Forcepoint

Forcepoint Data Classification

Powered by Getvisibility

Agent Deployment Flow

Forcepoint

Report

forcepoint.com

Forcepoint
15 July, 2024
Forcepoint Proprietary

Table of Contents

© 2024 Forcepoint

Bundles Distribution

The agent uses the same distribution flow as ML model deployments.

In the current implementation a bundle must be assigned to a cluster as there is no default bundle available which could be reused for all deployments.

Contact support.forcepoint.com for help with bundle deployment.

The deployed bundles are essential for two key functionalities:

- → **Dashboard**: The bundles are utilized by the Dashboard to populate the Download page, enabling users to access and download the available versions.
- → **Agent**: The bundles also support the AutoUpdate functionality of the agent, ensuring that it can automatically update itself to the latest version when available.

Deployment flow:

- → Once a new bundle is deployed, the requested agent artifacts are copied into a **MINIO** bucket on the customer's cluster.
- → Subsequently, the pod named `static-server` (a Nginx server) is restarted. Upon startup, this pod copies the artifacts from the **MINIO** bucket to `/var/static/agent/(stable|beta)`.
- → From this point, the artifacts can be accessed via the following URLs:
- → `https://{cluster}/static-server/static/agent/stable/` - for default stable deployment
- → `https://{cluster}/static-server/static/agent/beta/` - for optional beta deployment
- → The previous pods `auto-update-server` and `synergy-server` are deprecated.

Contact support.forcepoint.com for details about this.

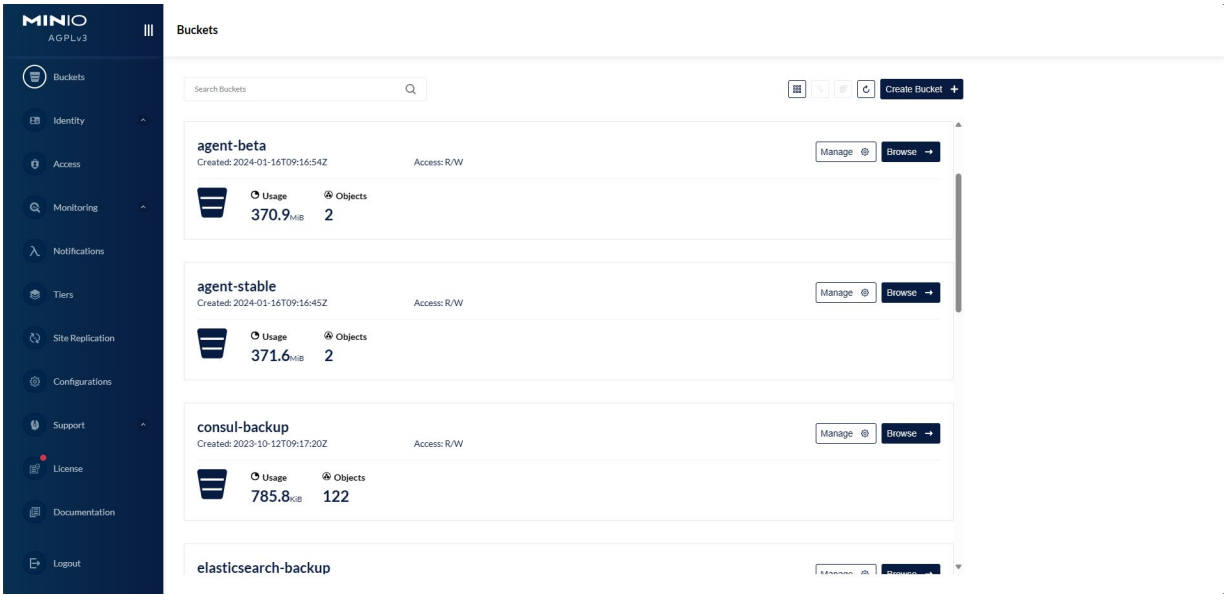

figure 1.

The agent supports two types of artifact distributions:

→ **Stable**: This is the default distribution method for artifacts.

→ **Beta** (**for agent version 4.1.0 and above**): This method is for optional beta distribution. The process for deploying beta artifacts is detailed further down on this page.

Agent Download Page
The dashboard dynamically generates a download page for the available versions of artifacts—either stable or beta—based on the deployed bundles.

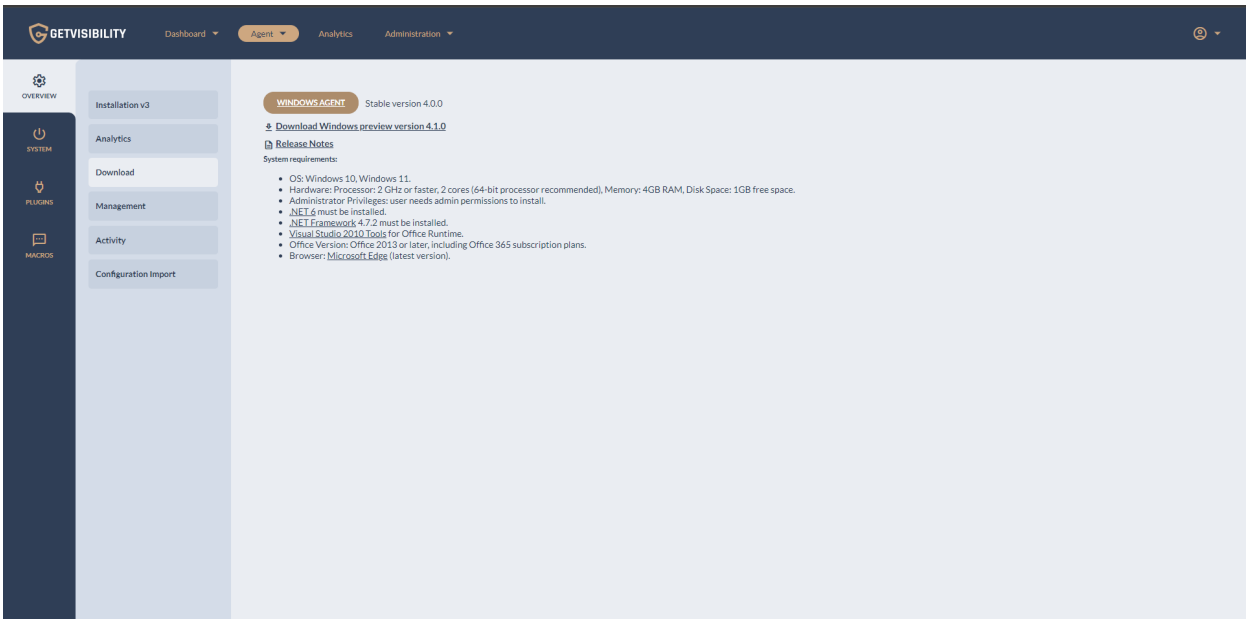

figure 2.

If no bundle has been deployed, the following warning message will be displayed:

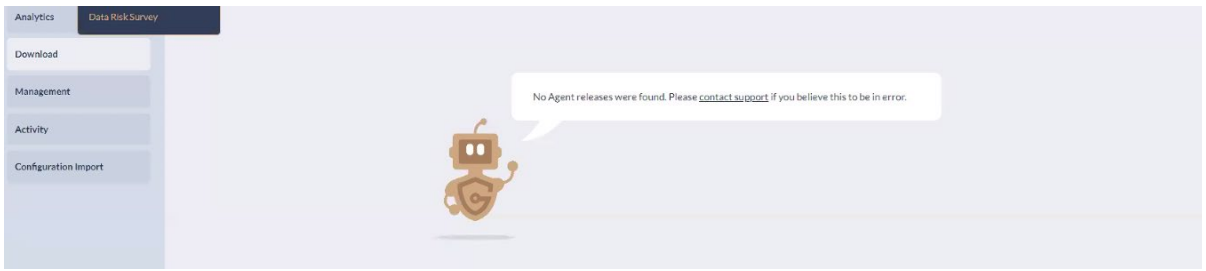

figure 3.

Agent Installation
This section addresses the different methods to install the GV Agent file on a single machine and across multiple machines.

Installation config
The agent supports various initial agent configs which can be specified via `installerConfig.json` or CLI arguments:
Forcepoint Data Classification Powered by Getvisibility Agent installerConfig.json and CLI config Manual Installation

© 2024 Forcepoint

Pre-requisites:

→ The MSI file of the agent.

→ `installerConfig.json` file (optional, provided by Forcepoint).

→ Windows 10 machine.

→ Admin access to install the agent.

Steps

1. **Download the Agent MSI File**: Obtain the MSI file and save it to the Windows machine.
2. **Prepare for Installation**:
   a) Ensure all Office applications are closed to guarantee a clean installation of the agent.
   b) Place the `installerConfig.json` file (if provided by GV) in the same directory as the MSI file.
3. **Configure the Installer**:
   a) Edit the `installerConfig.json` file as needed, based on the provided documentation.

   Forcepoint Data Classification Powered by Getvisibility Agent installerConfig.json and CLI config Manual Installation

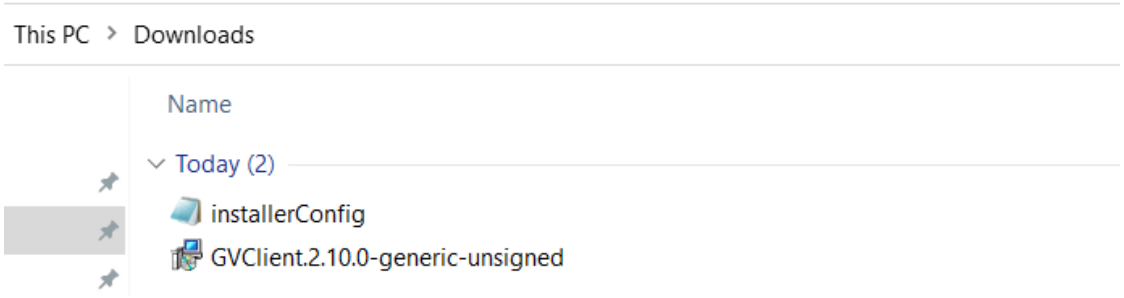

figure 4.

4. **Start the Installation**
   a) Double-click the MSI file to launch the setup.
   b) Accept the terms in the **License Agreement** by checking the box, then click **Install**.

© 2024 Forcepoint

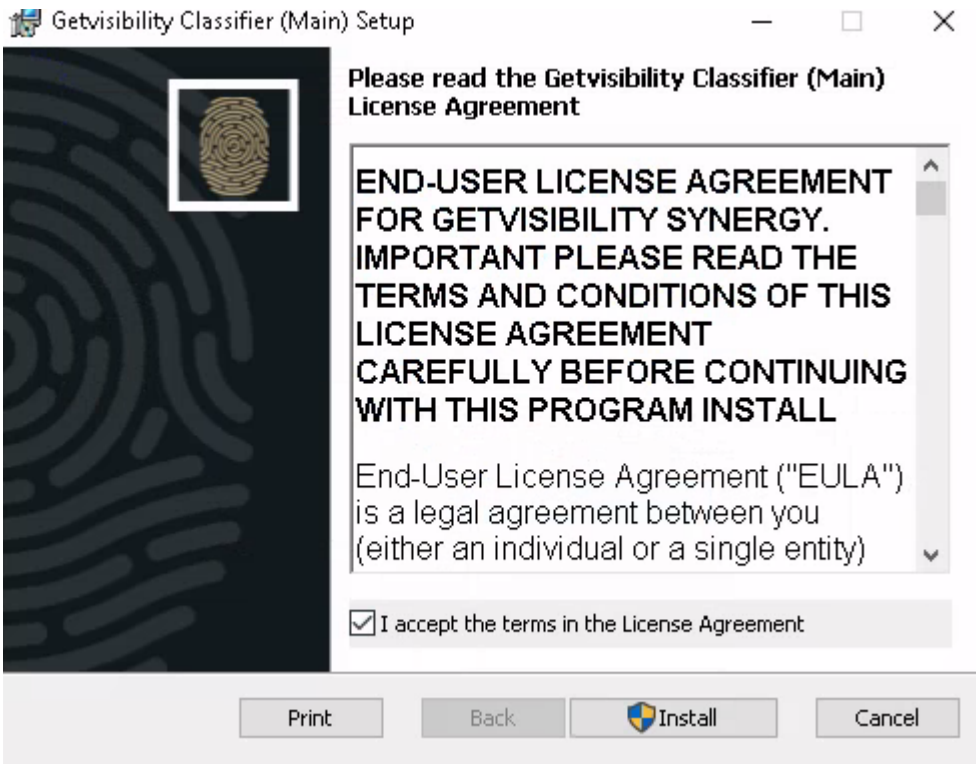

figure 5.

c) Click **Yes** when prompted to allow the app to update your device.

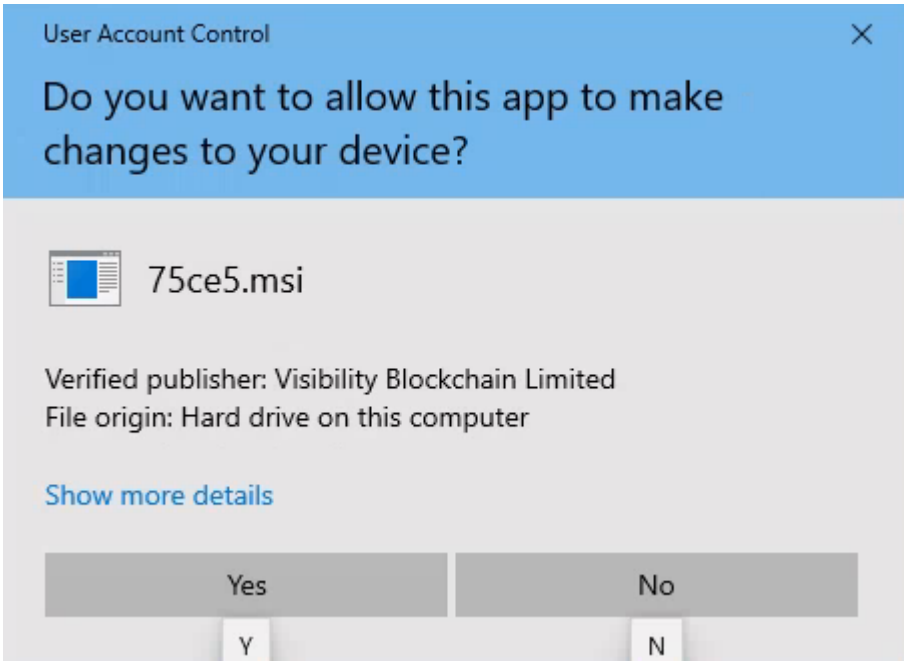

figure 6.

5. **Visual Studio Tools Check**:

© 2024 Forcepoint

a) During installation, if **Microsoft Visual Studio Tools 2010** is not detected, a dialog box will appear.

b) Check the box and click **Install** to add the necessary tools.

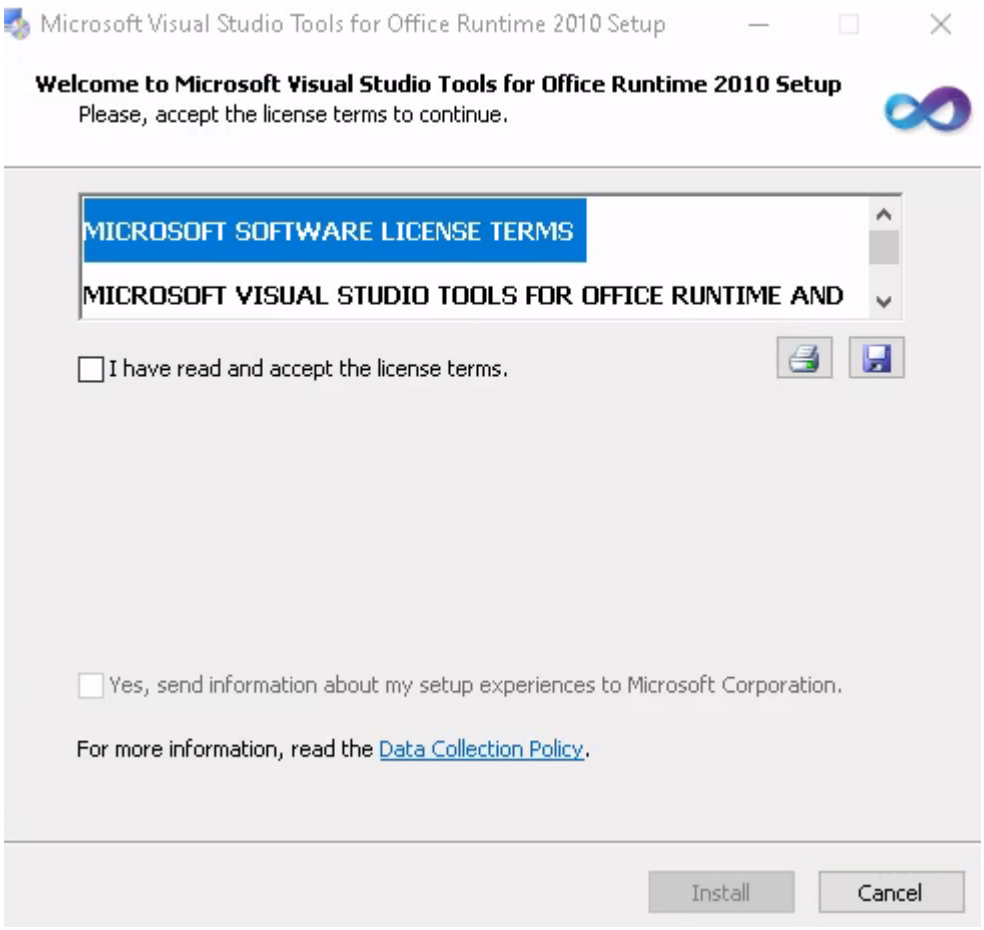

figure 7.

6. **Complete the Installation**:

a) After the installation completes, press **Finish**.

NOTE: In case the machine does not have access to the internet then either the Microsoft website should be whitelisted, or the executable file of the Visual Studio need to be brought inside to that machine. Here is the download link: Download Drivers & Updates for Microsoft, Windows and more - Microsoft Download Center

Installation through CLI

Pre-requisites:

→ **MSI File of the Agent +** `installerConfig.json` file. Ensure both files are ready and accessible.

→ **Windows 10 Machine**: The installation must be conducted on a Windows 10 system.

→ **Admin Access**: You must have administrative privileges to install the agent.

Installation Steps:

1. **Open PowerShell as Administrator**:

© 2024 Forcepoint

a) Search for **PowerShell** in the Windows search bar, right-click on it, and select **Run as administrator**.

2. **Install the Agent**:

a) PowerShell:

→ Use the following command to start the installation. Replace `{path_to_msi}` with the actual path to your MSI file:

```
Start-Process -Wait -ArgumentList "/qn" -PassThru -FilePath
'C:\Users\adm\Downloads\{path_to_msi}.msi'
```

→ In this command:

- `Start-Process` - initiates the installation process.
- `-Wait` - forces the script to wait until the installation is complete.
- `-ArgumentList "/qn"` - runs the installer silently without a user interface.
- `-PassThru` - passes the process information back to PowerShell, which can be useful for troubleshooting.

b) Command line:

→ Use the following command to start the installation:

```
msiexec /i "path_to_msi.msi"
```

3. **Check Installation**:

a) Ensure the installation completes successfully by checking for the agent in the installed programs list or any designated log files.

Installation through group policy (GPO)

Pre-requisites:

→ **MSI file of the agent**: Ensure you have the MSI installation file.

→ **Windows 10 machine**: Target machines must be running Windows 10.

→ **installerConfig.json file** (optional): Configuration file for the installation.

→ **Domain Admin level access**: You need access to the Domain Controller.

Steps:

1. **Prepare the Installation File:**

a) Create a folder on a network-accessible server and place the MSI file there.

© 2024 Forcepoint

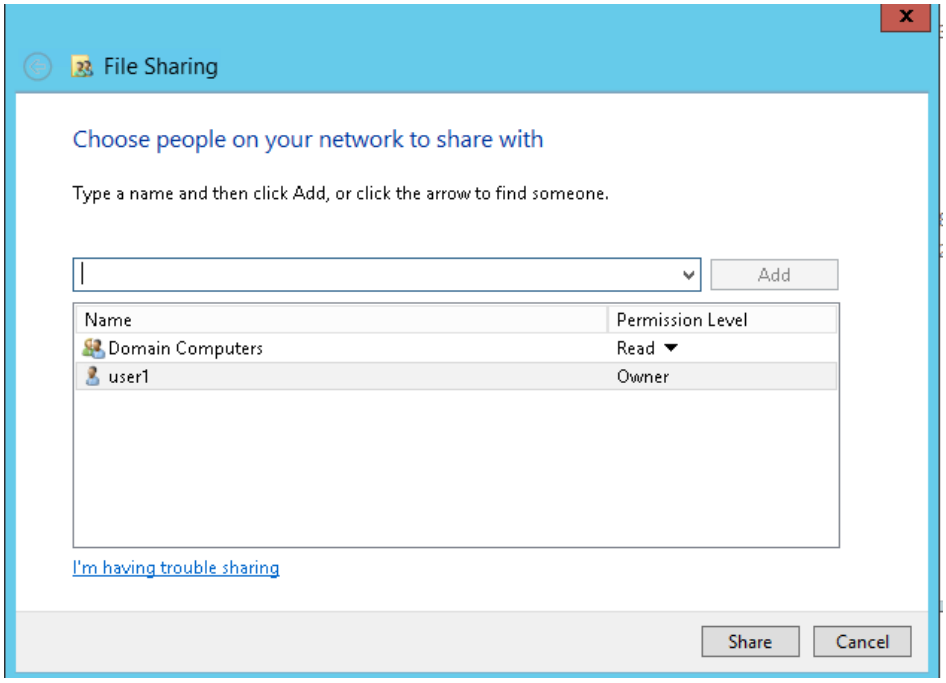

figure 8.

2. **Create a Network Share:**

   a) Share the folder where the agent's MSI file is stored. Assign **Read** permissions to **Domain Computers** to make the MSI file available to all domain accounts.

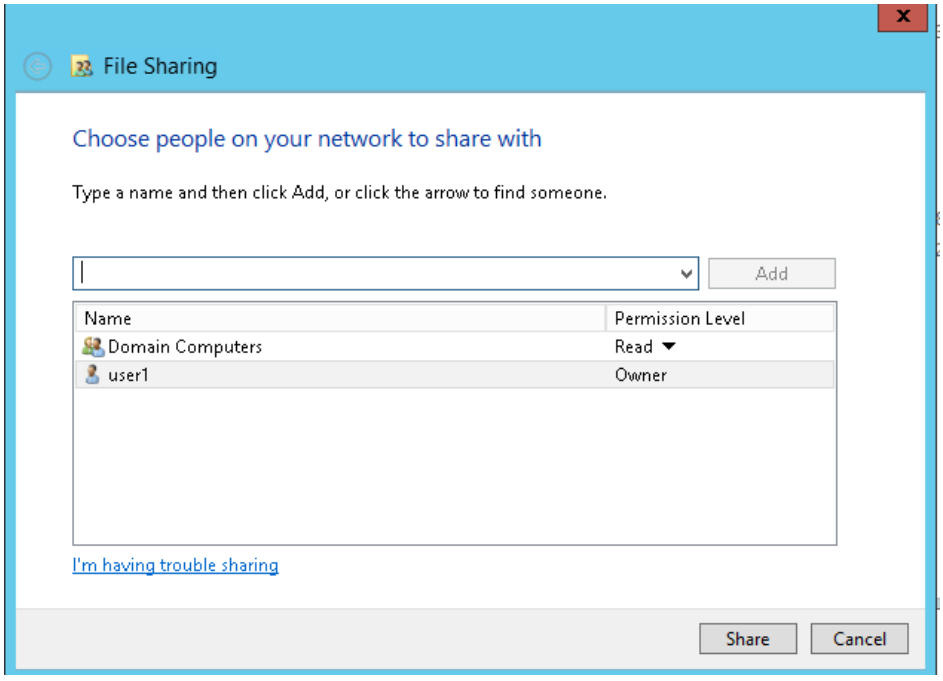

figure 9.

3. **Access the Group Policy Management Console:**

a) On your Domain Controller, open the **Group Policy Management Console**. Navigate to your domain under **Domains**.

4. **Create a Group Policy Object (GPO):**

a) Navigate to the **Organizational Unit** (OU) where you want the software to be installed on every computer.

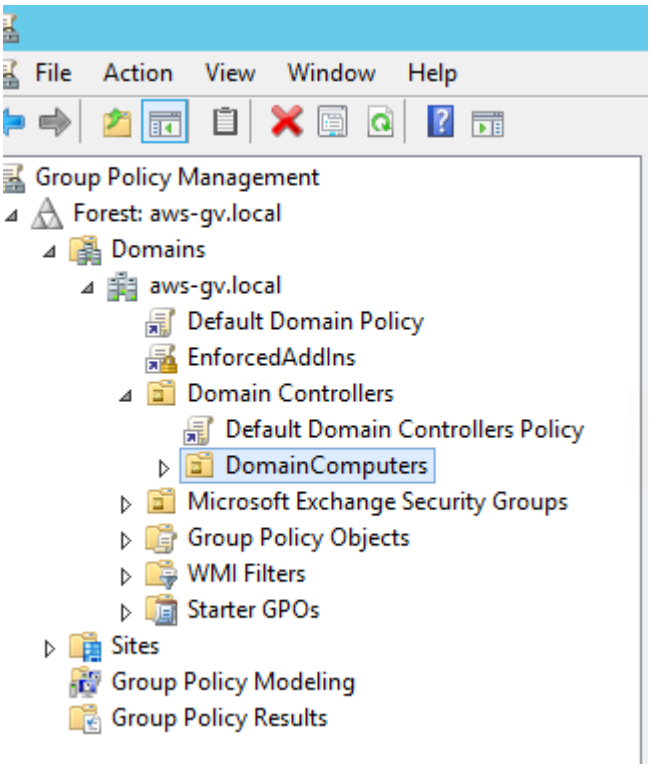

figure 10.

b) Right-click on the OU and select **Create a GPO in this domain and Link it here**. Name your GPO and click **OK**.

© 2024 Forcepoint

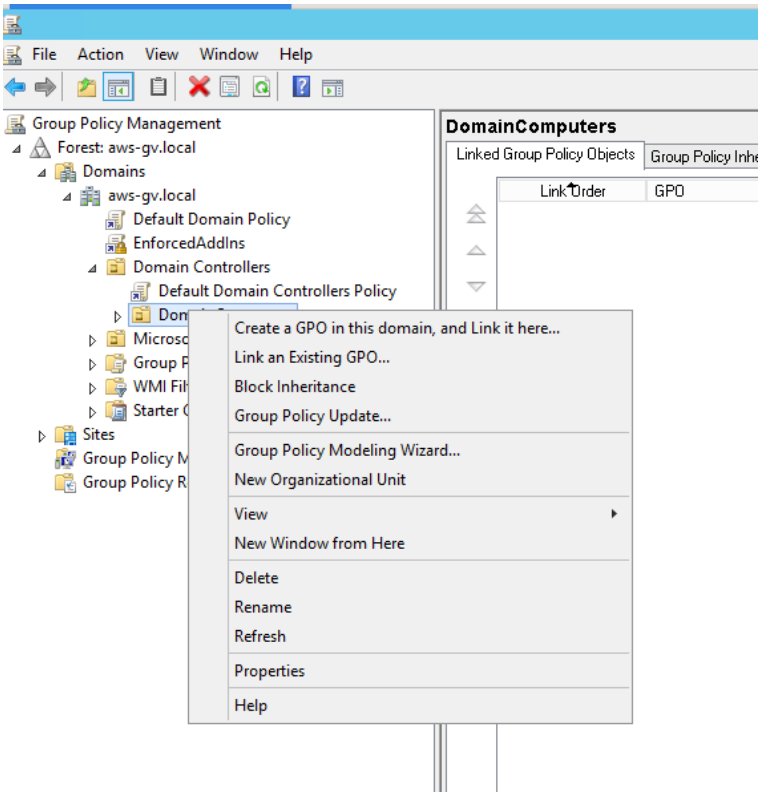

figure 11.

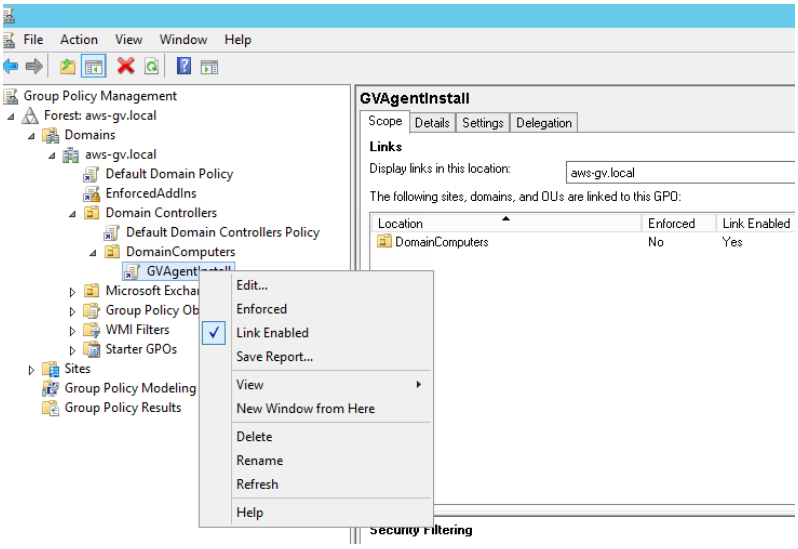

figure 12.

5. **Configure the GPO:**

   a) Select the newly created GPO under the OU, right-click and choose **Edit**.

© 2024 Forcepoint

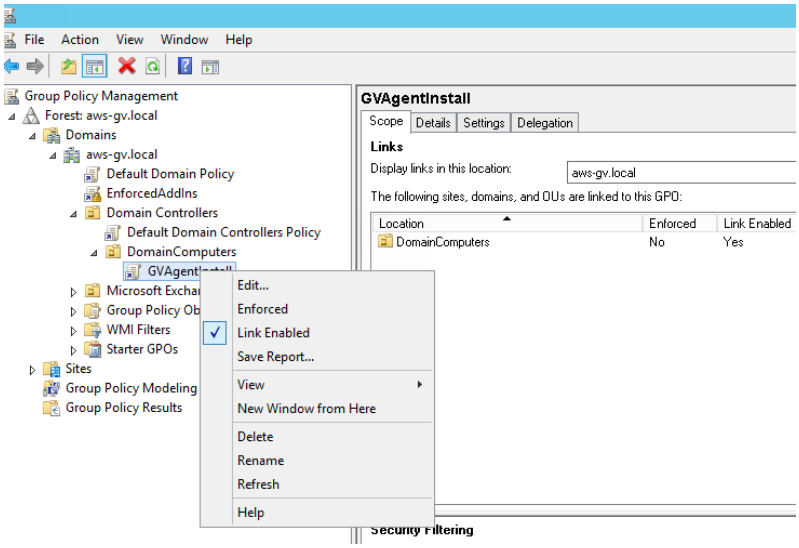

figure 13.

b) Navigate to **Computer Configuration -> Policies -> Software Settings**.

c) Right-click on **Software Installation**, select **New**, then click **Package**.

d) Browse to the network share location of your MSI file, select it, and click **Open**.

6. **Assign the Software:**

a) Select **Assigned** and then click **OK** to ensure the software will be installed automatically on the target machines.

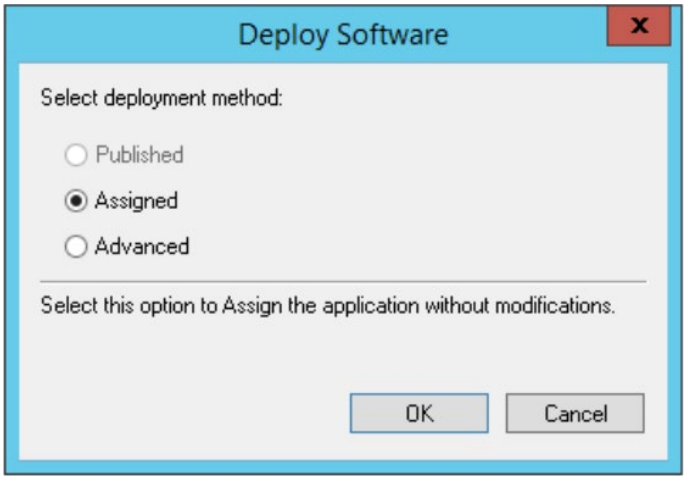

figure 14.

7. **Force Group Policy Update:**

a) On the **Domain Controller**, open **Command Prompt** and run the following command to update group policy across all computers immediately:

```
gpupdate /force
```

8. **Restart Client Machines:**

a) To complete the installation, perform a hard reboot on each client machine where the installation is intended. This ensures the new GPO is applied and the software installation is initiated upon startup.

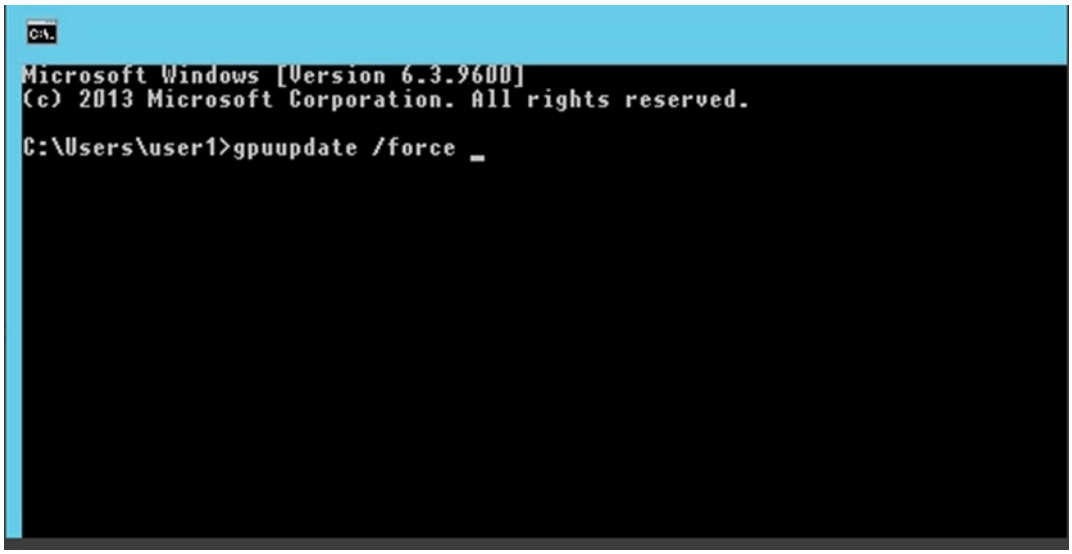

figure 15.

Mass deployment script - e.g. SCCM/PDQ

For mass software distribution, it is recommended to use the following deployment script available. Contact support.forcepoint.com for the script.

Actions Performed by the Script:

1. **Kill all agent processes**: Terminates any running agent processes to ensure a clean installation environment.
2. **Stop all services**: Halts all related services to prevent any interference during installation.
3. **Kill explorer.exe**: Shuts down explorer.exe to avoid file locking issues.
4. **Uninstall previous versions**: Removes earlier installations to eliminate potential conflicts.
5. **Cleanup registry**: Clears registry entries associated with previous versions and plugin deployment.
6. **Fresh install**: Installs the latest version of the software cleanly.

Important Considerations: The use of this script is crucial due to specific issues related to the behavior of `.msi` installers:

→ The installer may opt for a Repair operation instead of an Upgrade.

→ Files marked for deletion after a reboot can disrupt the installation process and even completely break the installation.

NOTE: Deployment via this script requires an `installerConfig.json` file to address configurations specific to your environment.

Installation through SCCM

Pre-requisites:

→ **SCCM Server**: Ensure SCCM is installed and operational.

→ **Access to the SCCM Server**: Administrative rights are needed.

→ **GV Agent MSI File**: Have the MSI file of the GV Agent ready for deployment.

© 2024 Forcepoint

Steps:

1. Open SCCM and Create an **Application**:
   a) Launch SCCM and navigate to the **Home** tab.
   b) Click on **Applications** and select **Create Application** to start the setup process for the new software deployment.
2. Create a **User Collection**:
   a) Click on **Create User Collection** to define a user group for the deployment.
   b) In the **Create User Collection Wizard**, browse and select the target distribution group. For example, set BPO users as the target group.
   c) Click the **Next** button to complete the settings.
3. Configure Deployment Settings:
   a) In the **Deployment Settings**, set the **Action** to **Install** and the **Purpose** to **Available**.
   b) Check the box labeled **Require administrator approval if users request this application**. This setting makes the software available to the end-users but requires administrator permission to install.
   c) Click **Next** to proceed.
4. Complete and **Close** the Deployment:
   a) Review the deployment details on the deployment completion page.
   b) Click **Close** to exit the program.
5. Monitoring Deployment:
   a) After closing the setup, you can monitor the deployment status and details from the SCCM console under the **Deployments** section.

Further installation steps
Further configuration steps after installation:

Forcepoint Data Classification Powered by Getvisibility Preventing Users From Disabling Agent

References:
MSI file installation through GPO: https://community.spiceworks.com/how_to/160869-how-to-install-exe-with-group-policy

MSI file installation through SCCM: https://pdf.wondershare.com/business/how-to-deploy-software-with-sccm.html

Auto-Update

The auto-update feature of the agent allows to distribute new versions of the agent without reinstalling it on a user machine.

The agent utilizes the published `.zip` bundles for the auto-update process.

Prerequisites
Before auto-update can be initiated, the installation must meet the following prerequisites:

→ Not a **Release Candidate** (RC) Version: The installation cannot be an RC version. The current version type can be verified as follows:

→ Windows: Check under the registry key `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Getvisibility\Global\IsRCVersion.`

→ Server Access: The agent must have access to the server.

© 2024 Forcepoint

→ Availability of Auto-update Artifacts: This is detailed in the **Distribution** section.

→ Auto-update Enabled: This is explained in the **Configuration** section.

NOTE: The file names must remain consistent with those provided by the development team when published to the artifactory. Any deviation in the naming could result in a malfunctioning installation.

Configuration

By default, the auto-update functionality is disabled and can be enabled in dashboard.

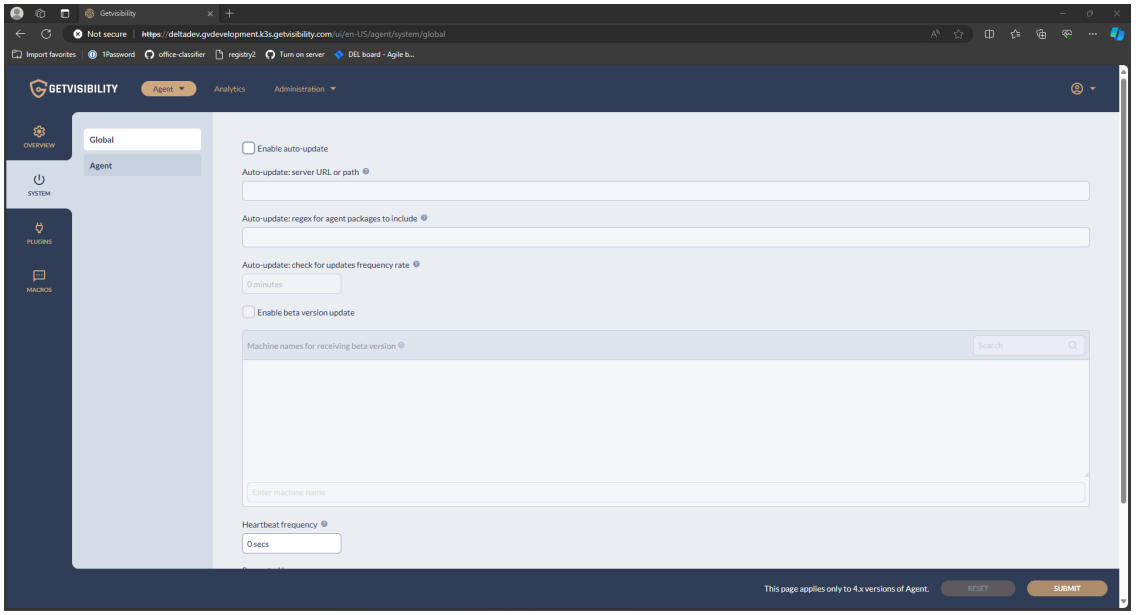

figure 16.

The following properties can be adjusted:

→ `Auto-update: Server URL or path` - specifies the endpoint from where the agent will attempt to download updates. By default, it should be left empty, and agent will assume default values.

→ By default, the endpoint defaults to:

https://{cluster}/static-server/static/agent/stable/ - for stable releases

https://{cluster}/static-server/static/agent/beta/ - for beta releases

→ Custom URLs or paths do not support beta releases.

→ It supports local file path - if this is the case, the full path to the directory must be provided, e.g. `C:/Artifacts`

→ If a custom URL is used it must be a NGINX File Server which lists the files in JSON format - configuration **autoindex_format json**. Example:

```
server {
  listen 80;
  server_name auto-updater;
  access_log /var/log/access.log;
  error_log /var/log/error.log;
```

© 2024 Forcepoint

```
    location /static/ {
      alias /var/static/;
      autoindex on;
     autoindex_format json;
      gzip_static on;
      expires max;
      add_header Cache-Control public;
    }
  }
```

→ `Auto-update: regex for agent packages to include` - specifies the regex which will be used for artifacts discovery. By default, it should be left empty, and agent will assume default values.

→ `Auto-upate: check for updates frequency rate` - how often the agent should look for updates. By default, it should be left empty, and agent will assume default values.

→ `Enable beta version update` - If this option is enabled and appropriate machine name entries are created, the targeted machines will attempt to fetch auto-updates from beta endpoints instead of stable endpoints (stable endpoint will be completely ignored by the agent).

NOTE: The agent only supports upgrading via auto-update. It is not possible to downgrade using auto-update functionality.

This means removing machine from beta endpoints will not result in the agent downgrading to the previous stable version.

© 2024 Forcepoint Forcepoint Proprietary

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's humanly attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.

© 2024 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. All other trademarks used in this document are the property of their respective owners.
[Forcepoint Data Classification Powered by Getvisibility Agent Deployment Flow] [Status]15 Jul. 24