



NWC OT Cybersecurity Network Devices Minimum Baseline Security Standard Appendix

National Water Company (NWC), KSA
SCADA/OT Information Security Implementation Project

Document Number: A01001045-MBSS-ND-APP
Document Title: NWC OT Cybersecurity Network Devices Minimum Baseline Security Standards
Document Version: 0
NWC Contract No.: 101200487
[atm] PO Ref.: ATMPO2020-034

NOTES AND COPYRIGHTS

The information contained in this document is confidential, privileged, and only for the intended recipient's information and may not be used, published, or redistributed without the prior written consent of ACET Solutions LLC. This document contains confidential, sensitive information of National Water Company (NWC).

Information contained herein is for the sole use of the customer (NWC) receiving this document. Acceptance of the document by the customer constitutes agreement by the customer & ACET Solutions that either party shall not disclose confidential information to any third party and shall not transmit any documents or copies thereof containing confidential information to any third party except as may be authorized in writing by NWC & ACET Solutions.

NWC has contracted this project to [atm] under contract number 101200487. ACET Solutions is the technical consultant of [atm] responsible for planning and execution of this project. All references to ACET Solutions in this document should be construed as [atm]/ACET Solutions for contractual purpose. Acceptance of this deliverable by NWC shall meet the requirements of the respective deliverable under NWC contract number 101200487.

No part of this document may be used, translated into another language, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written approval from ACET Solutions.

Questions or comment regarding this deliverable should be directed to the ACET Solutions Project Director.

ACET Solutions LLC
1400 Broadfield Blvd Suite 200
Houston TX, 77084
Email: sales@acetsolutions.com | URL: www.acetsolutions.com

APPROVALS

Name	Company	Signature	Date
Mubarik Mustafa (Project Director)	ACET Solutions		
Abdulhadi G. Alshammari (Project Manager)	NWC		
Ahmed I. Almutairi (Project Sponsor)	NWC		

REVISION HISTORY

Rev No.	Date	Author	Checked By	Approved By	Comments
00	16 February 2022	AMS	SK	MM	

Table of Contents

Appendix I - Cisco	5
Appendix II - Palo Alto.....	7
Appendix III - Nozomi.....	9

APPENDIX I - CISCO

For procedure to apply security baseline standards on Cisco switches refer to the following commands:

1. Setting user and password:

```
configure terminal
  enable secret XXX          (replace XXX with password)
  user XX secret XXX         (replace XX with user name and XXX with password)
```

Figure 1 creating user and password commands

2. Setting device host-name:

```
configure terminal
  hostname XX                (replace XX with host-name)
```

Figure 2 setting device host-name

3. Disabling ports:

```
configure terminal
  interface range gig 1/0/X-X (replace X with port number or X-X with range)
  description "XX"           (replace XX with descriptive text)
  shutdown
  exit
```

Figure 3 port disabling commands

4. Enabling ssh v2:

```
configure terminal
  crypto key generate rsa modulus 1024
  ip ssh version 2
  ip ssh time-out XX          (replace XX with idle session time-out time in seconds)
  ip ssh authentication-retries X (replace X with number of retries before lockout)
```

Figure 4 enabling ssh v2 commands

5. Mapping VLANs to physical interfaces:

```
configure terminal
  interface range gig 1/0/X-X (replace X with port number or X-X with range)
  switchport mode access
  switchport access vlan X     (replace X with the vland id)
  no shut
  exit
```

Figure 5 mapping VLANs commands

6. Setting up NTP server:

```
configure terminal
  set ntp server XXX.XXX.XXX.XXX (replace XXX.XXX.XXX.XXX with the NTP server's IP)
  set ntp client enable
```

Figure 6 setting up NTP server commands

7. Enabling Time Stamps on logs:

```
configure terminal
service timestamps log datetime [msec] [localtime] [show-timezone]
```

Figure 7 enabling time-stamps on logs command

APPENDIX II - PALO ALTO

For procedure to apply security baseline standards on Palo Alto Firewalls through Panorama refer to the following steps:

Creating Zones:

Step 1: Log in to Panorama Web Interface.

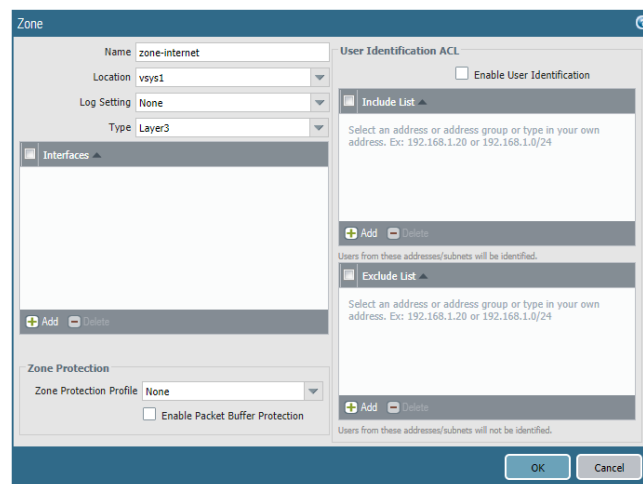
Step 2: Select **Network > Zones** and in the Template context drop-down, select the network template you previously created.

Step 3: **Add** a new zone.

Step 4: Enter zone-internet, for example, as the Name of the zone.

Step 5: For zone **Type**, select **Layer3**.

Step 6: Click **OK**.



Step 7: Repeat the previous steps to create the remaining zones. In total, you must create the following zones:

- zone-to-branch
- zone-to-hub
- zone-internal
- zone-internet

Step 8: **Commit** and **Commit and Push** your configuration changes.

Step 9: **Commit** your changes.

Configuring NTP:

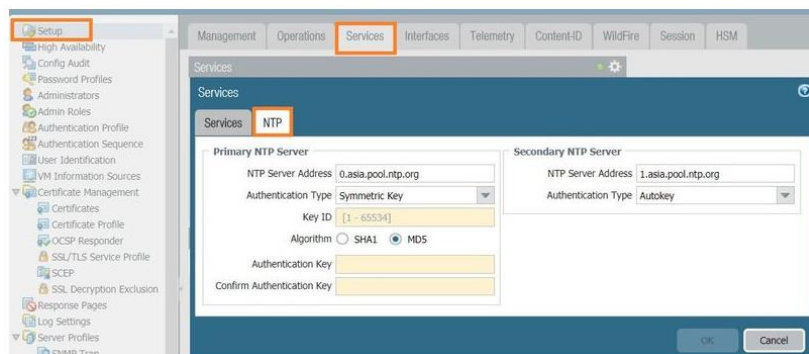
Step 1: Go to Device > Setup > Services and select the NTP tab.

Step 2: In the NTP Server Address field, enter the IP address or hostname of a NTP server.

Step 3: In the Authentication Type field, select one of the following:

- None (default). This option disables NTP authentication.
- Symmetric Key. This option uses symmetric key exchange, which are shared secrets. Enter the key ID, algorithm, authentication key, and confirm the authentication key.
- Autokey. This option uses auto key, or public key cryptography.

Step 4: Commit.

**Configuring Static Routes:**

Step 1: Select Network > Virtual Router and select the virtual router you are configuring, such as default.

Step 2: Select the Static Routes tab.

Step 3: Select IPv4 or IPv6, depending on the type of static route you want to configure.

Step 4: Add a Name for the route.

Step 5: For Destination, enter the route and netmask (for example, 192.168.2.2/24 for an IPv4 address or 2001:db8:123:1::1/64 for an IPv6 address). If you're creating a default route, enter the default route (0.0.0.0/0 for an IPv4 address or ::/0 for an IPv6 address).

Alternatively, you can create an address object of type IP Netmask.

Step 6: Enter an Admin Distance for the route to override the default administrative distance set for static routes for this virtual router (range is 10 to 240; default is 10).

Step 7: Enter a Metric for the route (range is 1 to 65,535).

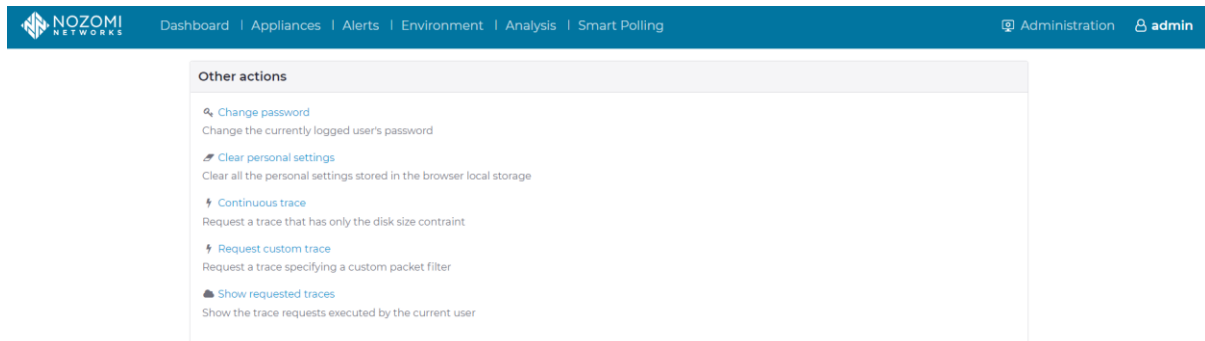
For further information refer to the document "Attachment 1-Panorama CCECG".

APPENDIX III - NOZOMI

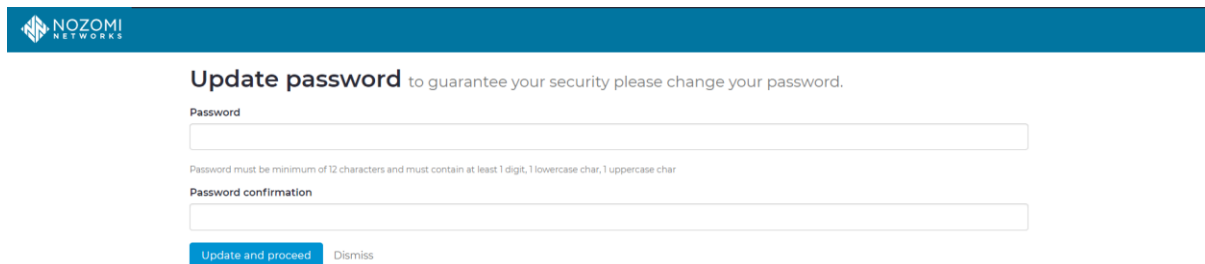
For procedure to apply security baseline standards on Nozomi Guardian refer to document

1. Changing default admin user password:

Admin > Others



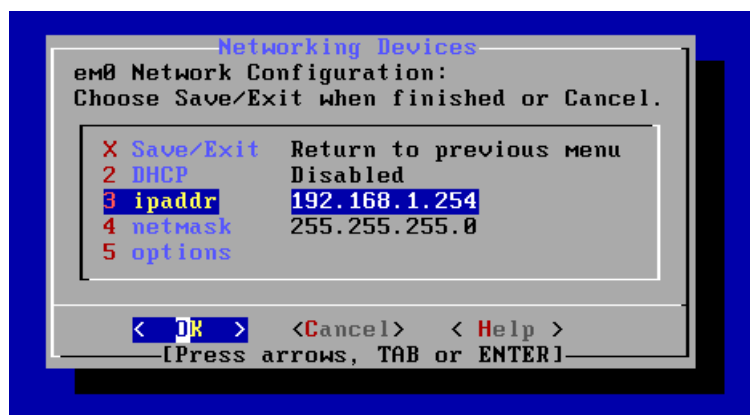
Change Password



The screenshot shows the 'Update password' form. The title is 'Update password to guarantee your security please change your password.' The form has two input fields: 'Password' and 'Password confirmation'. Below the 'Password' field, a note states: 'Password must be minimum of 12 characters and must contain at least 1 digit, 1 lowercase char, 1 uppercase char'. At the bottom of the form, there are two buttons: 'Update and proceed' and 'Dismiss'.

2. Change Default IP Address:

Access the Command Line Interface (CLI). Enter privileged mode (using the command "enable-me") and launch the configuration wizard (using the command "setup"). A dialog box will appear, select "Network Interfaces", then "em0", the following dialogue box will appear. The IP address can be changed under "ipaddr".



3. For further details refer to the document "Attachment 2-N2OS-UserManual".



ACET Solutions LLC

1400 Broadfield Blvd Suite 200 Houston TX, 77084.
United States of America.

Tel: +1 832 386 5593 | Fax: +1 832 201 0337

sales@acetsolutions.com | www.acetsolutions.com