

Honeywell Advanced Endpoint Security

INSTALLATION GUIDE

- Customer ONBOARDING PROCESS.....2**
 - Tenant Creation.....3
 - Device Policy Creation.....4
 - Device Group Creation.....6

- Installing HAES Agent..... 7**
 - Install HAES agent on a Windows device using CLI..... 7
 - Install HAES agent Using the Installation Screen..... 8

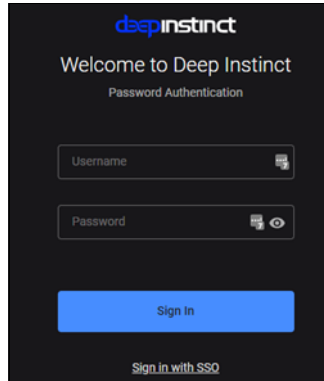
- Uninstalling HAES Agent..... 10**
 - Uninstall HAES agent using the Management C 10
 - Manually Uninstall HAES agent..... 12

- Appendix..... 13**
 - Windows HAES agent CLI Command reference..... 13
 - Network Prerequisites..... 14
 - Troubleshooting reference..... 15
 - Error 1 – Waiting to Validate token..... 15
 - Error 2 – Agent offline..... 15

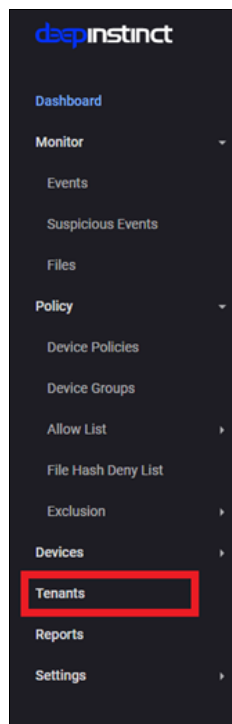
CUSTOMER ONBOARDING PROCESS

The Onboarding process is to help understand how a customer is provisioned into the HAES management portal, followed by the agent installation on endpoints. Please take the time to read and understand all relevant installation, configuration, and operation manuals and ensure that you regularly obtain the latest versions.

1. Login to the HAES Portal page (<https://customername.customers.deepinstinctweb.com/login/>). Two factor authentications must be configured for any accounts.

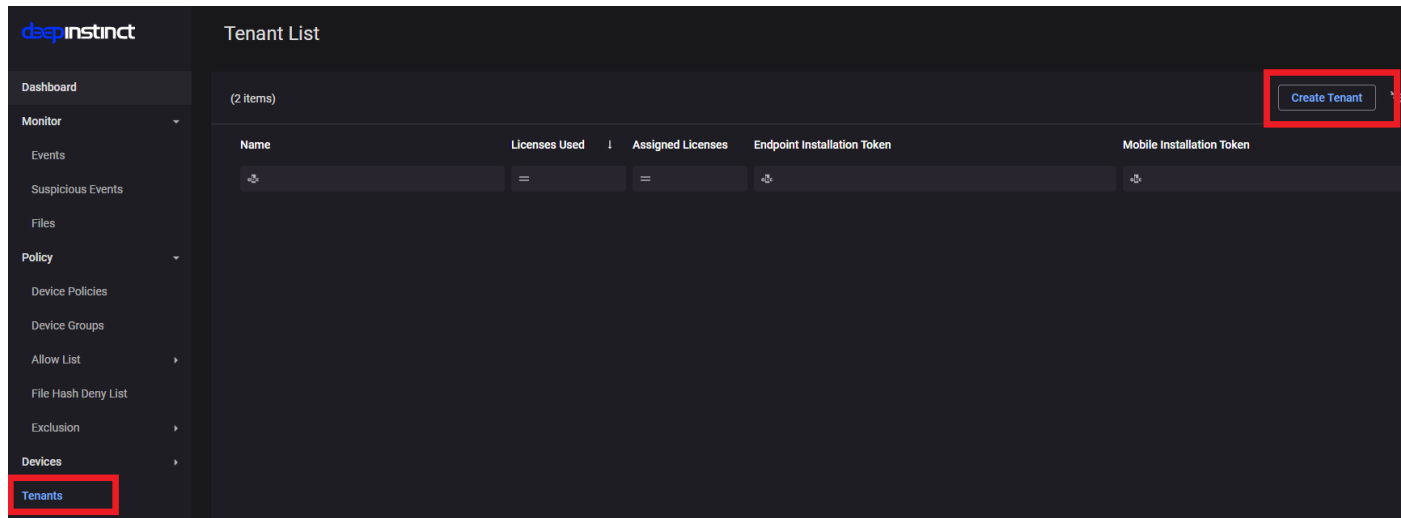


2. Click on the **Tenants** tab to create a new tenant with the customer's name.
A naming standard is recommended to use for customer names Ex: Location_Customername.



Tenant Creation

1. Click on "Create Tenant".



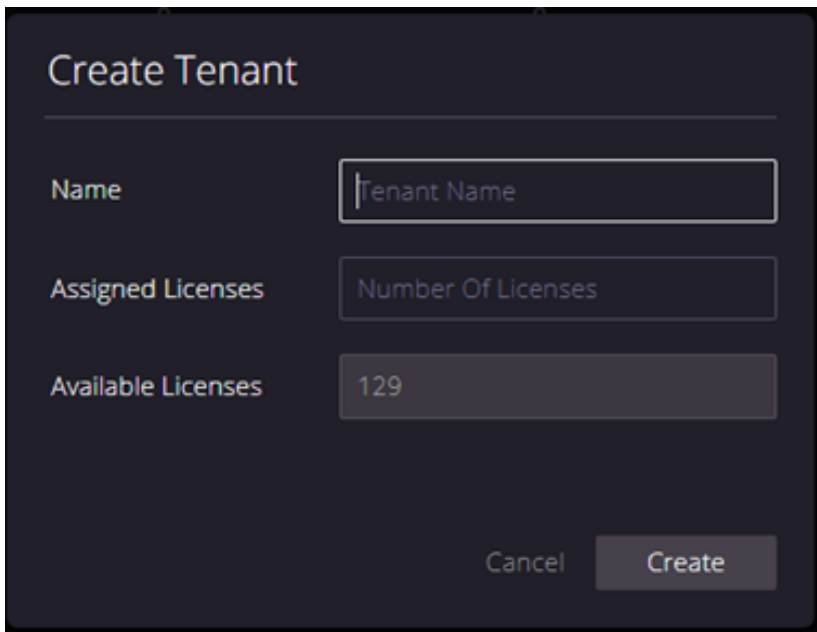
You will be prompted with a new popup window asking Name, Assigned Licenses, and Available Licenses.

Name: Provide a name for customer Ex: NSW - New Airport EBI

Assigned Licenses: Assigned the licenses mentioned on a license issued by the procurement team.

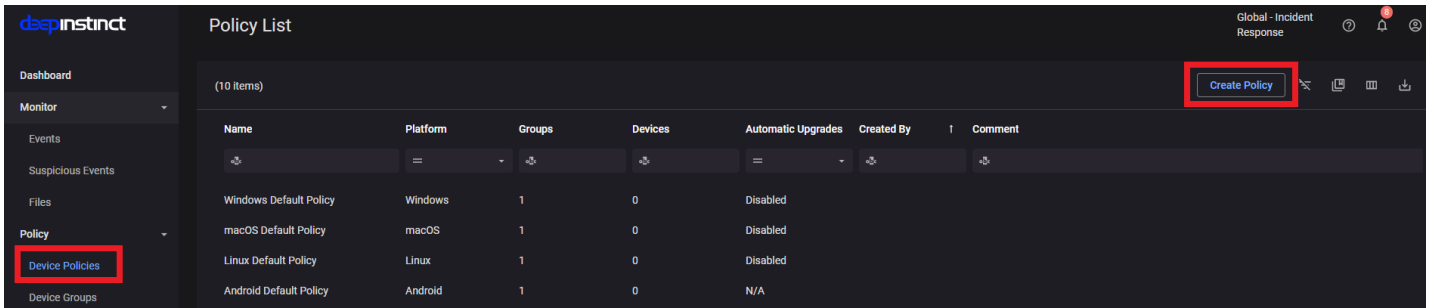
Available Licenses: Total number of available licenses on the console.

2. Click "Create" to save the changes once the above details are updated.



Device Policy Creation

1. Navigate to the **Device Policies** tab to set up a policy for the newly created Tenant by clicking on “**Create Policy**” and filling the details in the pop-up.



Name: Name the policy as same as the name of newly created Tenant in Tenant Creation.

Platform: As required (Windows/Linux)


Based on: #Onboarding Policy Template (Default policy with recommended vendor settings.)

NOTE: #Onboarding Policy Template settings are default and should not be modified without proper Communication/Approval as this directly affects the detection/prevention capabilities.

Deep Static Analysis

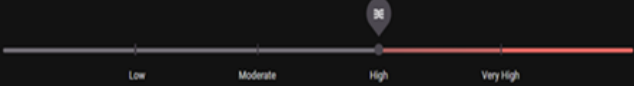
Threat protection settings
Changes on this slider affect actions only on PE files

Detection [Reset to default](#)
Moderate level threats and above generate events.



Low Moderate High Very High

Prevention [Reset to default](#)
High level threats and above are prevented and quarantined.



Low Moderate High Very High

Enable D-Cloud services
File-based reputation services

Known PUA

Prevent
 Detect
 Allow

Scan files accessed from network folders

Behavioral Analysis

Ransomware Behavior

Prevent
 Detect
 Allow

In-Memory Protection

Script Control

Macro execution

Prevent All by Windows
 Deep Static Analysis protection

PowerShell execution

Prevent
 Detect
 Allow

HTML Applications (HTA files) and JavaScript via rundll32 executions

Prevent
 Detect
 Allow

ActiveScript infrastructure

ActiveScript execution (JavaScript & VBScript)

Prevent
 Detect
 Allow

D-Client Control

Upgrade D-Client automatically

D-brain package 115wt

Disable password

Uninstall password

Integrate D-Client with Windows Security Center

Display D-Client user interface (device restart required)

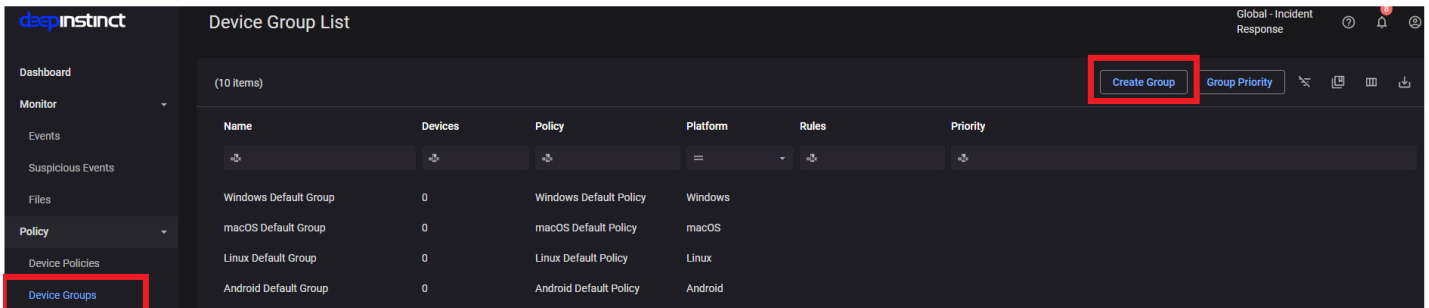
Permitted connections for network isolated devices
No connections

Scheduled Scan

Perform scheduled full scan

Device Group Creation

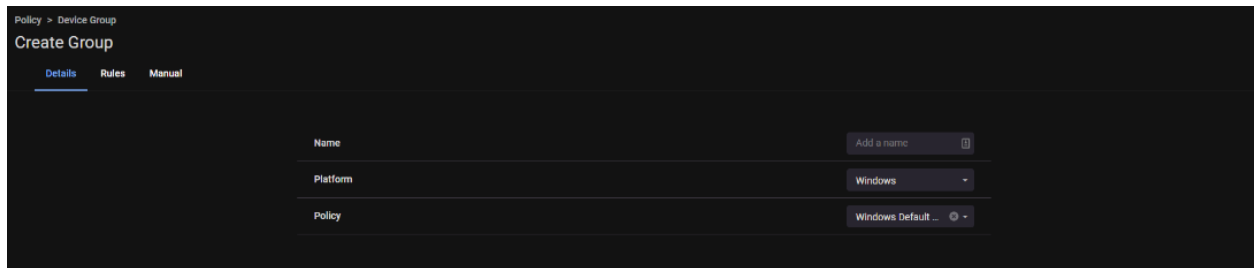
1. Navigate to the **Device Group** tab to create a new device group by clicking **Create Group** and filling in the details as asked in the following window.



Name: Same as Tenant name/Policy name created in Tenant Creation/Device Policy Creation.

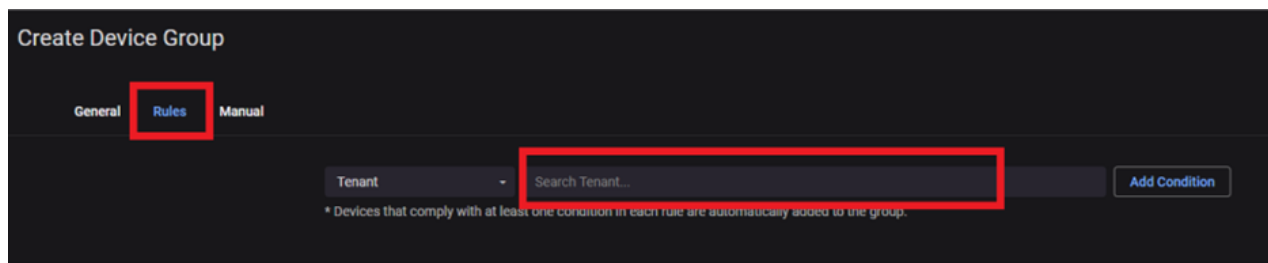
Platform: As required (Windows/Linux)

Policy: Select the policy created for this customer in Step 2.



2. Navigate to **Rules** tab:

Search the tenant name created in Tenant Creation > **Add condition** and click **Save & Apply**.

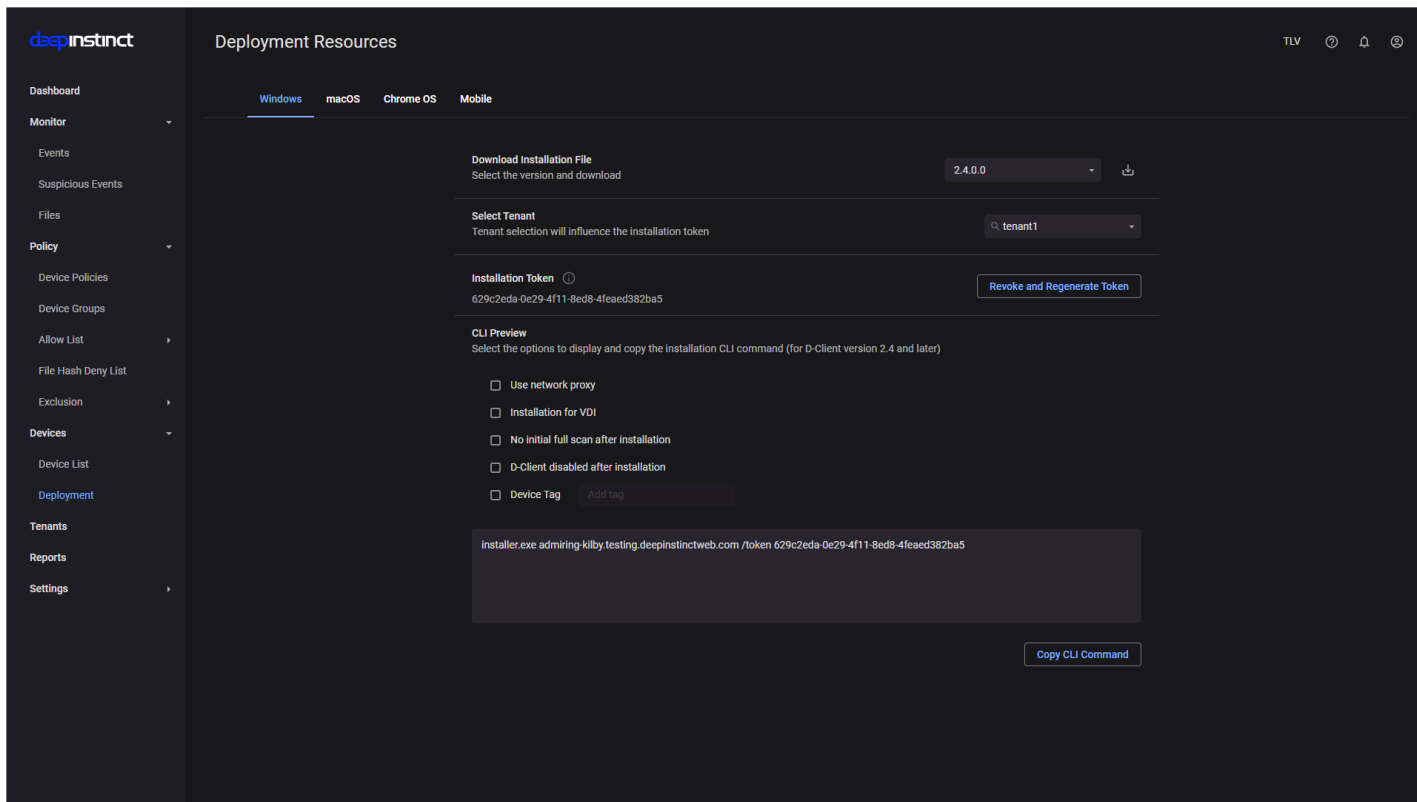


Customer provisioning is now complete. Copy the tenant ID from the **Tenants** tab, which should be used when installing agents at the customer network.

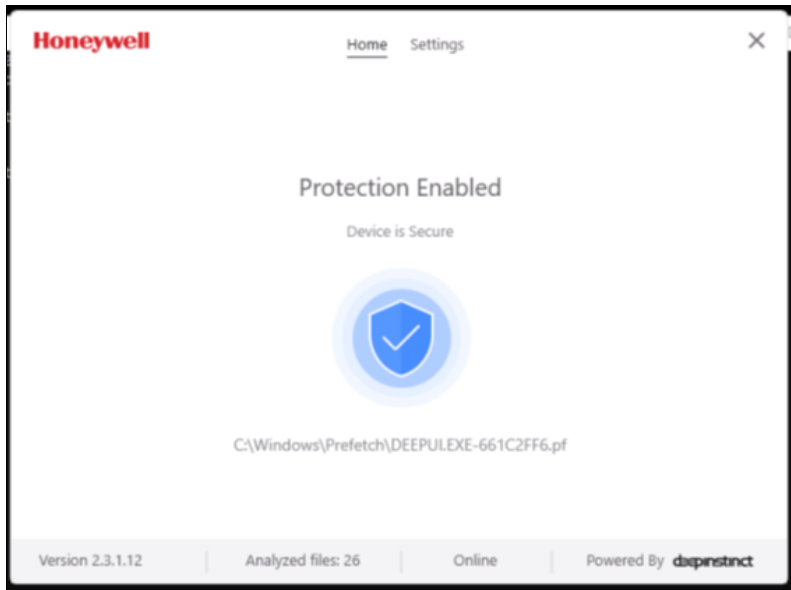
INSTALLING HAES AGENT

Install HAES agent on a Windows device using CLI

1. Download the installation file from the Windows Deployment Resources screen as shown below. The Windows Deployment Resources screen provides the resources and ability to download the Windows HAES agent and preview the required CLI command to install the Windows HAES agent on your devices. To download the Windows HAES agent file:
 - a. Log on to HAES management console.
 - b. From the left pane, click **Devices** > **Deployment** and then click the **Windows** tab.



- c. Select the version of the Windows HAES agent you want to download from the Download Installation File dropdown box.
 - d. Click the Download icon and the installation file will be downloaded.
2. Save the installation file to a location the device to install.
3. Open the Command Prompt as an administrator.
4. At the command prompt, type the CLI command with all required options and values in the command line.
5. 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
 - C:\Windows\system32> c:\users\administrator\downloads\Installer.exe customer.deepinstinctweb.com /token 12345678
6. After installation completes, open the HAES agent UI from the Windows tray icon which should be similar to the below snip as **“online”** and **“Protection Enabled”**.



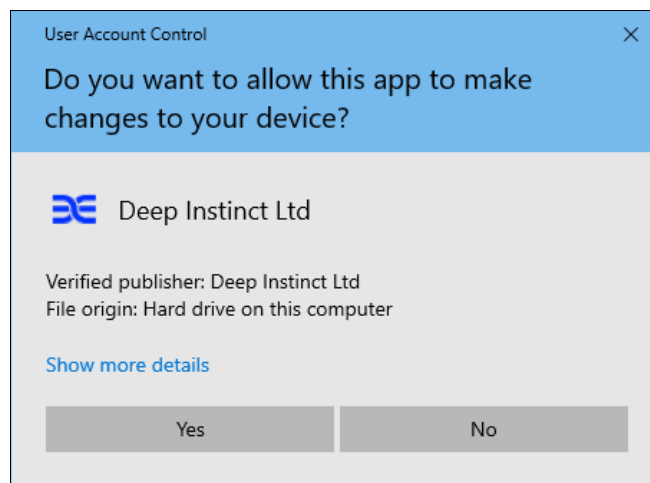
7. For further details on the option in the CLI command, please refer to Appendix.

Install HAES agent Using the Installation Screen

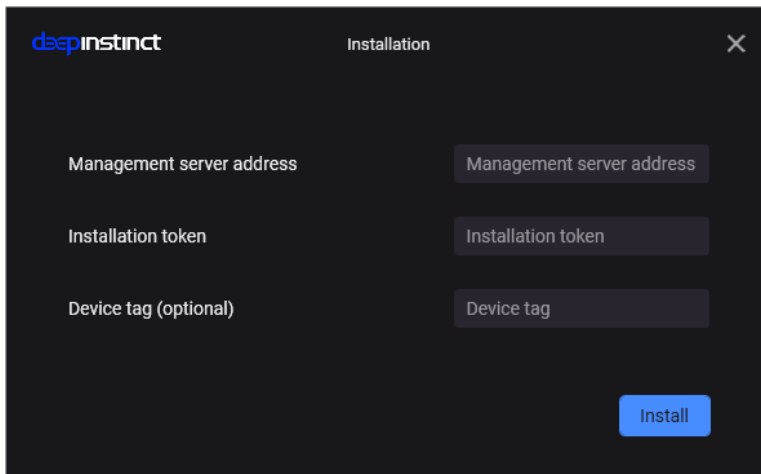
The Agent can also be installed on each Windows device using the Installation screen and then monitored using the Management Console. This may be practical when only a few devices need to be installed or for devices that the Active Directory does not manage.

To install Agent on a Windows device:

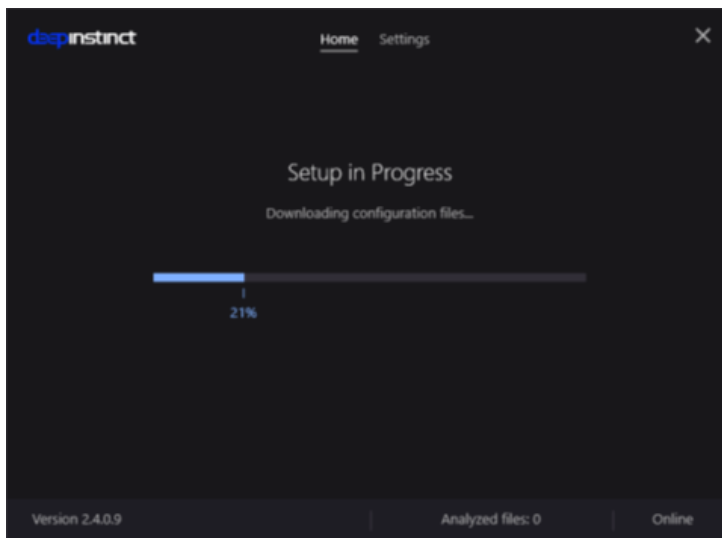
1. Download the installation file from the Windows Deployment Resources screen.
2. Save the installation file to a location where the Windows device has access.
3. Run the installation file. A message appears to confirm.



4. Click **Yes** to open the Agent Installation screen.



5. Enter the FQDN for the **Management server address**.
6. Enter the **Installation token** for the respective customer tenant.
7. As an option, enter a tag associated with the deployed device.
 - Device tags can be used with rules to add devices to a Device Group automatically. It can also be used for selecting and filtering devices in the Management Console.
8. Click **Install** to install the agent.
9. To determine whether the agent installation is in process, look at the agent 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 agent Console by right-clicking the icon and selecting Show Console.



11. When the installation completes successfully, the agent icon changes to a normal state, initiating a full scan.

UNINSTALLING HAES AGENT

When a device is no longer relevant to your organization, the HAES agent may be uninstalled from the device. Once the HAES agent has been uninstalled, the following occurs:

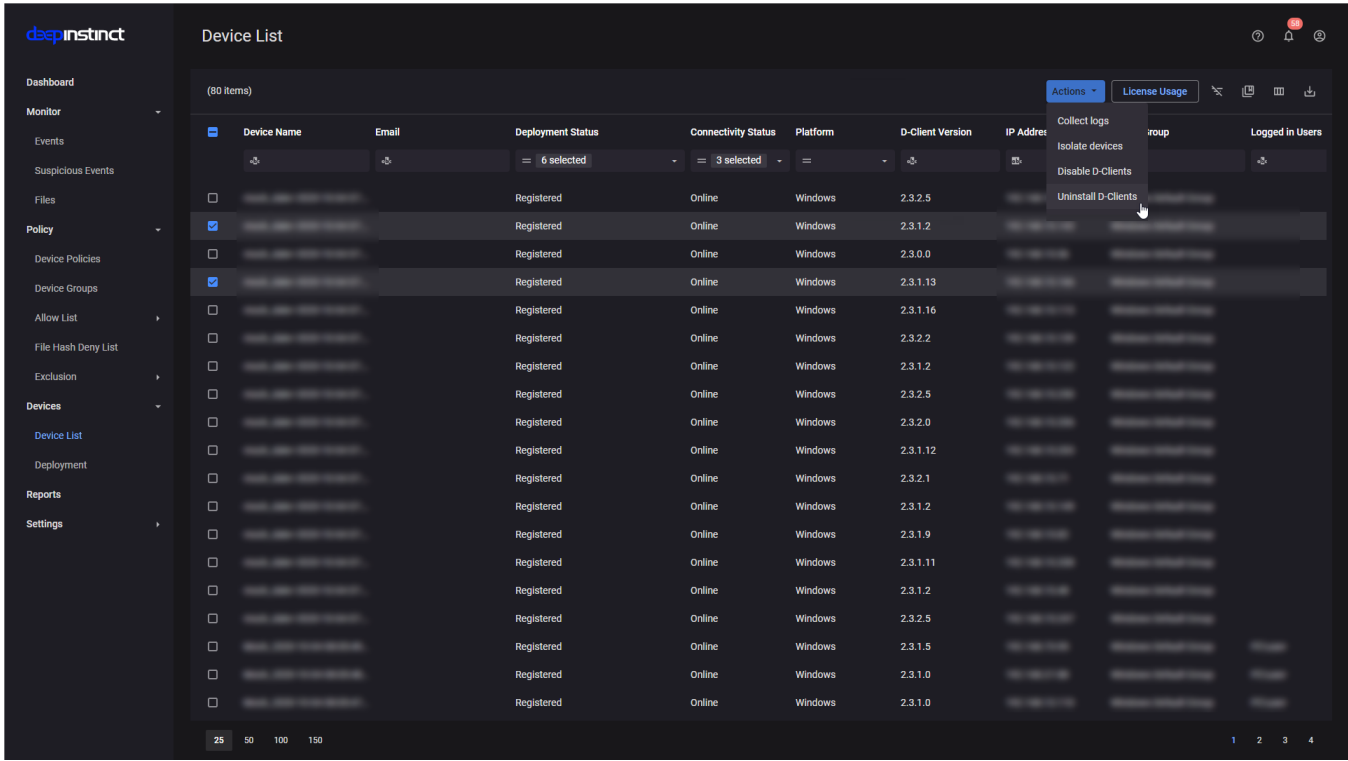
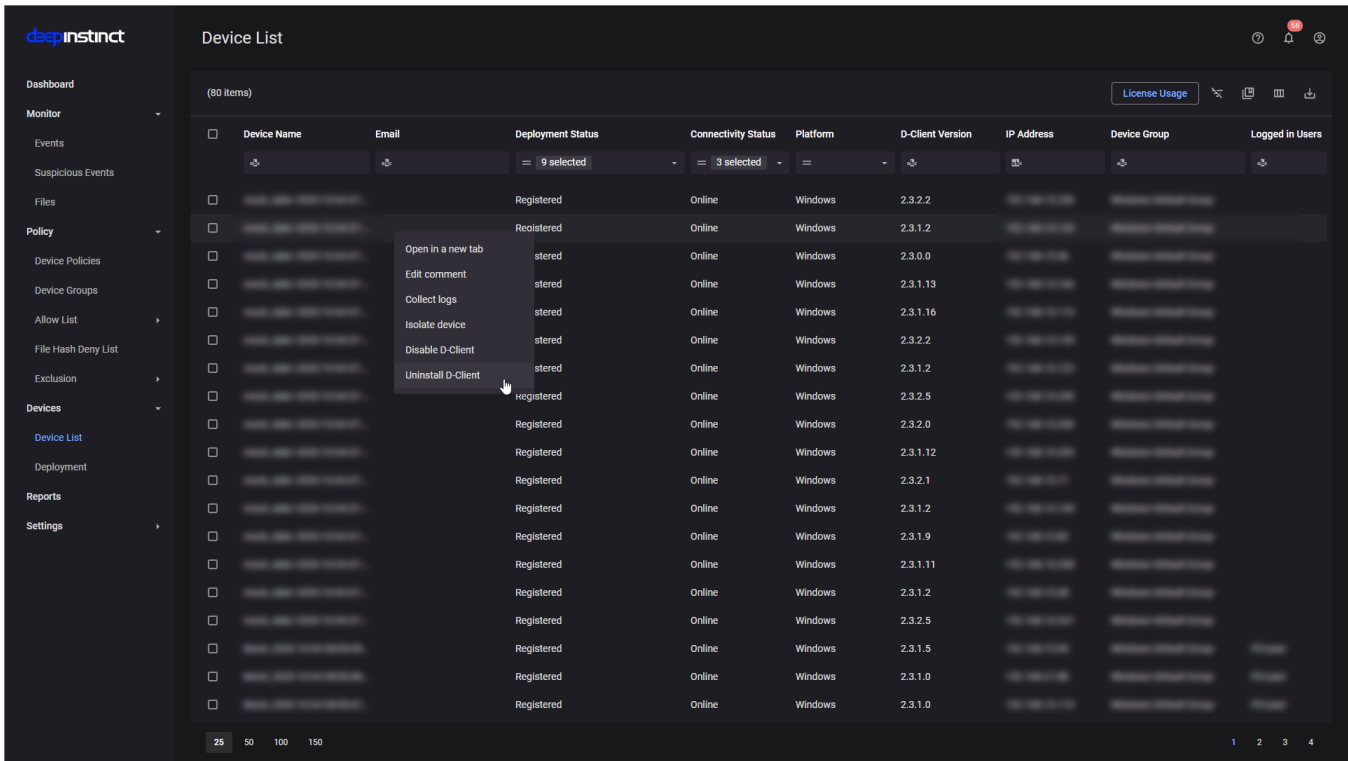
- As the default, uninstalled devices are not displayed in the Device List. However, the Device List can display these devices, by displaying devices with an Uninstalled status.
- The license is released, and the number of used licenses decreases accordingly. This can be viewed from the License Usage screen.

Uninstall HAES agent using the Management Console

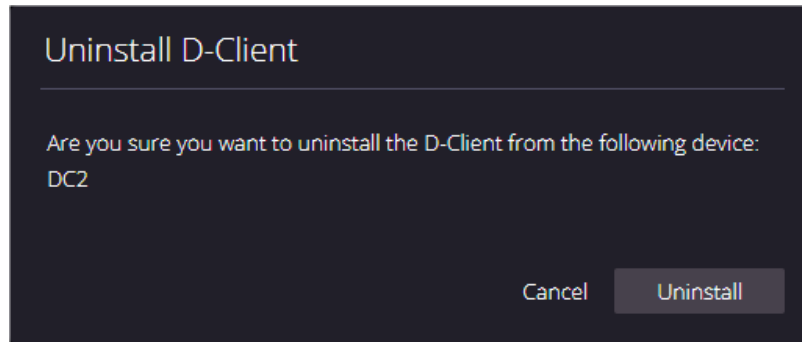
The Management Console includes an Uninstall feature that allows the removal of the HAES agent remotely from any device with which it is currently communicating with the console.

To uninstall the HAES agent from a device, using a single entry:

1. Select **Devices > Device List** from the left pane to open the Device List Or Select multiple by selecting the check-boxes of the entries for the devices. The **Actions** icon appears in the header of the table.



2. Right-click the device from where you want to uninstall the HAES agent and then select Uninstall HAES agent or Click “**Actions**” and select **Uninstall HAES agent**. A dialog box opens to confirm your request.



3. Click **Uninstall** to uninstall the HAES agent. The Deployment Status for the device changes to Pending Uninstall and the device is instructed to uninstall the HAES agent. After the HAES agent has been uninstalled, the status changes to **Uninstalled**.

Manually Uninstall HAES agent

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

To uninstall the HAES agent 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. In the command prompt, type the following command: `<exe path><installation file> /x <password>` Where:
 - exe path – Path for the appropriate installation file.
 - installation file – Filename 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.
4. The following is an example of the commands, where:
 - exe path = c:\users\administrator\downloads\
 - installation file = Installer.exe
 - password = UninstallPassword1!
 - `C:\Windows\system32> c:\users\administrator\downloads\Installer.exe /x 'UninstallPassword1!'`

APPENDIX

Windows HAES agent CLI Command reference

To install the HAES agent 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.

The installation CLI commands are as follows:

For installing HAES agent on a Windows device:

- `<exe path><installation file> <server address> /token <installation token> [/tag <tag>] [/disabled] [/nfs] [/np | /manualproxy <proxy server>:<port>]`

For installing HAES agent on a VDI machine:

- `<exe path><installation file> <server address> /token <installation token> /vdi [/tag <tag>] [/disabled] [/nfs] [/np | /manualproxy <proxy server>:<port>]`

For installing HAES agent on a Windows server with the Cluster Shared Volume (CSV) feature enabled:

- `<exe path><installation file> <server address> /token <installation token> /ignorecsv [/tag <tag>] [/disabled] [/nfs] [/np | /manualproxy <proxy server>:<port>]`

Where:

- **exe path** – Path for the appropriate installation file, where all the Windows devices have access.
- **installation file** – Filename for the appropriate installation file.
- **server address** – FQDN for the D-Appliance.
- **proxy server** – URL for the proxy server, including the scheme.
- **port** – Port number to access the proxy server.
- **installation token** – ID of the installation token, as displayed in the Windows Deployment Resources screen.
- **tag** – This is optional. Adds a tag associated with the deployed devices. Use quotation marks to enter values with spaces or 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` are included, the HAES agent is disabled during the installation. This allows the administrator to select when to initially enable the HAES agent.
- **/nfs** – This is optional. Starts the HAES agent without performing the initial full scan.
- **/np** – This is optional and cannot be used with `/manual proxy`. Enables the use of a network proxy server using the default proxy settings.
- **/manualproxy** – This is optional and only available for HAES agent version 2.5.1 or later. Enables the use of a network proxy server, using the specified settings of the proxy server address and port number. Do not use with `/np`.
- **/vdi** – This is required when installing the HAES agent on a VDI machine. For more information, see HAES agent Installation for Windows VDI.
- **/ignorecsv** – This is required when installing the HAES agent on a Windows server with the Cluster Shared Volume (CSV) feature enabled.



NOTE:

Files accessed from the Cluster Shared Volume are not scanned. However, all files copied to the local drive are scanned.

For example, where:

- 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 is as follows:
 - `c:\users\administrator\downloads\Installer.exe customer.deepinstinctweb.com /token 12345678`

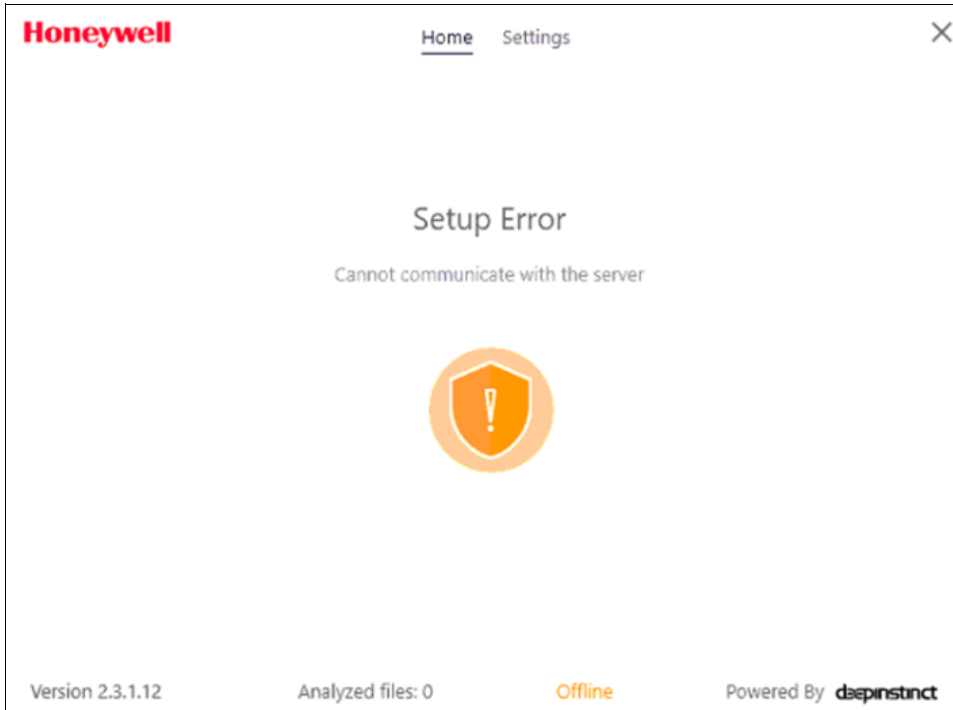
Network Prerequisites

An agent may show offline when it is unable to communicate with the HAES management console as shown below image. The instructions mentioned below can help troubleshoot and fix this issue.

- Make sure that the required firewall rules are enabled to allow necessary connections from the agent to the HAES management console.

Table 1 Ports Detail

Ports	Description	Source	Destination
443	Used for D-Cloud services. The address for the D-Cloud is cloud-api.deepinstinctweb.com.	HAES Agent	D-Cloud (cloud-api.deepinstinctweb.com)
443 4339	D-Client access to download the prediction model, policy, and send events. <ul style="list-style-type: none"> • At installation, the agent set the port to 443, if available. If not, the port is set to 4339. • When port 443 is used, the connectivity needs to open to both the console FQDN, and to “apiv2-<FQDN>”. • Once the port is set during installation, the D-Clients continue to use this port, including upgrades. 	HAES Agent	HAES Console FQDN examples for the console: <ul style="list-style-type: none"> • mycompany.customers.deepinstinctweb.com • apiv2-mycompany.customers.deepinstinctweb.com (“apiv2-<FQDN>”.)



Troubleshooting reference

Error 1 – Waiting to Validate token

After installation, if the agent status is offline and shows an error message “waiting to validate token”, follow the below steps:

- Make sure that the required network ports are allowed from the agent to the management console.
- Open command prompt and run the command “<exe path><installation file> /m <uninstall password> <server address> /token <installation token>”
 - This will try to reinitiate the communication before the timeout occurs.
 - Verify if the agent starts communication and shows online.

Error 2 – Agent offline

There are some certificates required for the agent to start communicating with the console. These certificates anyhow are embedded into Windows security updates. The issue may occur where the endpoints are not patched for long and the certificates are missing.

Follow the below procedure to install the certificates

- Copy the roots.sst file and agent installer file (same version as installed on the endpoint) files into C:\



roots.sst

- Open powershell on the endpoint as admin and run below commands:
 - Cd c:\
 - \$sstStore = (Get-ChildItem -Path C:\roots.sst)
 - \$sstStore | Import-Certificate -CertStoreLocation Cert:\LocalMachine\Root
- Run “<exe path><installation file> /m <uninstall password> <server address> /token <installation token>”
- The agent should start communicating and shows “Online” state and “Protection enabled.”
- If doesn't work then uninstall the agent with “<exe path><installation file> /x <uninstall password>”, this will need a restart of the endpoint.
- Re-install the HAES agent.

The material in this document is for information purposes only. The content and the product described are subject to change without notice. Honeywell makes no representations or warranties with respect to this document. In no event shall Honeywell be liable for technical or editorial omissions or mistakes in this document, nor shall it be liable for any damages, direct or incidental, arising out of or related to the use of this document. No part of this document may be reproduced in any form or by any means without prior written permission from Honeywell.

Honeywell Building Technologies

715 Peachtree St NE
Atlanta, Georgia 30308
customer.honeywell.com
buildings.honeywell.com

® U.S. Registered Trademark
©2022 Honeywell International Inc.
31-00540-01I Rev. 04-22

Honeywell