



NWC OT Cybersecurity Endpoint Protection Management Detailed-Level Design

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



Document Number: A01001045-DLD-EP
Document Title: NWC OT Cybersecurity Endpoint Protection Management Detailed-Level Design
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
0	11-Feb-2021	RAS	NR/SK	MM	Issued for Approval

GLOSSARY

Acronyms	Meaning
AD	Active Directory
ADC	Additional Domain Controller
ATM	Advance System and Technology
ATP	Adaptive Threat Protection
BU	Business Unit
DLDD	Detailed-Level Design Document
DMZ	Demilitarized Zone
DNS	Domain Name System
ECC	Essential Cybersecurity Controls
ePO	ePolicy Orchestrator
EP	Endpoint Protection
FTP	File Transfer Protocol
GB	Giga Byte
HCIS	High Commission for Industrial Security
HDD	Hard Disk Drive
HLD	High Level Design
HMI	Human Machine Interface
HTTP	Hypertext Transfer Protocol
HSE	Health, Safety, And Environmental
ICS	Industrial Control System
IDS	Intrusion detection System
IPS	Intrusion Prevention System
ISA	International Society of Automation
IT	Information Technology
JCBU	Jeddah Central Business Unit
KSA	Kingdom of Saudi Arabia
MCBU	Makkah Central Business Unit
MDCBU	Madinah Central Business Unit
MGMT	Management
NCA	National Cybersecurity Authority
NERC	North American Electric Reliability Corporation
NIST	U.S. National Institute of Standards and Technology
NWC	National Water Company
OT	Operational Technology
PDC	Primary Domain Controller
PS	Pumping Station
SA	Super-Agent
SCADA	Supervisory Control and Data Acquisition
TCP	Transmission Control Protocol
VM	Virtual Machine

REFERENCE DOCUMENTS

S/N	Document No.	Title
1	A01001045-HLD.00	NWC OT Cybersecurity High-Level Design
2	ECC – 1: 2018	KSA NCA Essential Cybersecurity Controls (ECC – 1: 2018)
3	ISA-62443-1-1 (99.01.01)–2007	Security for Industrial Automation and Control Systems Part 1-1: Terminology, Concepts, and Models
4	A01001045-INV.00	NWC SCADA Asset Inventory
5	A01001045-DLD-EP-App1	Appendix A

Table of Contents

1. Document Purpose	8
2. EPP Design Architecture	8
3. Detailed Design	9
3.1 ePO Server Configuration.....	9
3.1.1 IT ePO	9
3.1.2 OT ePO.....	9
3.1.3 Super Agents	11
3.2 Users Configurations	12
3.2.1 FTP Users Accounts.....	12
3.3 Ports Configurition.....	12
3.3.1 IT ePO – OT ePO Server Communication Ports.....	12
3.3.2 Client server Communication Ports.....	12
3.3.3 SQL Server Communication	13
3.4 Policies	14
3.5 Wonderware Excluded Folders.....	14

List of Figures

Figure 1: EPP DLD Architecture.....	8
Figure 2: Distributed Repository IT.....	9
Figure 3: Source site.....	10
Figure 4: Master Repository.....	10
Figure 5: Distributed Repositories SA	11
Figure 6: Repositories sequence.....	11
Figure 7: Distributed Repositories Accounts.....	12

List of Tables

Table 1: Server-Server Communication Ports	12
Table 2: Client Server Communication Ports.....	13
Table 3: SQL Server Ports.....	13

1. DOCUMENT PURPOSE

This document details the design of Endpoint Protection of NWC. The Endpoint Protection for NWC is provided using McAfee EP software. The document explains what is implemented or configured at each level. The document also explains the data flow and policies configured on endpoints.

2. EPP DESIGN ARCHITECTURE

It's a tiered based design where an ePO Server is deployed at Enterprise Level, another ePO Server at DMZ and Super-Agents at BU level. The below diagram shows the EP Design of NWC.

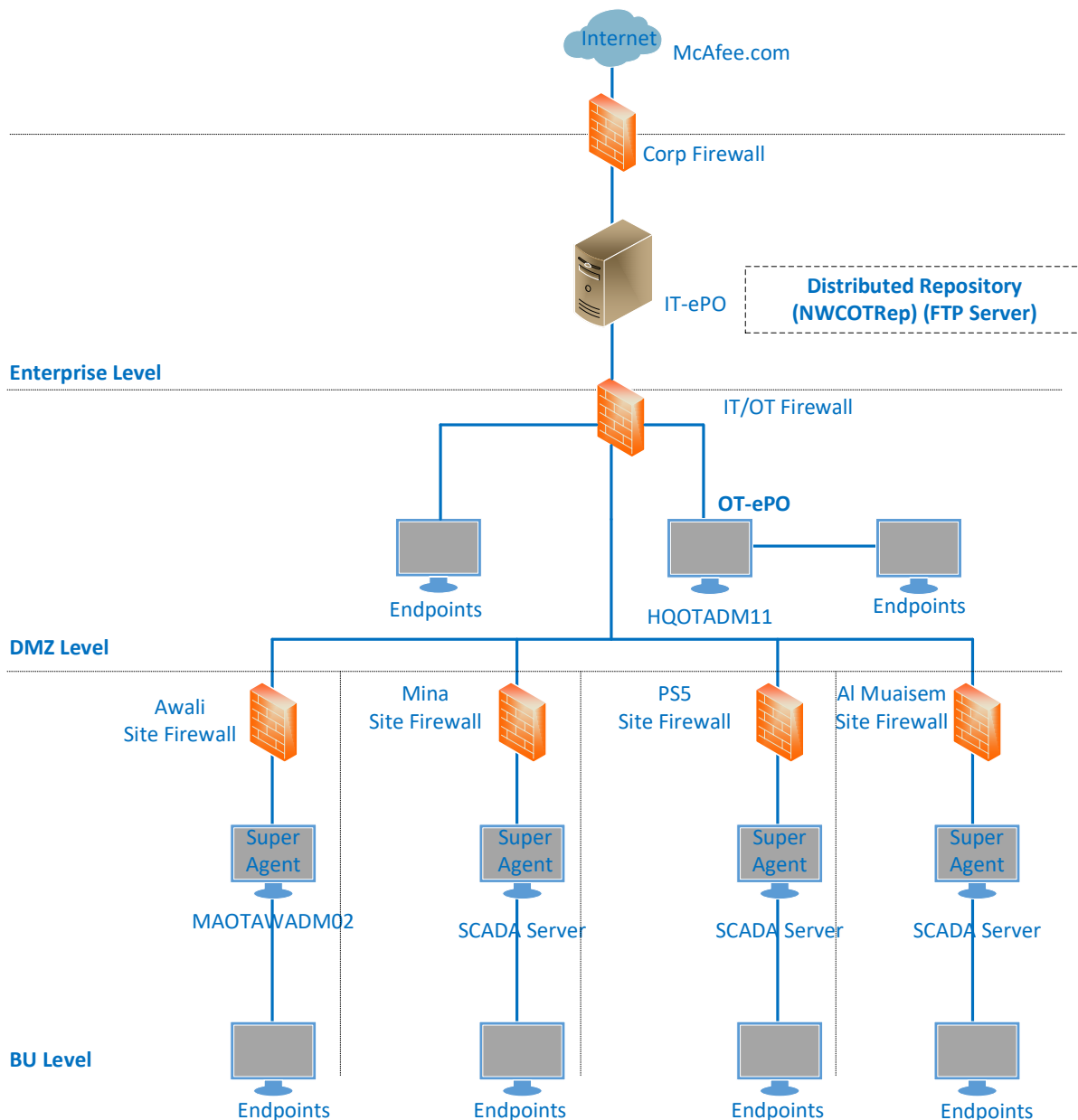


Figure 1: EPP DLD Architecture

The ePO Server at Enterprise level is configured to get updates from internet. Another ePO Server is configured on HQOTADM11 in OT-DMZ and will get updates from the distributed repository at enterprise level via IT/OT firewall. Super Agents are deployed on sites on BU level and all endpoints will take their updates from these super-agents. ePO Agents are deployed on endpoints in OT-DMZ, OT-Domain, BU level and will be managed by OT-ePO server.

3. DETAILED DESIGN

The ePO Server at Enterprise level is connected to internet and get updates from mcafee.com.

The ePO Server at DMZ gets its updates from a distributed repository in IT-ePO at Enterprise level. And the Super-Agents at BU level get their updates from OT-ePO at DMZ level.

3.1 EPO SERVER CONFIGURATION

3.1.1 IT EPO

The ePO Server at Enterprise level is configured to get updates from mcafee.com and replicate them to a distributed repository NWCOTRep. This repository is accessible to OT-ePO using FTP. Local FTP Server on IT-ePO will be created and updates will be manually pulled by OT ePO Server using FTP.

Refer to document “A01001045-DLD-EP-APP1.00” for details of the packages being copied to the distributed repository.

The below picture shows an example of configurations.

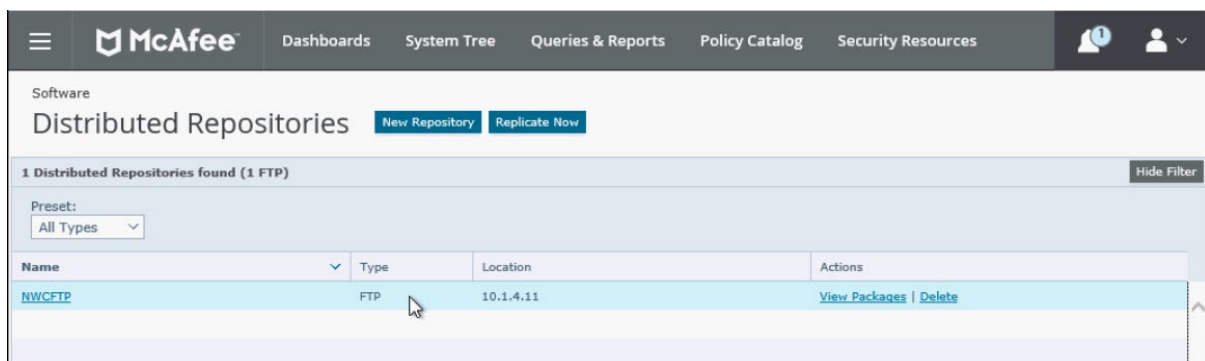


Figure 2: Distributed Repository IT

3.1.2 OT EPO

Assets in OT-Domain Zone, DMZ, and BU level are centrally managed by OT-ePO in HQOTADM11 with following configurations:

Component	Configurations
VM name	HQOTADM11
Processor	6 cores
HDD-1	100 GB
HDD-2	800 GB
Memory	12 GB

- On ePO Server at HQOTADM11, a new Source Site NWCOTRep is defined and configured to point to the distributed repository available in IT-ePO.
- Required updates are then pulled manually from this source site NWCOTRep to master repository via FTP.
- And then these updates are manually replicated to other Super-Agents distributed repositories at BU level. Endpoints take their update contents from Super Agents at BU level.

The following client packages and extensions are configured on HQOTADM11 and will be installed on managed clients:

- McAfee Endpoint Security
- McAfee Adaptive Threat Protection
- McAfee Threat Prevention

Policies for endpoints are configured on HQOTADM11. Refer to section 3.7 for details.

The below picture shows an example of configurations.

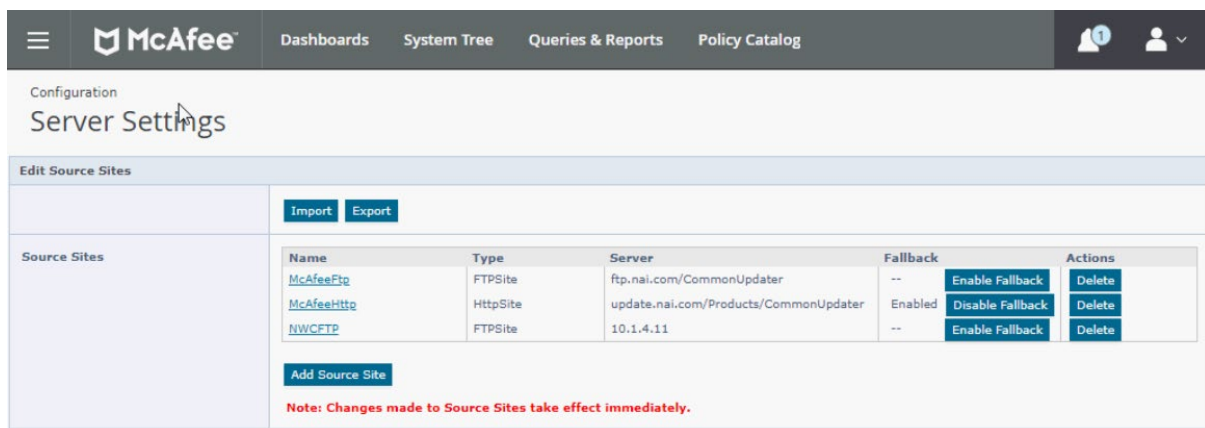


Figure 3: Source site

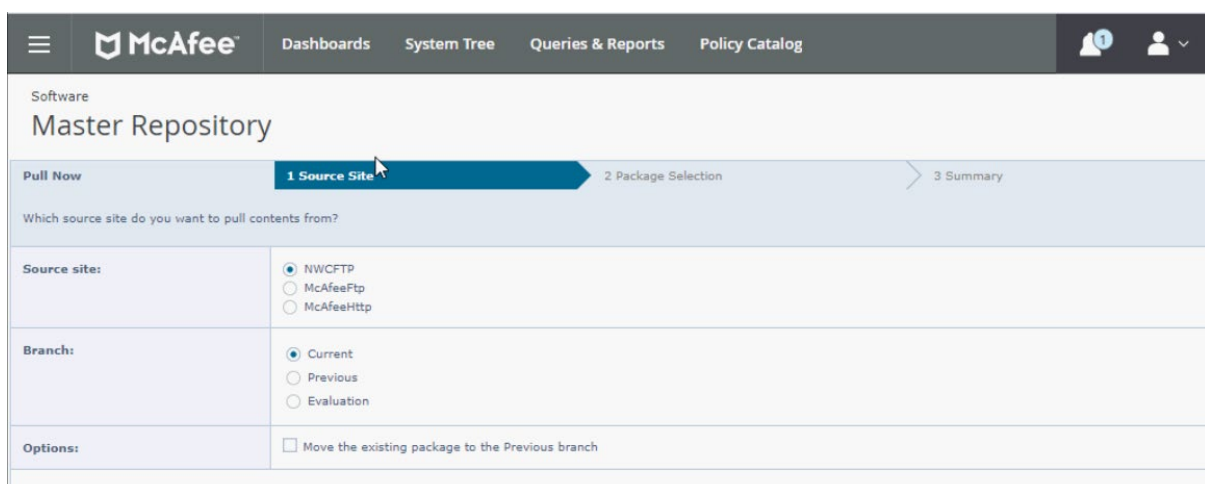


Figure 4: Master Repository

3.1.3 SUPER AGENTS

Assets in Awali, Mina, P5, and AI Muaisem take their updates from Super-Agents configured at each site. Updates are replicated to these Super-Agents by HQOTADM11.

A Super-Agent is configured in MAOTAWADM02 in Awali, SCADA Server in Mina, SCADA Server in PS5 and SCADA Server in AI Muaisem.

The below picture shows an example of configurations.

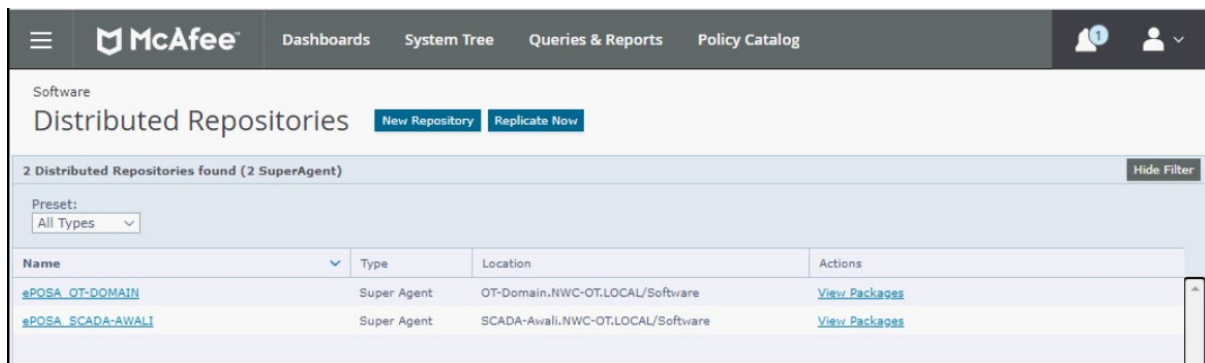


Figure 5: Distributed Repositories SA

Assets will take their updates from OT-ePO if none of the super agents is active.

The below picture shows an example of configurations.

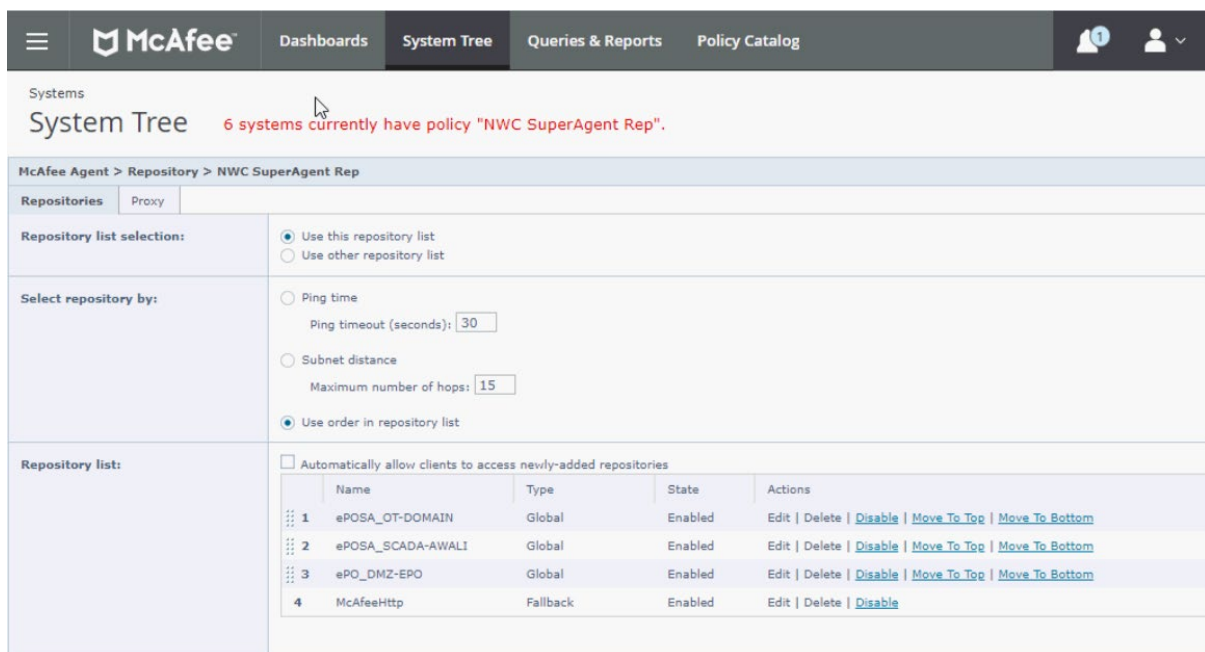


Figure 6: Repositories sequence

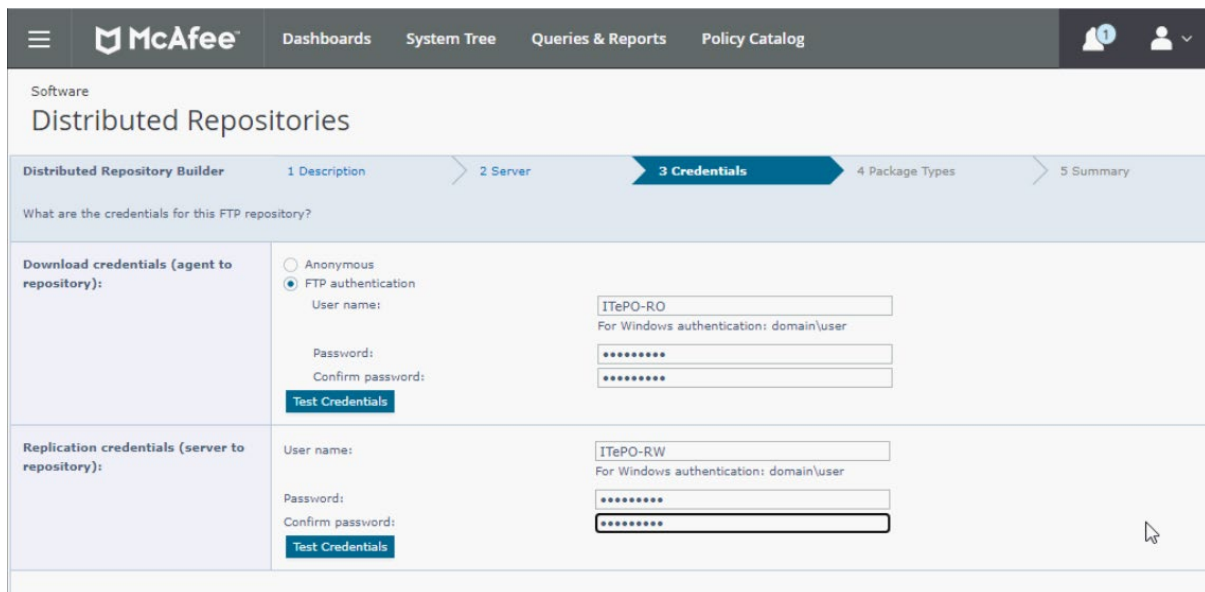
3.2 USERS CONFIGURATIONS

3.2.1 FTP USERS ACCOUNTS

A user OTePO-RO with read only permissions will be configured in IT AD at Enterprise level, this user is configured in OT-ePO to download contents of distributed repositories from IT ePO.

A user ITePO-RW with read-write permissions will be configured in IT AD at Enterprise level, this user will be configured in IT-ePO to synch contents of distributed repository to FTP location.

For FTP, enter domain user account information.



The screenshot shows the McAfee Distributed Repositories configuration page. The breadcrumb trail is: Distributed Repository Builder > 1 Description > 2 Server > 3 Credentials > 4 Package Types > 5 Summary. The current step is '3 Credentials', which asks 'What are the credentials for this FTP repository?'. There are two sections: 'Download credentials (agent to repository):' and 'Replication credentials (server to repository):'. Both sections have radio buttons for 'Anonymous' and 'FTP authentication'. The 'FTP authentication' option is selected. For each section, there are input fields for 'User name', 'Password', and 'Confirm password'. The 'User name' field is pre-filled with 'ITePO-RO' for download and 'ITePO-RW' for replication. Below the password fields are 'Test Credentials' buttons. A mouse cursor is visible at the bottom right.

Figure 7: Distributed Repositories Accounts

3.3 PORTS CONFIGURATION

The following sections describe the details of port configurations.

3.3.1 IT EPO – OT EPO SERVER COMMUNICATION PORTS

Port	Default Value	Description
Server-server FTP communication port	21	Used to pull contents of distributed repository

Table 1: Server-Server Communication Ports

3.3.2 CLIENT SERVER COMMUNICATION PORTS

Port	Default Value	Description
Agent-server communication port	80	TCP port that the McAfee ePO server service uses to receive requests from agents.

Port	Default Value	Description
Agent-server communication secure port	443	TCP port that the McAfee ePO server service uses to receive requests from agents and Remote Agent Handlers. TCP port that the McAfee ePO server's Software Manager uses to connect to McAfee. TCP port that the McAfee ePO server uses to connect to the McAfee software updates server (s-download.mcafee.com), McAfee license server (lc.mcafee.com), and McAfee Product Compatibility List (epo.mcafee.com).
Agent wake-up communication port	8081	TCP port that agents use to receive agent wake-up requests from the McAfee ePO server or Agent Handler. TCP port that the Super-Agents configured as repositories that are used to receive content from the McAfee ePO server during repository replication, and to serve content to client systems.
Agent broadcast communication port	8082	UDP port that the Super-Agents use to forward messages from the ePO server/Agent Handler.
Console-to-application server communication port	8443	TCP port that the ePO Application Server service uses to allow web browser UI access.
Client-to-server authenticated communication port	8444	TCP Port that the Agent Handler uses to communicate with the McAfee ePO server to get required information (such as LDAP servers).
LDAP Server port	389	TCP port used to retrieve LDAP information from Active Directory servers.
SMB Windows domain controller port	445	TCP port used for ePO console logon when authenticating Active Directory users.
Syslog server port (optional)	6514	Default port for Syslog using TLS: only required if syslog forwarding is configured

Table 2: Client Server Communication Ports

3.3.3 SQL SERVER COMMUNICATION

A dedicated SQL Server Express is configured for McAfee ePO.

Port	Default Value	Description
SQL Server TCP port	1433	TCP port used to communicate with the SQL Server. This port is specified or determined automatically during the setup process.
SQL Server UDP port	1434	UDP port used to request the TCP port that the SQL instance hosting the ePO database is using.

Table 3: SQL Server Ports

3.4 POLICIES

Policies for ePO agents are configured in HQOTADM11. These policies include configurations for Adaptive Threat Protection, Threat Prevention, McAfee Agent and McAfee Firewall for endpoints.

Following Policies will be configured on the endpoints:

- Adaptive Threat Protection
- Threat Prevention
- McAfee Agent
- Endpoint Security Common
- Endpoint Security Firewall
- Endpoint Security Web Control

Refer to Appendix file “A01001045-DLD-EP-APP1.00” for detailed configuration of policies.

3.5 WONDERWARE EXCLUDED FOLDERS

Following Wonderware folders are excluded from any McAfee actions.

64-bit Operating System

- C:\Program Files (x86)\Archestra*.*
- C:\Program Files (x86)\Common files\Archestra*.*
- C:\Program Files (x86)\FactorySuite*. * (may not exist in newer installations)
- C:\Program Files (x86)\Wonderware*.*
- C:\InSQL\Data*.*
- C:\Historian\Data*.*
- C:\ProgramData\Archestra *.*



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