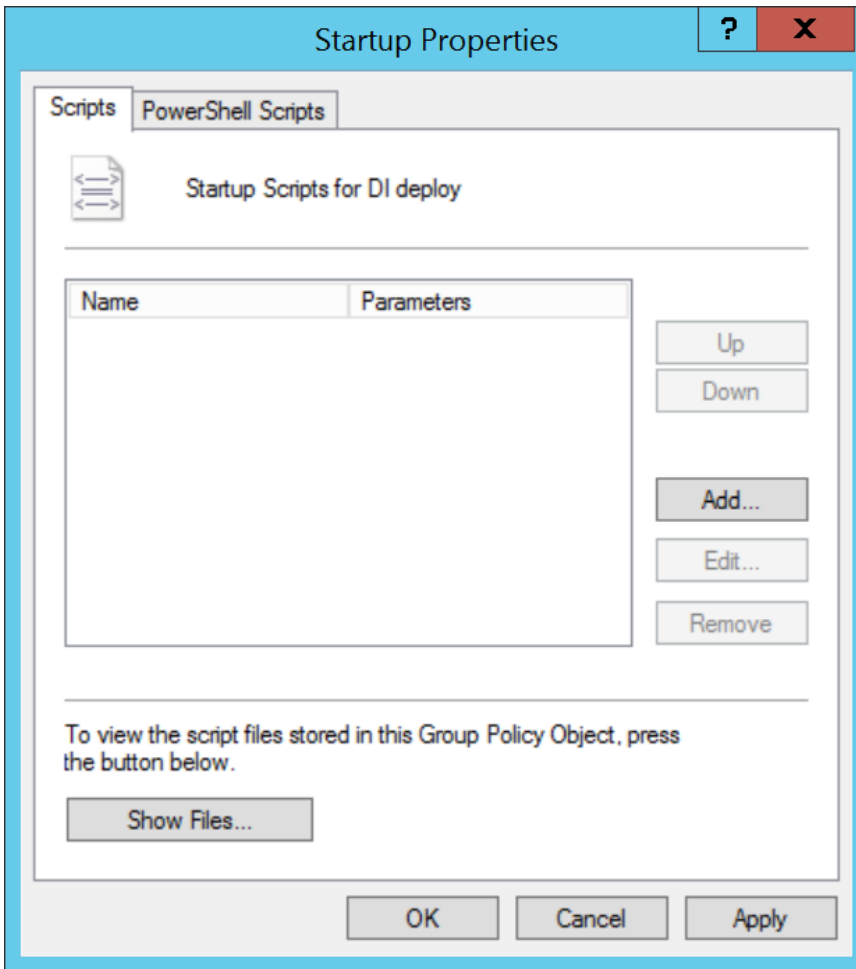
Uninstall D-Clients using GPO

To uninstall D-Clients using GPO:

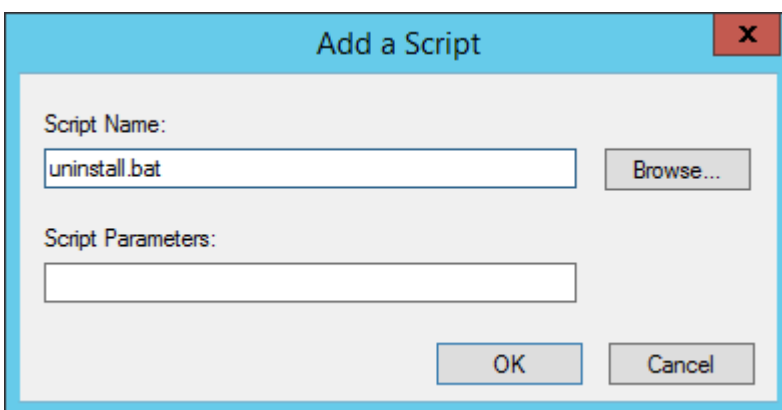
1. Create the uninstall batch file.
2. Save the uninstall batch file to the Startup Script folder.
3. Save the EXE and batch files to a location where all the organization's Windows devices have access.
4. Log on to the Domain Controller (DC) and start the Microsoft Group Policy Management Console (GPMC).
5. 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.



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.



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



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](#).



NOTE

To upgrade macOS D-Clients prior to version 3.4.2, use one 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.



NOTE

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 /xUninstallPassword1!
```

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>	Path for the appropriate installation file	N/C
<installation file>	File name for the appropriate installation file.	To enter the file name, click Browse and select the file from the folder.
<installation token>	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.

Command Parameter	Description	Comments
<tag>	Adds a tag associated with the deployed VDI machines	<ul style="list-style-type: none"> ■ Optional ■ Device Tag must comply to the following: <ul style="list-style-type: none"> ■ Maximum character length = 256 ■ Case sensitive ■ Valid characters: <ul style="list-style-type: none"> ■ 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)

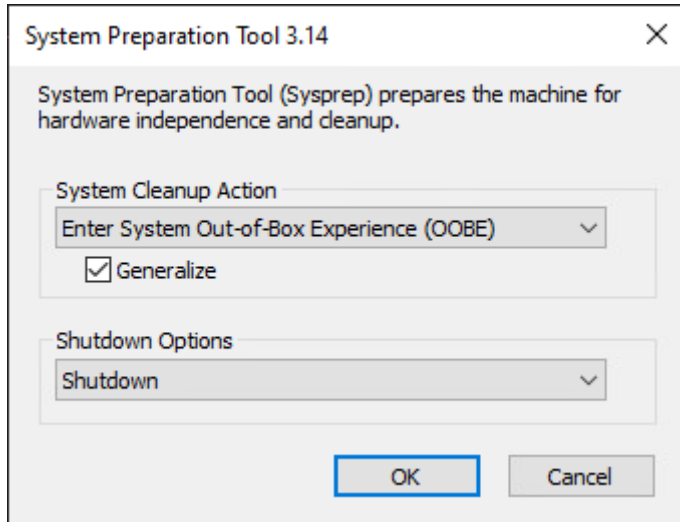
Once the above is completed:

- 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.



- 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.



NOTE

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](#)



IMPORTANT

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> <installation 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\Installer.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.

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>** = Installation path
- **<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
APT	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.
ATA	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 network 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 provides the centralized management and configuration for the Windows operating systems, applications, and users' settings in an Active Directory environment.
Malware	An abbreviation for malicious software, which is any software/application 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 software 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.



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