



# Authenticated Scanning

VULNERABILITY MANAGEMENT

# Authenticated Scanning

- Firewalls, intrusion protection systems, and other security devices can prevent some details of a scan from being successful
- Using an authenticated scan can overcome this issue
- Provide the scanner read-only access to the servers
- Scanner can access the operating system, databases, and applications on the server



# Nessus Authenticated Scanning

Nessus

Policies Reports Mobile Scans Policies Users Configuration

**+ Add Policy**

Credential Type Windows credentials

General

Credentials

Plugins

Preferences

SMB account :

SMB password :

SMB domain (optional) :

SMB password type : Password

Additional SMB account (1) :

Additional SMB password (1) :

Additional SMB domain (optional) (1) :

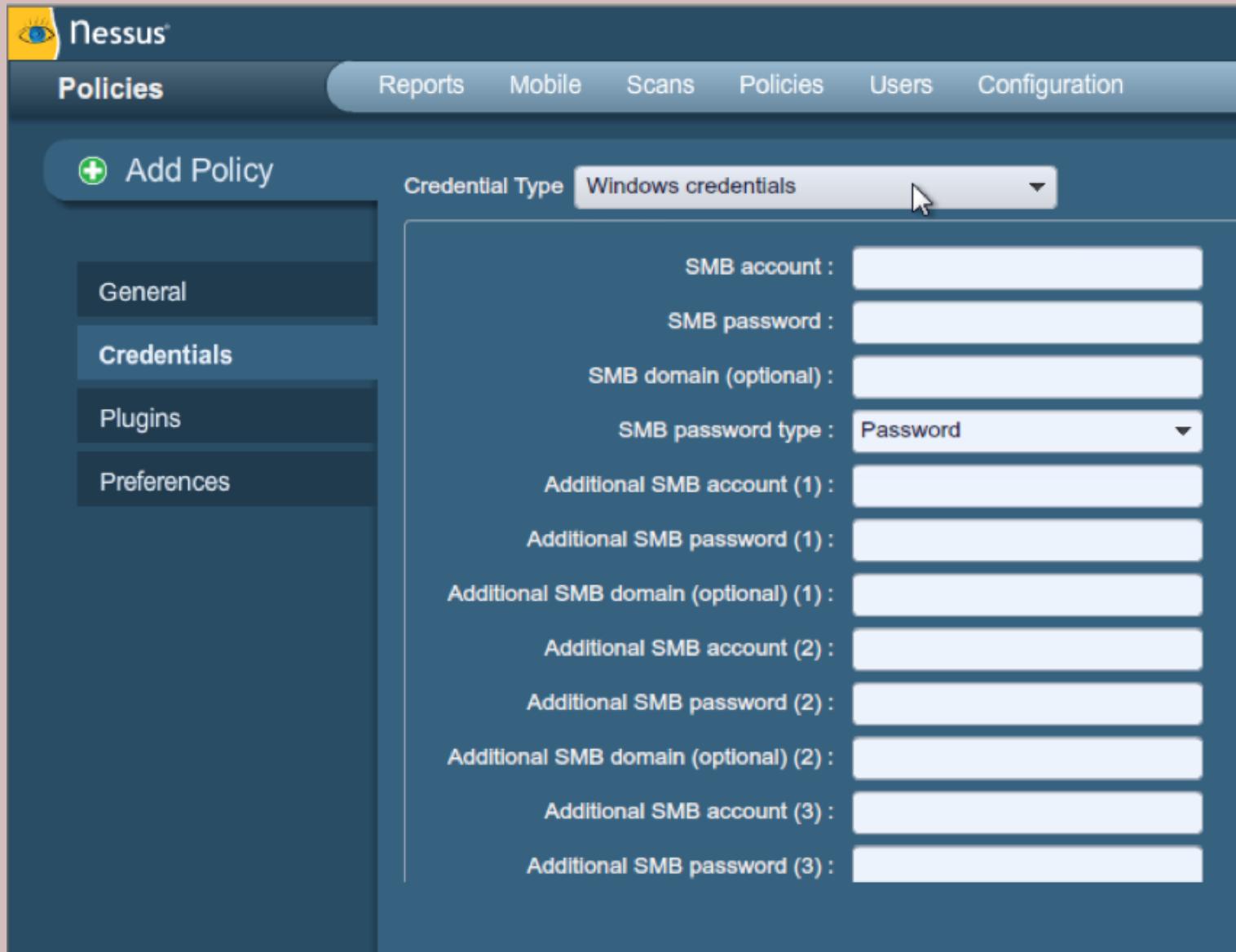
Additional SMB account (2) :

Additional SMB password (2) :

Additional SMB domain (optional) (2) :

Additional SMB account (3) :

Additional SMB password (3) :



# QualysGuard Authenticated Scanning

Vault Title >

**Login Credentials** >

Comments >

**Login Credentials**

Provide information and credentials to access to the Thycotic Secret Server.

URL: \*

User Name: \*

Password: \*

Confirm Password:

Domain:

**Cancel**

**Save**



# Agent-based Scanning

- Small software agents installed on your server or clients
- Provides an “inside-out” perspective of vulnerabilities on the server or client
- Agent-based approaches require more resources on the server and often system administrators fight against their installation

