Managing WiseMo Remote Control Using Windows Active Directory

0.0 Table of Contents

0.0 Table of Contents 1

1.0 Introduction 2

1.1 Prerequisites 2

1.2 Overview 2

2.0 Guest-side integration with Active Directory 3

3.0 Host-side integration with Active Directory 5

3.1 Creating Host configuration template files 5

3.2 Retriving the Host licensing file 8

4.0 Deploying and Configuring the WiseMo Host Using Active Directory Group Policy 9

Step 1: Prepare a Software Distribution Share 9

Step 2: Define the Target Computer Group 9

Step 3: Create and Scope the Group Policy Object 9

Step 4: Install the WiseMo Host via MSI 10

Step 5: Distribute the Host Configuration File 10

Step 6: Distribute the Host License File 11

Step 7: Restart the WiseMo Host Service 12

Result 12

5.0 Updating the WiseMo Host When a New Version Is Released 13

Key Principle 13

Step 1: Prepare the New MSI Package 13

Step 2: Update the Existing GPO Package 13

Step 3: Deployment Behavior 14

Step 4: Configuration and license File Compatibility 14

Rollback Considerations 14

Summary 15

6.0 Handling User and Computer Lifecycle Changes 15

6.1 When a New User Joins the Company 15

6.2 When a User Leaves the Company 15

6.3 When a New Computer Is Added to the Network 16

6.4 When a Computer Is Removed or Repurposed 16
6.5 Key Advantage 17
7.0 WiseMo Glossary 17

1.0 Introduction

1.1 Prerequisites

This guide assumes a Windows-based environment with an operational **Microsoft Active Directory (AD)** domain. The following prerequisites must be met:

- A Windows Active Directory domain with domain-joined computers
- General knowledge of the WiseMo Remote Desktop Guest and Host modules and associated terminology. Please refer to section *7.0 WiseMo Glossary*.
- One or more **WiseMo Remote Desktop Host** installations on Windows computers joined to the AD domain
- The **WiseMo Remote Desktop Guest** installed on client computers that have network access to the Hosts
- Domain administrator or delegated administrative rights to:
    - Create and manage Active Directory groups
    - Deploy software and configuration files using **Group Policy Objects (GPO)**
    - Manage Windows security group membership
- Direct network connectivity between Guest and Host computers on the local network (LAN/WAN)

No WiseMo servers or cloud-based infrastructure is required for the scenarios described in this guide.

1.2 Overview

WiseMo can be tightly integrated with Windows Active Directory to provide centralized discovery, authentication, and authorization for remote control sessions within a local area network.

The WiseMo Remote Desktop Guest is the module you remote control from and the WiseMo Remote Desktop Host is the module installed on the computer being remote controlled.

On the **Guest side**, WiseMo can enumerate Active Directory groups that contain one or more computers. These groups are presented to the user, and selecting a group reveals the member computers. By creating and maintaining dedicated Active Directory groups, a domain administrator can centrally control which computers are visible and accessible to Guest users—without any WiseMo-specific server configuration.

On the **Host side**, WiseMo can be configured to use **Windows Security Management**, leveraging Active Directory for authentication and authorization. Access control is implemented through predefined Windows security groups mapped to WiseMo security roles. By adding or removing users from these groups, administrators can precisely control which users are allowed to connect to which Hosts.

By relying on existing Active Directory infrastructure, this approach significantly reduces operational and management overhead. No additional servers, databases, or supporting backend services are required, which lowers deployment complexity and eliminates the cost otherwise associated with operating and maintaining extra server components.

This model scales cleanly and remains predictable even as users and computers are added, removed, or reassigned.

Deployment and lifecycle management of the WiseMo Host can also be handled through Active Directory. Using Group Policy, the Host software can be installed, licensed, updated, and reconfigured across multiple computers. Configuration changes—including updated Host configuration files—can be distributed centrally and applied automatically.

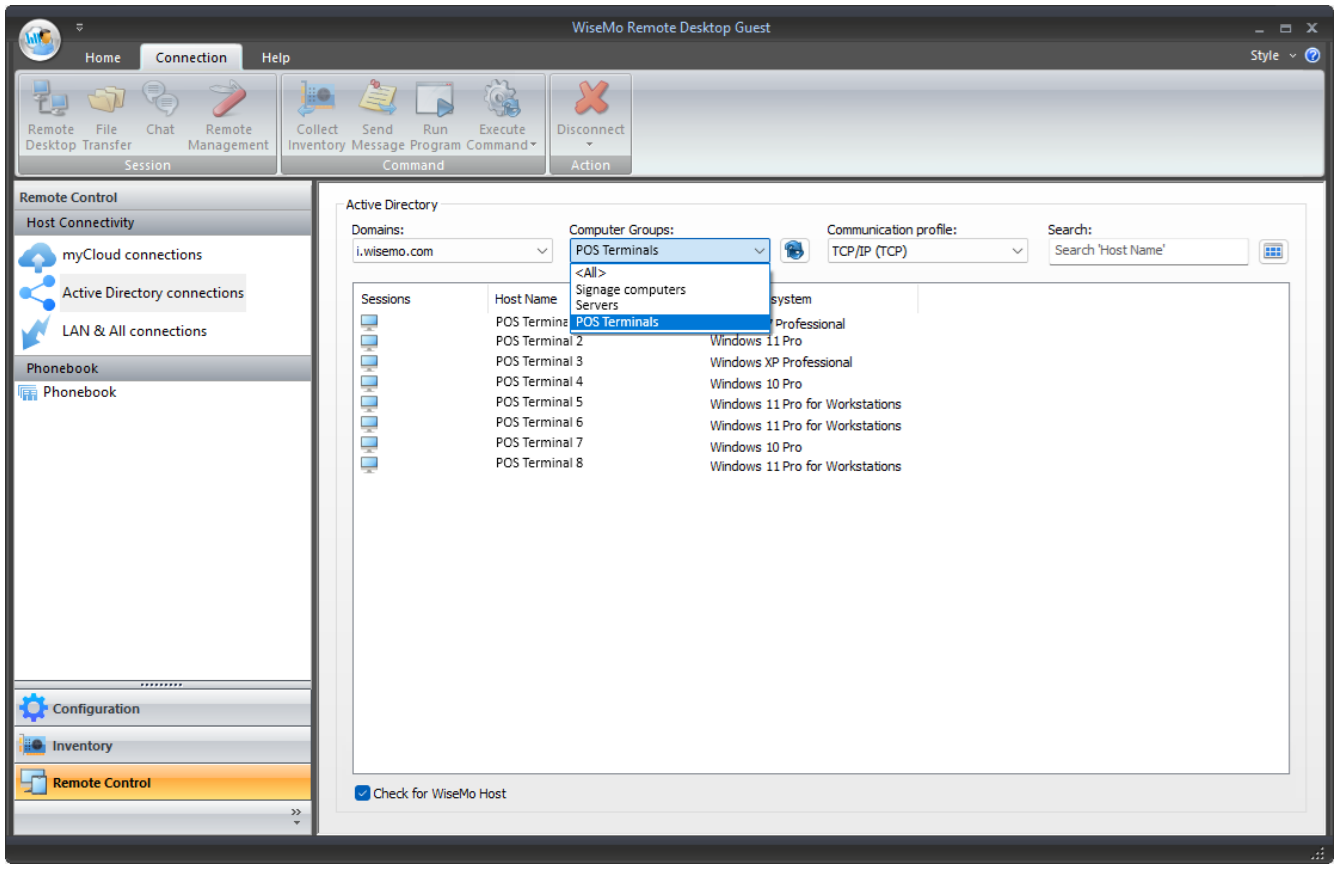
The WiseMo Guest can be deployed and updated in a similar manner using Group Policy. Guest deployment is typically simpler, as it does not involve a background service and therefore does not require service restarts. Guest deployment procedures are not covered in this document.

2.0 Guest-side integration with Active Directory

On the **WiseMo Remote Desktop Guest** side, Active Directory is used to centrally control which computers are visible and available for remote control. A domain administrator creates one or more **Windows Active Directory groups** and assigns the relevant **computer accounts** to these groups. Only groups that contain at least one computer are exposed to the user operating the WiseMo Guest module.

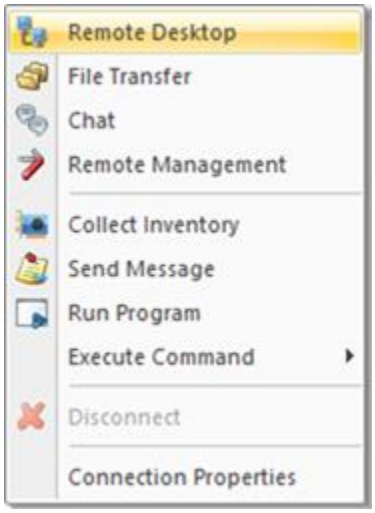
When a Guest user opens the **Active Directory connections** tab, the available domains are listed and can be selected if multiple domains are present. For the selected domain, the WiseMo Guest module displays the Active Directory groups and, when a group is chosen, shows the member computers in a list. From this list, the user can initiate a remote control session directly.

This model allows administrators to organize computers in a way that reflects operational needs. For example, the administrator might create separate groups such as **Signage computers**, **Servers**, and **POS Terminals**, and then add the appropriate computers to each group.

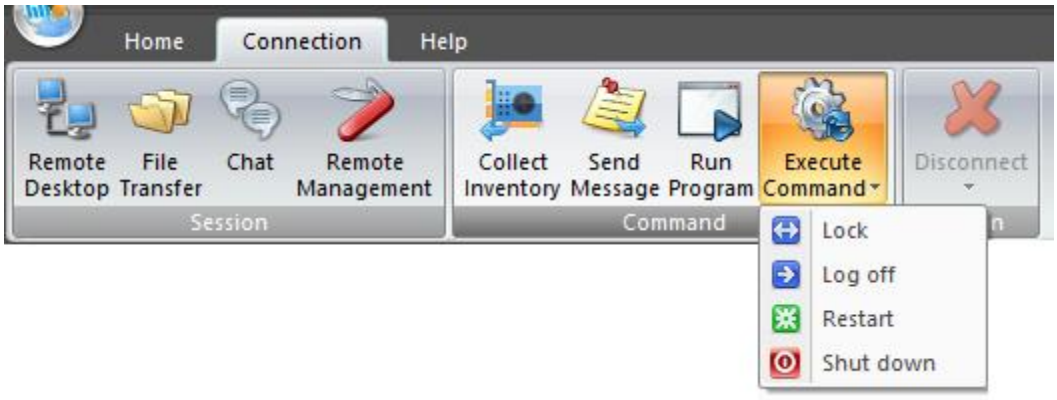


As a result, Guest users see a structured and role-oriented view of available systems, without requiring any manual configuration on the Guest side or the setup of dedicated WiseMo servers.

To initiate a remote control session, the Guest user can **double-click** a computer in the list. Alternatively, the user can **right-click** a computer to access additional session options, desired type of session



or use the **ribbon controls** to start the desired type of session.



3.0 Host-side integration with Active Directory

On the **WiseMo Remote Desktop Host** side, Active Directory can be used for both **authentication and authorization** by configuring the Host to use **Windows Security Management**. This allows access control to be fully managed through standard Windows and Active Directory security groups, without maintaining separate user databases in WiseMo.

3.1 Creating Host configuration template files

Access control on the Host is based on **WiseMo security roles** (such as *Full Access* and *View Only*), to which one or more **Windows security groups** are assigned. When a user connects, the Host evaluates the user's Active Directory group memberships and grants permissions according to the mapped WiseMo role.

As a starting point, the domain administrator should create Groups to suite the required **permission granularity** and **computer roles**. Using the same example as on the Guest side, assume three Host computer types:

- Signage Computers
- Servers
- POS Terminals

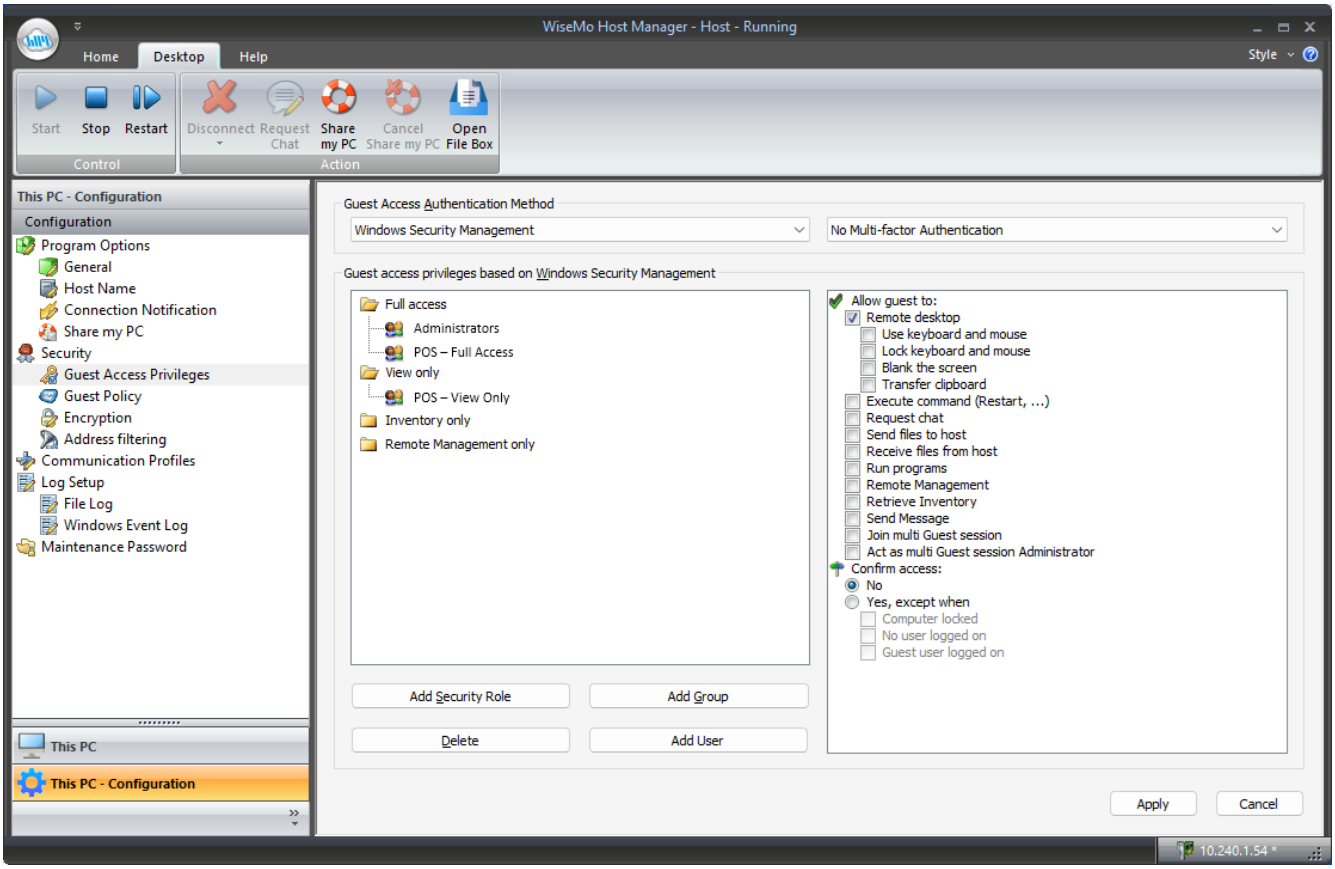
For each computer type, corresponding **Active Directory user groups** can be created to represent access levels, for example:

- POS – Full Access
- POS – View Only
- Servers – Full Access
- Servers – View Only
- Etc.

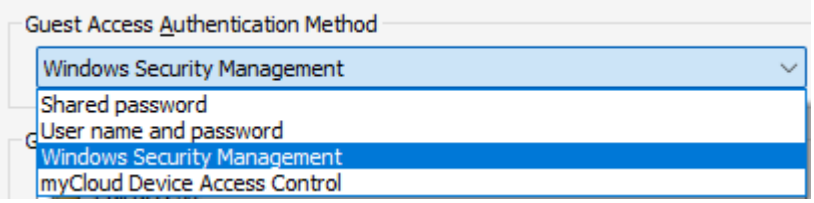
Please note that for the Guest usage we created groups in AD and assigned computers to them. For the Host, we create groups in AD and assign users to them.

On the Host side, create **separate Host configuration template files** for each Host type (for example one for POS terminals, one for servers, and one for signage computers).

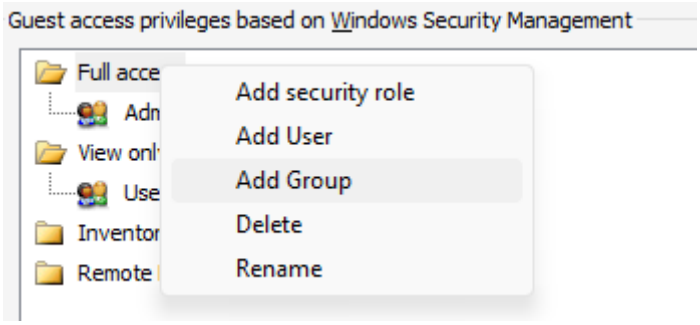
To configure a Host template, open the WiseMo Host Manager and navigate to:
This PC – Configuration > Security > Guest Access Privileges.



In the **Guest Access Authentication Method**, select **Windows Security Management**.



The predefined WiseMo security roles are shown in the left pane. To assign an Active Directory group to a role, right-click the desired role (for example **Full Access**) and select **Add group**.



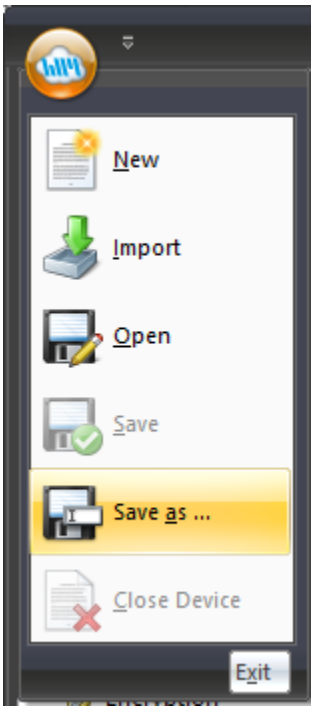
In the Windows group selection dialog, locate the relevant Active Directory group—using **Advanced** and **Find Now** if needed—and select it (for example *POS Terminal Supporters*).

Repeat this process to achieve the desired level of control. For example:

- Add the predefined Windows **Administrators** group to the **Full Access** role
- Add the predefined Windows **Users** group to the **View Only** role

If additional permission sets are required, new **WiseMo security roles** can be created and configured with a custom combination of privileges.

When the role configuration is complete, click **Apply**. Then open the system menu in the upper-left corner of the Host Manager and select **Save as…** to save the configuration as a Host configuration file.



Save the file as for example host_pos.xml.

This file contains the complete Host security configuration and will later be distributed—using Group Policy—to the computers in the corresponding Active Directory computer group (for example the *POS Terminals* group created for Guest-side discovery).

This approach ensures consistent, centrally managed access control across all Hosts, fully aligned with existing Active Directory policies and administrative workflows.

3.2 Retriving the Host licensing file

Proper licensing of the Host module is done via a licensing file store locally on the Host computer. A licensing file must be available on all systems where the Host is installed.

After completing a template Host installation and registering the WiseMo Host with the appropriate license, the license file, host.lic, can be retrieved from the Host installation directory:

%ProgramFiles(x86)%\WiseMo\WiseMo RSM\Remote Desktop Host\

Copy the host.lic file from the template Host installation to a central file share accessible by all target computers. We'll need it for the deloyment.

4.0 Deploying and Configuring the WiseMo Host Using Active Directory Group Policy

Windows Active Directory Group Policy can be used to centrally install, license, configure, and maintain the WiseMo Host on selected computers. This allows administrators to deploy the Host to specific computer groups and to distribute the Host configuration files and license file in a controlled and repeatable manner.

Prerequisites

- The WiseMo Host MSI installer (WsmHost-[version].msi)
- One or more Host configuration files (for example host_pos.xml)
- The Host licensing file (host.lic)
- A Windows file share accessible to all target computers (read access)
- Administrative rights to create and edit Group Policy Objects (GPOs)

Step 1: Prepare a Software Distribution Share

Create a central file share, for example:

\\FILESERVER\Software\WiseMo\

Place the following files in the share:

- WsmHost-[version].msi
- Host configuration files (for example host_pos.xml, host_server.xml)
- Host licensing files (host.lic)

Ensure that **Domain Computers** have **Read** permissions to the share.

Note: MSI packages must always be deployed from a UNC path.

Step 2: Define the Target Computer Group

In Active Directory, create or reuse a **computer group** containing the computers that should receive the WiseMo Host.
For example:

- POS Terminal Computers

Add the relevant computer accounts to this group.

Step 3: Create and Scope the Group Policy Object

1. Open **Group Policy Management**

2. Create a new GPO, for example:

   Deploy WiseMo Host – POS Terminals

3. Link the GPO to the appropriate OU, or use **Security Filtering**:
   - Remove *Authenticated Users*
   - Add the target computer group (for example POS-Terminal-Computers)

This ensures the GPO only applies to the intended computers.

Step 4: Install the WiseMo Host via MSI

1. Edit the GPO
2. Navigate to:

   Computer Configuration

   → Policies

   → Software Settings

   → Software installation
3. Right-click **Software installation** → **New** → **Package**
4. Select the MSI using its UNC path:

   \\FILESERVER\Software\WiseMo\WsmHost-[version].msi
5. Choose **Assigned**

The WiseMo Host will be installed automatically during the next system startup.

Step 5: Distribute the Host Configuration File

The Host configuration file created earlier (for example host_pos.xml) must be copied to the WiseMo Host configuration directory on each target computer.

1. In the same GPO, navigate to:
2. Computer Configuration

   → Preferences

   → Windows Settings

   → Files

3. Create **New → File**
4. Configure the item as follows:
    - **Action**: Update
    - **Source file**:
    - \\FILESERVER\Software\WiseMo\host_pos.xml
    - **Destination file**:
    - %ProgramData%\WiseMo\WiseMo RSM\Remote Desktop Host\host.xml

Using %ProgramData% ensures compatibility across different system drive configurations.

Step 6: Distribute the Host License File

The Host licensing file copied earlier must be copied to the WiseMo Host installation folder directory on each target computer.

1. In the same GPO, navigate to:
2. Computer Configuration
   → Preferences
   → Windows Settings
   → Files
3. Create **New → File**
4. Configure the item as follows:
    - **Action**: Update
    - **Source file**:
    - \\FILESERVER\Software\WiseMo\host.lic
    - **Destination file**:
    - %ProgramFiles(x86)%\WiseMo\WiseMo RSM\Remote Desktop Host\host.lic

Using %ProgramFiles(x86)% ensures compatibility across different system drive configurations.

The Host license key itself can also be applied via the MSI installation command line.

Important Notes

- When using file-based licensing, the host.lic file is not machine-specific and can be distributed to multiple Hosts, subject to the license agreement.

- License distribution should be scoped to the same Active Directory computer groups used for Host deployment.
- If the license file is updated or replaced, it can be redeployed using the same Group Policy mechanism.

Step 7: Restart the WiseMo Host Service

For configuration and licensing to take effect, the WiseMo Host service must be restarted.

The WiseMo Host runs as a Windows service with the following details:

- **Service name**: WsmHostAgent
- **Display name**: WiseMo RSM Host Agent

To restart the service via Group Policy:

1. In the same GPO, navigate to:
2. Computer Configuration

   → Preferences

   → Control Panel Settings

   → Services
3. Create **New → Service**
4. Configure:
   - **Service name**: WsmHostAgent
   - **Action**: Restart service
   - **Startup type**: No change

This ensures the Host loads the configuration after the configuration file has been applied and likewise uses the license applied via the license file.

Result

Repeat this for all computer groups.

With this configuration and licensing in place:

- The WiseMo Host is installed automatically on all computers in the selected AD computer group
- The correct Host configuration file and license file is deployed consistently
- The WiseMo Host service (WsmHostAgent) is restarted to apply configuration changes

- Different Host types (POS terminals, servers, signage computers) can be managed using separate GPOs and configuration files

This approach enables fully centralized deployment, licensing and configuration of the WiseMo Host using standard Active Directory and Group Policy mechanisms, without requiring any manual installation or additional WiseMo infrastructure.

5.0 Updating the WiseMo Host When a New Version Is Released

When a new version of the WiseMo Host is released, it is delivered as a new MSI file with a different filename (for example WsmHost-20.0.2025.286.msi replacing WsmHost-20.0.2025.184.msi). Active Directory Group Policy can be used to upgrade existing installations in a controlled and predictable manner.

Key Principle

Group Policy–based software deployment tracks the **assigned package**, not just the product on disk. To upgrade the WiseMo Host, the existing MSI assignment must be replaced with the new MSI package in the same GPO (or a superseding GPO).

Step 1: Prepare the New MSI Package

1. Copy the new MSI file to the central software distribution share, for example:

   \\FILESERVER\Software\WiseMo\WsmHost-[new-version].msi

2. Do **not** overwrite or rename the old MSI file. Keep previous versions available until the upgrade is complete.

Ensure that **Domain Computers** still have read access to the share.

Step 2: Update the Existing GPO Package

1. Open **Group Policy Management**
2. Edit the GPO used to deploy the WiseMo Host (for example *Deploy WiseMo Host – POS Terminals*)
3. Navigate to:
4. Computer Configuration

   → Policies

   → Software Settings

   → Software installation
5. Right-click the existing WiseMo Host package and select **Properties**
6. Go to the **Upgrades** tab

7. Click **Add…**
8. Select the new MSI package using its UNC path:

   \\FILESERVER\Software\WiseMo\WsmHost-[new-version].msi
9. Choose **Package can upgrade over the existing package**
10. Confirm and close the dialog

This explicitly defines the new MSI as an upgrade of the previously deployed version.

Step 3: Deployment Behavior

After the GPO is updated:

- Existing computers with the WiseMo Host installed will automatically upgrade to the new version
- New computers joining the target AD group will install the **latest version only**
- No manual uninstallation is required

The upgrade will occur at the next system startup (or after a Group Policy refresh, depending on system state).

Step 4: Configuration and license File Compatibility

The Host configuration file (for example host_pos.xml) continues to be deployed via Group Policy Preferences and is **independent of the MSI version**.

If a Host build introduces new configuration options:

- Update the configuration template file accordingly
- Replace the source file in the software share
- The updated file will be copied automatically to all target computers
- The WiseMo Host service (WsmHostAgent) will be restarted as part of the existing GPO configuration

The license file depends on Host version (but not the build number), so if the Host version in the future is updated, a new license file corresponding to the MSI version must be used and distributed similarly.

Rollback Considerations

If a rollback is required:

- Disable or unlink the upgrade GPO
- Reassign the previous MSI package

- Restart affected computers

Because each version is deployed as a separate MSI, rollback follows the same controlled GPO process as the upgrade.

Summary

Using Group Policy–based MSI upgrades ensures that:

- Host updates are centrally managed
- Only targeted computers are affected
- Existing installations are upgraded, not reinstalled
- New computers automatically receive the latest approved version

This approach aligns Host lifecycle management with standard Active Directory and Group Policy practices and avoids manual updates or per-machine intervention.

6.0 Handling User and Computer Lifecycle Changes

By basing discovery, access control, and deployment on Active Directory groups, WiseMo integrates naturally with standard IT lifecycle processes. No WiseMo-specific actions are required when users or computers are added or removed—only normal Active Directory administration.

6.1 When a New User Joins the Company

When a new user starts:

1. Create the user account in Active Directory (as per normal IT procedures).
2. Add the user to the appropriate **Active Directory user groups** that are mapped to WiseMo security roles on the Hosts (for example *POS – Full Access* or *Servers – View Only*).

The user will automatically:

- Be authenticated using Active Directory credentials
- Receive the correct WiseMo permissions based on group membership
- Gain access to the relevant computers in the WiseMo Guest

No changes are required on the Guest or Host systems.

6.2 When a User Leaves the Company

When a user leaves:

- Disable or delete the user account in Active Directory, **or**
- Remove the user from the WiseMo-related Active Directory groups

Access is immediately revoked:

- The user can no longer authenticate
- No further WiseMo configuration changes are required

This ensures that access control remains consistent with corporate security policies.

6.3 When a New Computer Is Added to the Network

When a new computer is introduced (for example a new POS terminal or server):

1. Join the computer to the Active Directory domain.
2. Add the computer account to the appropriate **Active Directory computer group** (for example *POS-Terminal-Computers*).

At the next reboot:

- The Group Policy Object scoped to that group will apply
- The WiseMo Host MSI (WsmHost-[version].msi) will be installed **only on that computer**
- The correct Host configuration file (for example host_pos.xml) and licensing file (host.lic) will be deployed
- The WiseMo Host service (WsmHostAgent) will be started and configured

Existing computers are **not reinstalled**. Group Policy ensures that only computers that do not already have the WiseMo Host installed receive the installation.

6.4 When a Computer Is Removed or Repurposed

If a computer is removed from service or changes role:

- Remove it from the relevant Active Directory computer group
- Optionally move it to a different group if it changes function (for example from POS to Server)

On the next policy refresh:

- The deployment GPO will no longer apply
- The computer will disappear from the WiseMo Guest if it is no longer a member of the relevant group

This keeps discovery, deployment, and access aligned without manual cleanup.

6.5 Key Advantage

By using Active Directory group membership as the single source of truth:

- User onboarding and offboarding follow standard AD processes
- New computers are automatically configured and licensed without affecting existing installations
- No centralized WiseMo servers or databases need to be updated
- Operational overhead is minimized

This model scales cleanly and remains predictable even as users and computers are added, removed, or reassigned.

7.0 WiseMo Glossary

Computer - any Server, Workstation, Desktop, Laptop that runs an operating system supported by the Guest or Host module.

Device - any Smartphone, Tablet, Set-top box, Scanner, or other handheld or un-attended device that runs an operating system supported by the Guest or Host module.

Guest – the module installed on a computer or device, e.g. PC, on an iPad, iPhone, Android device or running from a supported Browser. From the Guest module, a user is able to remote control another device or computer where the Host module is running.

Host – the module installed on the target computer or device that should be remotely controlled from the Guest module. It can for example be a PC, Mac, Smartphone, Tablet, Set-top box, or any other type of device that runs a supported operating system.

Host Manager – also termed Host Configuration Manager. A tool used for configuring a WiseMo Host application. It is installed on a Windows desktop computer and communicates with the Host service.

The Host Manager can also export the configuration file that in turn can be imported on another computer/device or copied directly to the Host configuration folder on the disk.

Communication profile – protocol configuration for the communication between a Guest module and a Host module. Before connecting from a Guest to a Host you should specify on the Guest which communication profile should be used.