Craig ELlrod

senior cloud security architect

Deploying Armor Agent with N-Able

N-Central

Table of Contents

[Introduction 3](#_Toc87866777)

[Prerequisites 3](#_Toc87866778)

[How it works 3](#_Toc87866779)

[Create Automation Manager .amp File 4](#_Toc87866780)

[Step 1 – Log into the Armor Portal to grab the Windows Installation Script and License Key 4](#_Toc87866781)

[Step 2 – Log Into N-Central and start the Automation Manager 5](#_Toc87866782)

[Step 3 – Select New Policy 6](#_Toc87866783)

[Step 4 – Select Input in Policy Builder 6](#_Toc87866784)

[Step 5 – ADD an Input Parameter 7](#_Toc87866785)

[Step 6 – Search for PowerShell Script 8](#_Toc87866786)

[Step 7 – Select Add 🡪 the Armor License Input Parameter. 9](#_Toc87866787)

[Step 8 – Select the Script Tab and Edit 10](#_Toc87866788)

[Step 9 – Paste the Armor Installation Script into the “Script” window 11](#_Toc87866789)

[Step 10 – Save the Armor Installation Policy 12](#_Toc87866790)

[Step 11 – Upload the Armor Installation Policy 12](#_Toc87866791)

[Create Scheduled Task in N-Central 13](#_Toc87866792)

[Step 12 – Navigate back to the N-Able N-Central Web Browser Interface 13](#_Toc87866793)

[Step 13 – Navigate to Configuration 🡪 Profiles 13](#_Toc87866794)

[Step 14 – Add Task Name 14](#_Toc87866795)

[Step 14 – Select the ArmorInstall Repository from the Automation Manager 14](#_Toc87866796)

[Step 15 – Select the ARMOR-LICENSE-KEY input parameter 15](#_Toc87866797)

[Step 16 – Select Save 16](#_Toc87866798)

[Create Automation Rule in N-Central 16](#_Toc87866799)

[Step 17 – Navigate to Monitoring 🡪 Rules 🡪 Add 16](#_Toc87866800)

[Step 18 – Give the Rule a name 🡪 ARMOR-CLOUD-SECURITY-INSTLSL-RULE 17](#_Toc87866801)

[Step 19 – Navigate to the Scheduled Task Profiles tab 18](#_Toc87866802)

[Step 20 – Navigate to the Select Customers tab 18](#_Toc87866803)

[Enter Armor License Key for each Customer 19](#_Toc87866804)

[Step 21 – Navigate the All Devices view from the SO or MSP level. 19](#_Toc87866805)

# Introduction

This ARMOR Defense field guide will present a step-by-step method to deploy the Armor Agent automatically using the automation tools within N-Able’s N-Central platform.

## Prerequisites

An account with N-Able N-Central access.

<https://n-able.com>

An Armor Management Portal account – Managed Service Provider

<https://amp.armor.com>

The github for this tutorial.

<https://github.com/surfd4wg/armor_NAble>

The scripts for this tutorial.

ArmorAgentInstall.ps1

ArmorInstall.amp

Note: The N-Able automation scripts and platform do not work with MAC OSX.

Additionally, there is a distinction with N-Able where they refer to the Managed Service Provider (MSP) account as the Service Organization (SO). Some illustrations in this document will refer to the “SO” or “MSP”, while other illustrations will refer to the MSP’s or SO’s customer, as “Customer”.

## How it works

Installing the Armor Agent for Windows through N-Able N-Central, involves these simple steps.

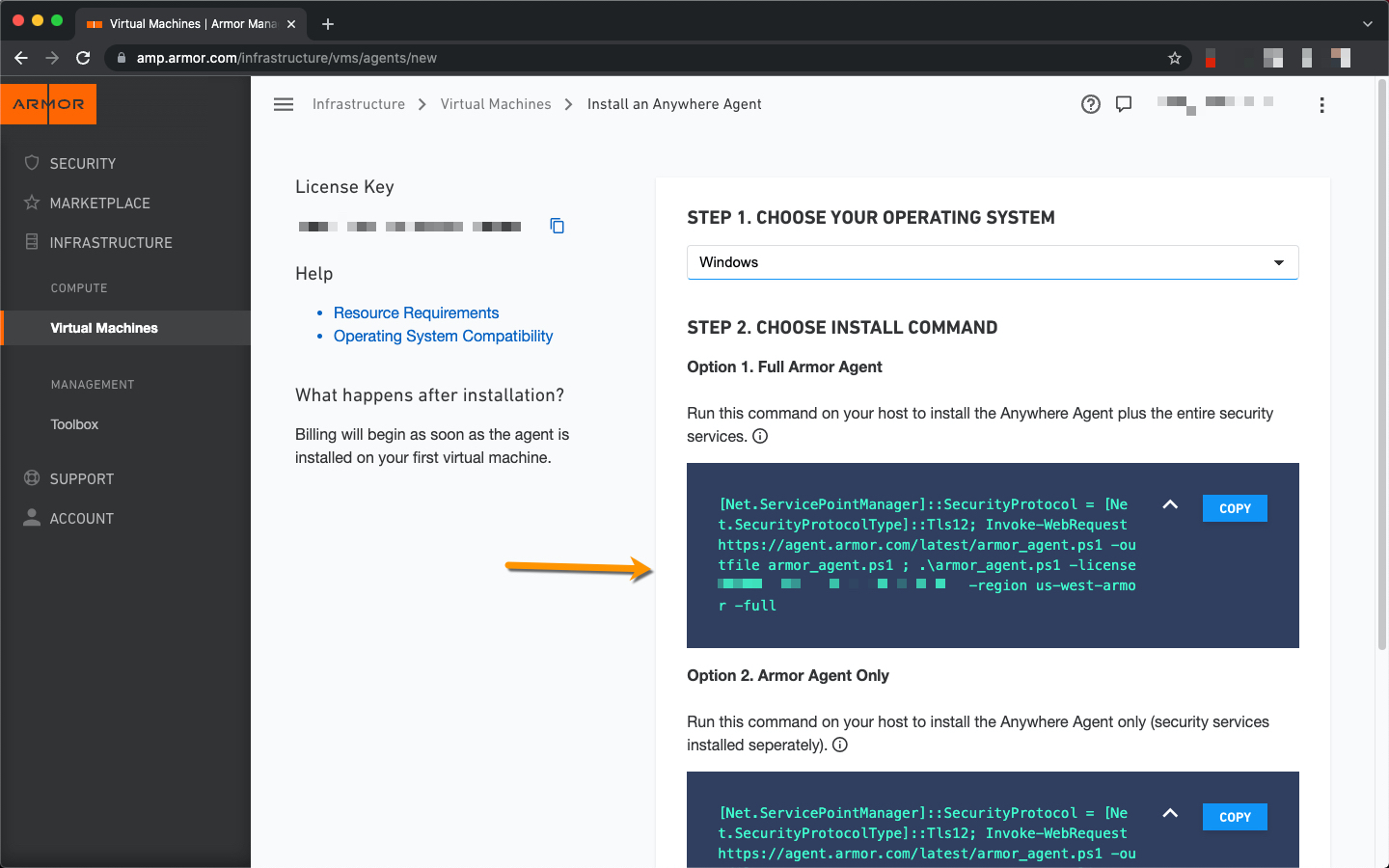
* Create an automation policy .amp file in N-Able Automation Manager
* Create a task profile in N-Central that uses the automation policy
* Create an automation rule in N-Central
* Assign the Armor License to each customer in N-Central

# Create Automation Manager .amp File

### Step 1 – Log into the Armor Portal to grab the Windows Installation Script and License Key

The preferred method of installing the Armor Agent into a Windows machine, is by executing the installation PowerShell script in a Windows PowerShell shell.

Log into the Armor Management Portal and copy the Windows installation PowerShell script.



Note: Paste the PowerShell script into a text editor, as we will turn the license key into a scripting variable in N-Central.

Add the following to the main.tf terraform file. Replace the license key placeholder XXXXX-XXXXX-XXXXX-XXXXX-XXXXX with your AMP license key.

Note: The PowerShell installation script can be found by logging into the Armor Management Portal (<https://amp.armor.com>) and navigating to Infrastructure 🡪 Virtual Machines 🡪 + sign. Click on the shield. Select the Windows operating system. For reference the PowerShell installation script is as follows:

﻿[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12; Invoke-WebRequest https://agent.armor.com/latest/armor\_agent.ps1 -outfile armor\_agent.ps1; .\armor\_agent.ps1 -license XXXXX-XXXXX-XXXXX-XXXXX-XXXXX -region us-west-armor -full

### Step 2 – Log Into N-Central and start the Automation Manager

Navigate to the SO level (Top Level) of N-Central, and launch the Automation Manager.

A picture containing text, screenshot, monitor

Description automatically generated

﻿

### Step 3 – Select New Policy

Text, whiteboard

Description automatically generated

### Step 4 – Select Input in Policy Builder

Graphical user interface

Description automatically generated

Graphical user interface

Description automatically generated

### Step 5 – ADD an Input Parameter

Graphical user interface

Description automatically generated

Create the parameter with the following fields

Name: inputARMORlicense

Display: Input Armor License

Type: Password

Value: <empty>

Graphical user interface

Description automatically generated

Click on ‘Ok’, then ‘Ok’.

### Step 6 – Search for PowerShell Script

In the left navigation search for “Run PowerShell”, then drag that script to the middle bar between Input and Output.

Graphical user interface

Description automatically generated

### Step 7 – Select Add 🡪 the Armor License Input Parameter.

Graphical user interface, application, Teams

Description automatically generated

Graphical user interface

Description automatically generated

### Step 8 – Select the Script Tab and Edit

Graphical user interface, application

Description automatically generated

### Step 9 – Paste the Armor Installation Script into the “Script” window

Graphical user interface, text, application

Description automatically generated

Note: Make sure the Armor License Key XXXXX-XXXXX-XXXXX-XXXXX-XXXXX with the parameter we just created ex: $inputARMORlicense.

Note: Use the following PowerShell script, which can also be found on the GitHub site.

[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12; Invoke-WebRequest https://agent.armor.com/latest/armor\_agent.ps1 -outfile armor\_agent.ps1 ; .\armor\_agent.ps1 -license $inputARMORlicense -region us-west-armor -full

### Step 10 – Save the Armor Installation Policy

Graphical user interface

Description automatically generated

### Step 11 – Upload the Armor Installation Policy

Graphical user interface

Description automatically generated

# Create Scheduled Task in N-Central

### Step 12 – Navigate back to the N-Able N-Central Web Browser Interface

Graphical user interface, text, application, Word

Description automatically generated

### Step 13 – Navigate to Configuration 🡪 Profiles

Select Add 🡪 Automation Policy

Graphical user interface, text, application

Description automatically generated

### Step 14 – Add Task Name

Graphical user interface, text, application

Description automatically generated

### Step 14 – Select the ArmorInstall Repository from the Automation Manager

Graphical user interface, text, application

Description automatically generated

### Step 15 – Select the ARMOR-LICENSE-KEY input parameter

Graphical user interface, application, Teams

Description automatically generated

A screenshot of a computer

Description automatically generated

### Step 16 – Select Save

# Create Automation Rule in N-Central

### Step 17 – Navigate to Monitoring 🡪 Rules 🡪 Add

Graphical user interface

Description automatically generated

### Step 18 – Give the Rule a name 🡪 ARMOR-CLOUD-SECURITY-INSTLSL-RULE

Select Windows Servers, Workstations and Laptops

Graphical user interface, text

Description automatically generated

### Step 19 – Navigate to the Scheduled Task Profiles tab

Select the Scheduled Task Profile created in the previous section.

Graphical user interface, text

Description automatically generated

### Step 20 – Navigate to the Select Customers tab

Select which customers you want to have this policy turn on for

Graphical user interface, application

Description automatically generated

Click ‘Save’.

# Enter Armor License Key for each Customer

### Step 21 – Navigate the All Devices view from the SO or MSP level.

Click on Custom Properties, for each customer. Enter the Armor License key for each customer.

A screenshot of a computer

Description automatically generated

Graphical user interface, application

Description automatically generated