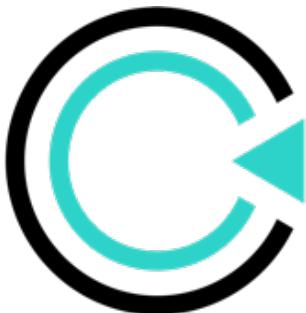


COVE DATA PROTECTION

N-CENTRAL INTEGRATION

INTRODUCTION	2
REQUIREMENTS	2
PREPARATION	2
STEP 1: UPLOAD THE AUTOMATION POLICY	3
STEP 2: UPLOAD THE AUTOMATION POLICY	4
STEP 3: SELECT THE DEVICE(S) FOR DEPLOYMENT	5
STEP 4: SELECT AUTOMATION TASK	6
STEP 5: GET THE CUSTOMER UID FROM THE COVE DATA PROTECTION PORTAL.....	7
STEP 6: ENTER DETAILS IN THE AUTOMATION POLICY TASK	8
STEP 7: CREATE FILTER FOR COVE DATA PROTECTION	9
STEP 8: ADD FILTER TO EXISTING RULE	10
STEP 9: MODIFY MONITORING THRESHOLDS	11
STEP 10: CREATE A MONITORING DASHBOARD	12
STEP 11: CONFIGURE MONITORING OPTIONS.....	13
STEP 12: CHECK DASHBOARD	14
SUMMARY.....	15



Cove
Data Protection™

INTRODUCTION

With use of the following guide, you'll be able to roll out Cove Data Protection into your N-Central devices with just a few mouse clicks. After the roll-out, the software is not only installed, but also configured with a profile and product of your choice.

The automation policy is going to:

- Download the latest Cove Data Protection Backup manager
- Save the download in C:\Windows\Temp
- Execute the download with extra parameters for a silent install with a profile and product attached.
- Remove the downloaded installer after installation

REQUIREMENTS

- N-Central 11 or higher
- For Servers: Windows 2008R2 or higher, .NET framework 4.5 or higher
- For Workstations: Windows 7 or higher, NET framework 4.5 or higher

PREPARATION

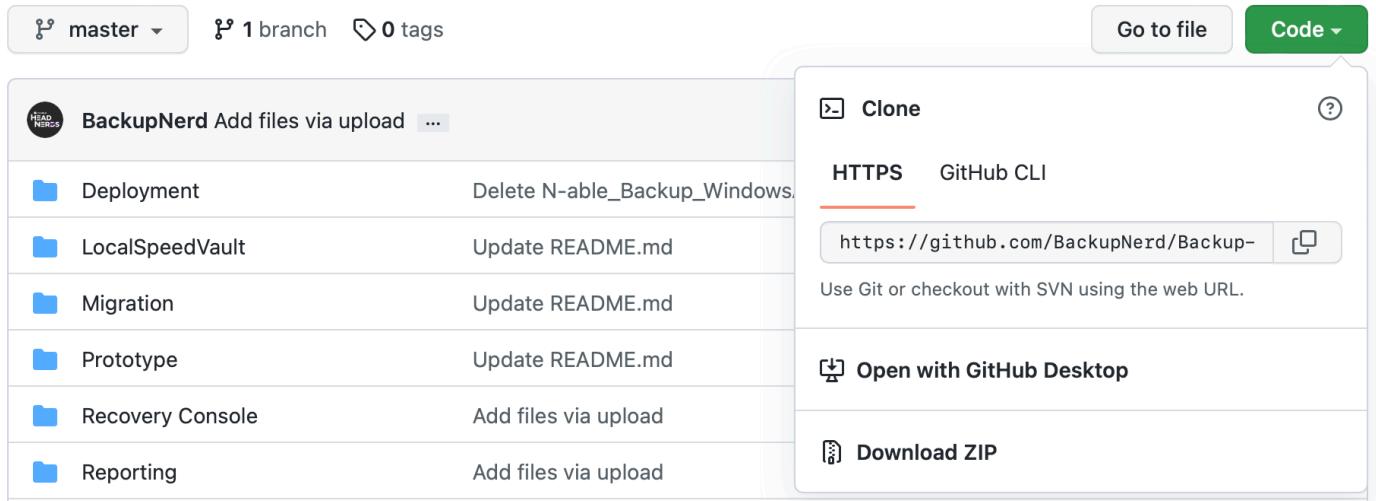
Before running this automation task, please make sure you have available or add:

- access to the Cove Data Protection portal, at <https://backup.management>
- a Profile
- a Product
- the customer(s) created in the Cove Data Protection portal

STEP 1: UPLOAD THE AUTOMATION POLICY

Download 'Cove Data Protection AutoDeploy.vXX.amp' automation policy from the github page:
<https://github.com/BackupNerd/Backup-Scripts>

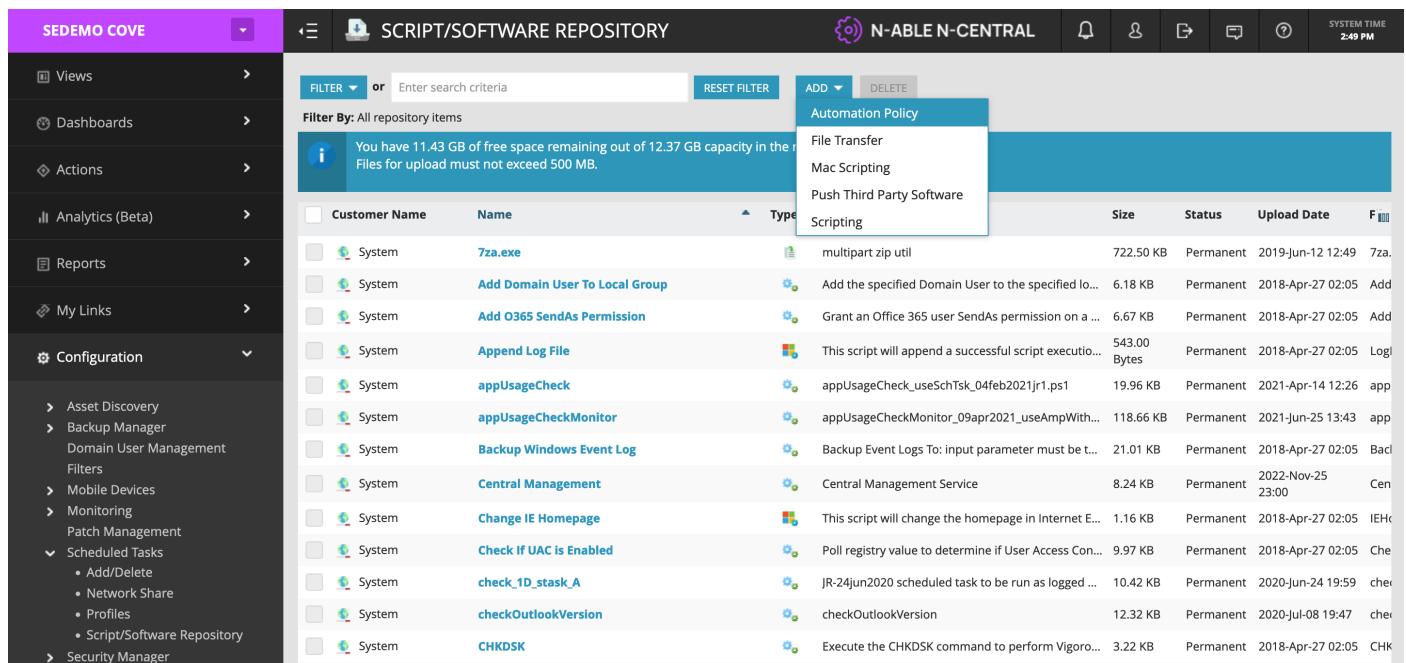
- Click the green 'Code' button and select 'Download ZIP'



The screenshot shows a GitHub repository named 'BackupNerd'. The 'Deployment' folder is highlighted. On the right, there are download options: 'Clone' via HTTPS or GitHub CLI, 'Open with GitHub Desktop', and 'Download ZIP'.

The 'Cove Data Protection AutoDeploy.vXX.amp' file is located in the *Deployment/N-able Automation Policies* folder.

Login to your N-Central dashboard, select the Service Organization you want to use for the policy and browse to Configuration -> Scheduled Tasks -> Script/Software Repository. Click ADD and select the option Automation Policy.



The screenshot shows the N-Central dashboard with the 'SCRIPT/SOFTWARE REPOSITORY' tab selected. A context menu is open over a list of files, with 'Automation Policy' highlighted. The list includes various system scripts like '7za.exe', 'Append Log File', and 'CHKDSK'.

STEP 2: UPLOAD THE AUTOMATION POLICY

Browse to the *Cove Data Protection AutoDeploy.vXX.amp* file and click **OK** to upload the policy into your repository.

The screenshot shows the N-Central interface with a purple header bar containing the text "SEDEMO COVE". Below the header is a sidebar with various navigation options like Views, Dashboards, Actions, Analytics (Beta), Reports, My Links, Configuration, Administration, Integrations, and Help. The main content area has a title "ADD SCRIPT/SOFTWARE REPOSITORY ITEM" with a gear icon. A blue banner at the top states: "You have 11.43 GB of free space remaining out of 12.37 GB capacity in the repository. Files for upload must not exceed 500 MB." Below this is a "DETAILS" section with fields for Type (set to Automation Policy), Name, and Description. Under the "Details" tab, there is a "File Name" field containing "Cove Data Protection Agent Deploy v22.07.amp", a "BROWSE ..." button, and a "CANCEL" button. At the bottom of the dialog are "OK" and "CANCEL" buttons. The top right corner of the interface shows "N-ABLE N-CENTRAL", system time "2:53 PM", and several small icons.

STEP 3: SELECT THE DEVICE(S) FOR DEPLOYMENT

Select the device(s) you want to deploy through the automation policy, click on **ADD TASK** and select **Run an Automation Policy**.

The screenshot shows the N-ABLE N-CENTRAL software interface. On the left is a sidebar with various navigation links: Views, Active Issues, All Devices, Job Status, NetPath, Topology Maps, Navigate to SO Level, Dashboards, Actions, Analytics (Beta), Reports, My Links, Configuration, Administration, Integrations, and Help. The main area is titled 'ALL DEVICES' and shows a list of network devices. At the top of this list is '2012R2-BOG'. To the right of this device, a context menu is open, listing several options under 'ADD TASK': File Transfer, Push Third Party Software, Run a Mac Script, Run a Script, and Run an Automation Policy. The 'Run an Automation Policy' option is highlighted with a blue border. Below the device list, there are buttons for 'REFRESH NOW', 'ON', and 'Refresh in: 10 minutes', along with status indicators for 'Selected: 1' and 'Total: 1'.

STEP 4: SELECT AUTOMATION TASK

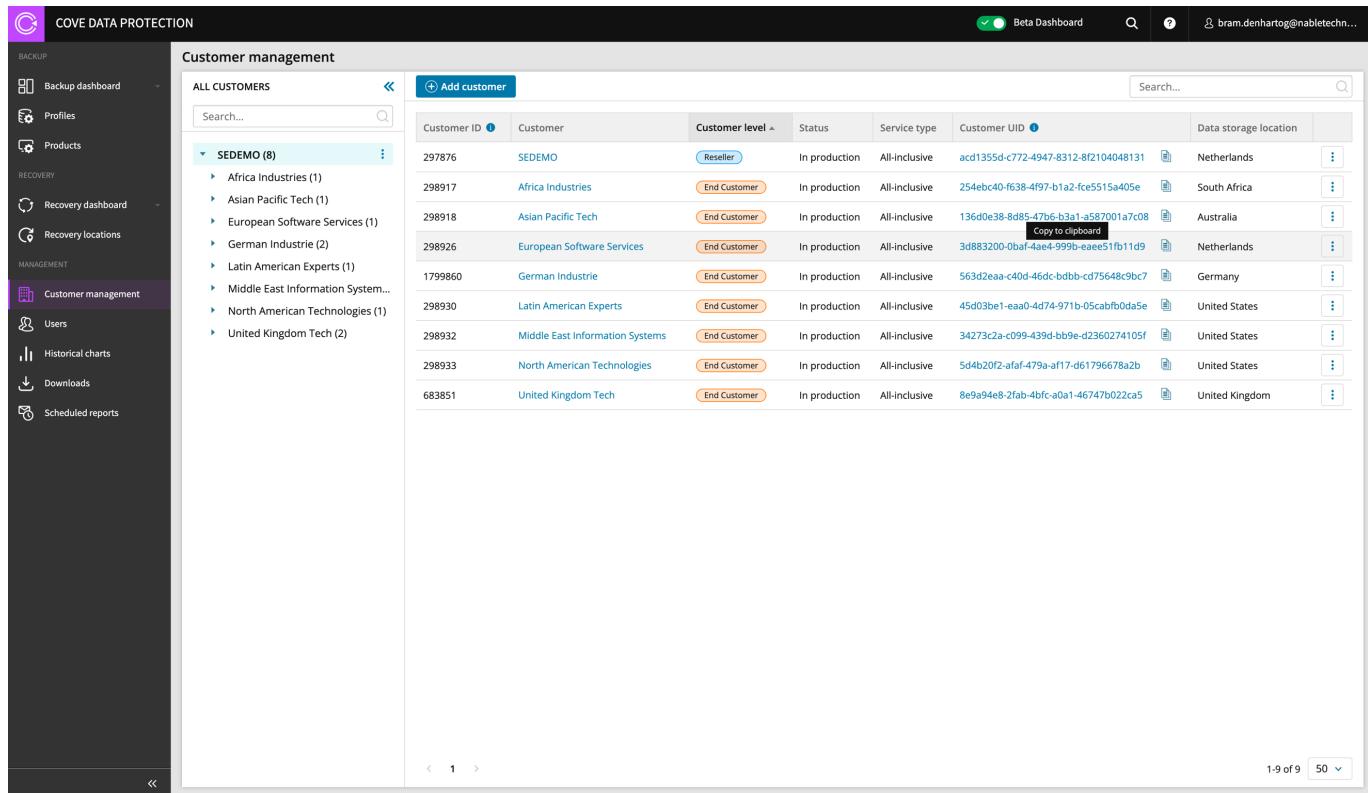
Select **Cove Data Protection AutoDeploy.vXX.amp** as your **Repository Item**. The interface will ask for a Customer UID, Profile Name and Product Name. Please proceed to **Step 5** that will guide you to these details.

Optional you can set an Archive schedule and Bandwidth limitation.

The screenshot shows the 'AUTOMATION POLICY TASK' configuration screen. The left sidebar contains navigation links such as Views, Dashboards, Actions, Analytics (Beta), Reports, My Links, Configuration, Administration, Integrations, and Help. The main panel has tabs for Details, Executing Devices, Targets, Schedule, and Notifications. The 'DETAILS' tab is active, showing the Task Name 'Automation Policy - 2023-03-16 15h04m15s' and the Enabled checkbox checked. The 'CREDENTIALS' tab shows options for Use LocalSystem credentials (selected), Use Device Credentials, Custom Credentials, and Use Currently Logged On User. The 'AUTOMATION POLICY' tab displays the Repository Item 'Cove Data Protection Agent Deploy v22.07', Description 'v22.07 Abort if prior install found Https download Set Customer Set Profile Set Product ~3 min deploy delay Set Archive Get FP Visa Set Throttle', and File Name 'Cove Data Protection Agent Deploy v22.07.amp'. The 'INPUT PARAMETERS' tab lists two parameters: 'Cove Customer UID' with value 'i.e. 9696c2af4-678a-4727-9b6b-fc1a217e38ec' and 'Set Backup Profile (true|false)' with value 'true'. At the bottom are 'SAVE' and 'CANCEL' buttons.

STEP 5: GET THE CUSTOMER UID FROM THE COVE DATA PROTECTION PORTAL

Please login to the Cove Data Protection portal, make sure you have the customers (Customers in N-Central) created. Go to Customer Management and copy the '**Customer UID**' of the particular customer.



The screenshot shows the 'Customer management' page in the Cove Data Protection portal. The left sidebar includes options for Backup, Recovery, and Management (with Customer management selected). The main area displays a table of customers under 'ALL CUSTOMERS'. The columns include Customer ID, Customer name, Customer level (Reseller or End Customer), Status, Service type, Customer UID (with a 'Copy to clipboard' button), and Data storage location. A search bar and a 'Customer level' dropdown are also present at the top of the table.

Customer ID	Customer	Customer level	Status	Service type	Customer UID	Data storage location
297876	SEDEMO	Reseller	In production	All-inclusive	acd1355d-c772-4947-8312-8f2104048131	Netherlands
298917	Africa Industries	End Customer	In production	All-inclusive	254ebc40-f638-4f97-b1a2-fce5515a405e	South Africa
298918	Asian Pacific Tech	End Customer	In production	All-inclusive	136d0e38-8d85-47b6-b3a1-a587001a7c08	Australia
298926	European Software Services	End Customer	In production	All-inclusive	3d883200-0ba1-4ae4-999b-eae51fb11d9	Netherlands
1799860	German Industrie	End Customer	In production	All-inclusive	563d2eaa-c40d-46dc-bdbb-cd75648c9bc7	Germany
298930	Latin American Experts	End Customer	In production	All-inclusive	45d03be1-eaa0-4d74-971b-05cabfb0da5e	United States
298932	Middle East Information Systems	End Customer	In production	All-inclusive	34273c2a-c099-439d-bb9e-d2360274105f	United States
298933	North American Technologies	End Customer	In production	All-inclusive	5d4b20f2-afaf-479a-af17-d61796678a2b	United States
683851	United Kingdom Tech	End Customer	In production	All-inclusive	8e9a94e8-2fab-4bfc-a0a1-46747b022ca5	United Kingdom

STEP 6: ENTER DETAILS IN THE AUTOMATION POLICY TASK

Paste the Customer UID from the Cove Data Protection portal and type the exact name of the Profile and Product in the correct fields. After clicking **SAVE**, Cove Data Protection will be downloaded, installed and configured on the device(s), according to the details you just entered. The download is a little over 100MB, depending on your download speed the process should take 2-5 mins.

The screenshot shows the 'AUTOMATION POLICY TASK' configuration page. On the left is a navigation sidebar with 'EUROPEAN SOFTWARE SEF' selected. The main area has tabs for 'Details', 'Executing Devices', 'Targets', 'Schedule', and 'Notifications'. The 'Details' tab is active. It shows a 'Task Name' field containing 'Automation Policy - 2023-03-16 15h04m15s' and an 'Enabled' checkbox checked. Below this are sections for 'CREDENTIALS' (using LocalSystem credentials), 'AUTOMATION POLICY' (repository item 'Cove Data Protection Agent Deploy v22.07'), and 'INPUT PARAMETERS'. The 'INPUT PARAMETERS' section contains fields for 'Cove Customer UID' (set to '9696c2af4-678a-4727-9b6b-fc1a217e38ec'), 'Set Backup Profile (true|false)' (set to 'true'), 'Backup Profile Name' (set to '4 hour RPO'), 'Set Backup Product (true|false)' (set to 'true'), 'Backup Product Name' (set to '90 Days'), 'Set Archiving (true|false)' (set to 'true'), and 'Archive Day of Month' (set to 'Last'). At the bottom are 'SAVE' and 'CANCEL' buttons.

STEP 7: CREATE FILTER FOR COVE DATA PROTECTION

To make sure the devices are reporting correctly back into your N-Central environment, we need to add the following filter. Go to **Configuration -> Filters -> ADD**.

In the following screen, enter a filter name, e.g. **Cove Data Protection**. Select **Application - Windows Service Name - EQUAL TO - Backup Service Controller** and click **SAVE**.

The screenshot shows the N-ABLE N-CENTRAL web interface. On the left, there is a sidebar with various navigation options like Views, Dashboards, Actions, Reports, My Links, Configuration, and Administration. The main area is titled "CREATE NEW FILTER". It has fields for "Filter Name" (set to "Cove Data Protection") and "is available to" (set to "Everyone"). Below this, there's a "Description" field and a checkbox for "Show in my Drop-Down". A "ADVANCED MODE" section contains a "Find devices where:" dropdown menu. The menu is set to "Application" and shows a search bar with "Windows Service Name" and a dropdown menu with "EQUAL TO" and "Backup Service Controller". There is also an "ADD" button. At the bottom of the filter creation screen are three buttons: "SAVE", "PREVIEW", and "CANCEL".

STEP 8: ADD FILTER TO EXISTING RULE

Go to **Configuration -> Monitoring -> Rules**. Click on the **N-able Backup Manager** rule. In the next screen make sure you're on the **Devices to Target** tab. You'll be presented with the list of available filters. Select the just created filter **Cove Data Protection**, move it to the right and click **SAVE**.

The screenshot shows the 'RULE DETAILS' page for a rule named 'N-able Backup Manager'. The 'Devices to Target' tab is selected. In the 'FILTERS' section, a list of available filters is shown on the left, and 'Selected Filters' is on the right. The filter 'Cove Data Protection' is highlighted in blue. Below the filters, there is a section for 'INELIGIBLE FILTERS (9)'. At the bottom, there are 'SAVE' and 'CANCEL' buttons.

Available Filters:

- Filters
- Cisco Umbrella
- CompetitorSearch
- covidProperty
- Dell Remote Access Controller
- Dell Servers
- devices with
- Devices with Discovered Name not Matching Given Name
- Devices with Office 2007
- Devices with Office 2010
- Devices with Scheduled Tasks Enabled
- Devices without PowerShell V2

Selected Filters:

- Cove Data Protection

INELIGIBLE FILTERS (9)

Buttons:

- SAVE
- CANCEL

STEP 9: MODIFY MONITORING THRESHOLDS

Go to **Configuration -> Monitoring -> Service Templates** and click the **N-able Backup Manager Monitoring on Servers**. You can repeat this step for the **Workstations** and **Laptops** template.

Click on the **Backup Monitoring – N-able Backup Product Status** template.

Select the tab **Thresholds** and switch **Installation Status** to **Off** and click **SAVE**.

In order to re-apply the template to existing devices, select on the **Add Service Template** page the tab **Associated Devices**. Select all devices and click on **Save and re-apply Service Template**. Now all devices will have the new monitoring applied.

BUTTONS: BACKUP MONITORING - MSP BACKUP PRODUCT STATUS
Details **Thresholds** Self-Healing

INSTALLATION STATUS

Monitoring:	Off	?
Range:	0	- 255
Normal:	0	- 0
Warning:	1	- 1
Failed:	2	- 255

PRODUCT STATUS

Monitoring:	Default	?
Range:	0	- 255
Normal:	0	- 0
...

Buttons: SAVE CANCEL

STEP 10: CREATE A MONITORING DASHBOARD

Go to **Dashboard -> Manage Dashboards**. Click **ADD** and enter the Dashboard name. We suggest **Cove Data Protection**. Select the filter **Cove Data Protection** and add it to the **Selected Items**.

The screenshot shows the 'ADD DASHBOARD' page in the N-ABLE N-CENTRAL interface. On the left, there's a sidebar with 'Views' (Active Issues, All Devices, Job Status, NetPath, Topology Maps), 'Dashboards' (Backup devices, Device - ESX Hosts, Device - MSP Backup, Device - Network Devices, Device - Printers, Device - Servers, Device - Workstations, Intune Compliance, Manage - Antivirus, Manage - EDR, Manage - EDRs, Manage - Patch Status, N-Able Backup, Manage Dashboards), 'Actions', 'Reports', 'My Links', and 'Configuration'. The main area has tabs for 'Devices to Target' (selected) and 'Monitoring Options'. Below these are sections for 'FILTERS' and 'Available Items'. In the 'FILTERS' section, under 'Selected Items', 'Cove Data Protection' is listed. The 'Available Items' list includes: *Chrome Install*, 3rd party Disk Encryption, Africa Industries - HQ Devices, Agent Check-in greater than 30 day, Agent Check-in greater than 90 days, Agent Status Normal, aggressive monitoring devices, appUsageCheck_useSchTask, and AV Defender Enabled Devices. At the bottom are 'SAVE' and 'CANCEL' buttons.

STEP 11: CONFIGURE MONITORING OPTIONS

Go to the tab **Monitoring Options**. Select the **N-able Backup Product Status** and **N-able Backup Status** and add it to the **Selected Items**. Click **SAVE**.

The screenshot shows the 'Edit Dashboard' screen in the N-able N-Central interface. The 'Monitoring Options' tab is active. On the right, under the 'SERVICES' section, there are two columns: 'Available Items' and 'Selected Items'. The 'Available Items' column lists various monitoring services. Two specific items, 'N-able Backup Product Status' and 'N-able Backup Status', are highlighted in the 'Selected Items' column. Below these items are four buttons: '>>' (move all available items to selected), '>' (move selected item to selected), '<' (move selected item to available), and '<<' (move all selected items to available). At the bottom of the screen are 'SAVE' and 'CANCEL' buttons.

STEP 12: CHECK DASHBOARD

Go to **Dashboards** -> **Cove Data Protection**. Your devices with Cove Data Protectionw should appear, with the correct status behind it.

The screenshot shows the N-ABLE N-CENTRAL interface with the 'COVE DATA PROTECTION' dashboard selected. The left sidebar contains navigation links for Views, Dashboards, Actions, Reports, My Links, and Configuration. The main content area displays a table of devices with columns for Customer, Site, Remote Control, Tools, Device Name, MSP Backup, and MSP Backup Selected Status. The table lists various devices across different regions, each with a status indicator. At the bottom of the dashboard, there are refresh controls and a total count of 13 devices.

Customer	Site	Remote Control	Tools	Device Name	MSP Backup	MSP Backup Selected Status
Asian Pacific T...	--	[Icon]	[Icon]	10-CJU	[Icon]	[Icon]
European Soft...	--	[Icon]	[Icon]	Windows10-Bram	[Green Check]	[Green Check]
European Soft...	--	[Icon]	[Icon]	2016-DME	[Green Check]	[Green Check]
European Soft...	--	[Icon]	[Icon]	2016-BRU	[Green Check]	[Green Check]
Africa Industri...	--	[Icon]	[Icon]	2016-ATL	[Green Check]	[Green Check]
Africa Industri...	--	[Icon]	[Icon]	2012R2-JED	[Green Check]	[Green Check]
Africa Industri...	--	[Icon]	[Icon]	2012R2-DXB	[Green Check]	[Green Check]
European Soft...	--	[Icon]	[Icon]	2012R2-BOG	[Green Check]	[Green Check]
European Soft...	--	[Icon]	[Icon]	2008R2-TXL	[Green Check]	[Green Check]
Africa Industri...	--	[Icon]	[Icon]	2012R2-PEK	[Grey]	[Grey]
Africa Industri...	--	[Icon]	[Icon]	2008R2-MEX	[Grey]	[Grey]
Africa Industri...	--	[Icon]	[Icon]	2008R2-JNB	[Grey]	[Grey]
Africa Industri...	--	[Icon]	[Icon]	2008R2-GRU	[Grey]	[Grey]

SUMMARY

After finalizing this guide, you've uploaded the Automation Policy and executed the automatic deployment and configuration. In the N-Central dashboard, a daily check for the Backups is also added.

We advise to use the portal at <https://backup.management> for further configuration changes, such as fine tuning the profiles. For daily management we also advice to use that portal, it gives you a highly detailed view of all of your backups and (automated) restores in one view. If you'd like additional help in setting that up, please reach out to us.