bmcsoftware

WHITE PAPER

Best Practices for Configuring PATROL for Microsoft Exchange Servers

Contents

INTRODUCTION

E-mail and messaging applications are mission-critical tools in today's business environments. Business productivity and effective communication require that these applications offer 24X7 availability and perform in real time. Microsoft Exchange is the leading collaboration tool offering mail and messaging capabilities. Now, more than ever, Exchange is being deployed in the most demanding environments including large organizations with thousands of users.

Managing these demanding environments is a challenge. PATROL for Microsoft Exchange Servers can help administrators simplify this challenge. PATROL for Microsoft Exchange Servers is a comprehensive monitoring solution that can help ensure the performance and availability of your mission-critical Microsoft Exchange environment. Once installed and configured, it provides the PATROL Agent with access to Exchange configuration and performance data to

- alert you of critical problems
- perform system recovery
- provide administrative control of the Exchange system

This white paper discusses the account requirements for the latest version of PATROL for Microsoft Exchange Servers 5.0.00.05 to be able to manage your Exchange servers and provides tips for streamlining the product configuration process.

PATROL SECURITY

PATROL provides extensive security options including a security pack for implementing security policy, key database, and support for digital signatures. Security configurations range from simple (FIPS140 Level 0) up to the most secure (FIPS140 Level 4). To best illustrate the minimal security and configuration requirements of PATROL for Microsoft Exchange Servers, the descriptions and examples in this whitepaper assume the simplest security enforcement level.

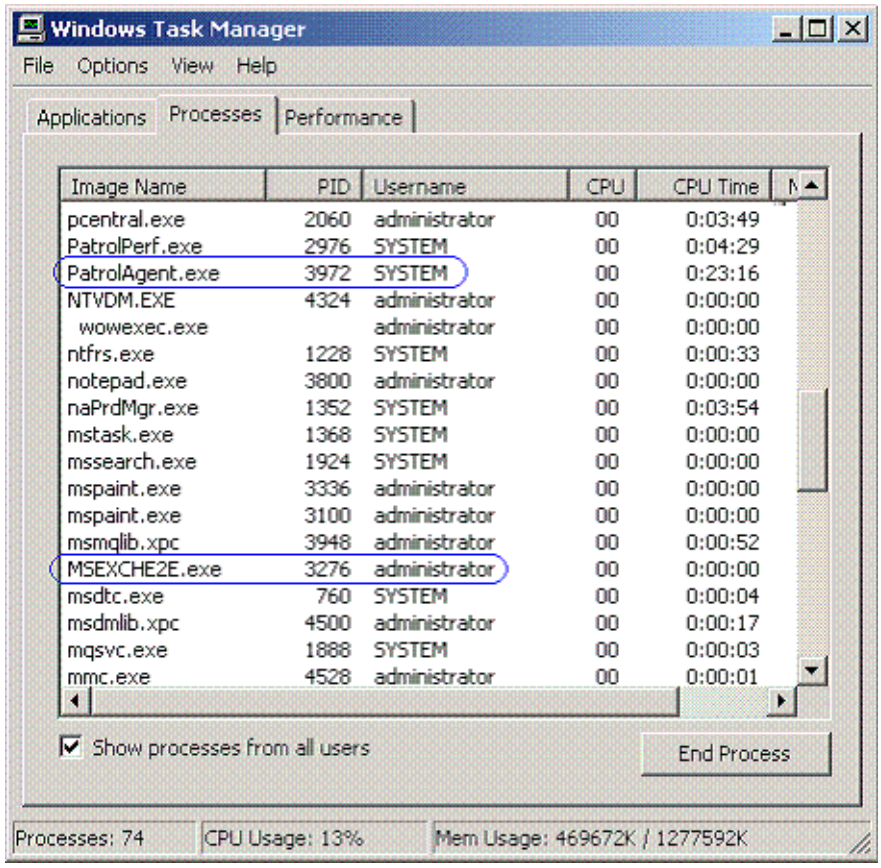
The PATROL Agent (**PatrolAgent.exe** process) runs as a Windows service on the managed system and starts under the context of the *LocalSystem* account. The LocalSystem account is a special account that has complete, unrestricted access to local computer resources. On a domain controller (DC) this account has unrestricted access to the Windows Active Directory. The agent maintains a secure environment by running all child processes under the context of user accounts other than LocalSystem. The PATROL administrator enforces system security standards by maintaining the user rights assignments of all PATROL user accounts.

Knowledge Modules contain the object definitions and run-time program instructions that the agent uses to manage a particular application or operating system environment. These program instructions include byte code instructions compiled from PATROL Script Language (PSL) and external commands such as operating system-level commands and command-line interfaces. Byte code instructions are executed by the **PatrolAgent.exe** process running as the LocalSystem account; external commands are executed as a separate process under the context of another user account.

AGENT ACCOUNT (AGENT DEFAULT ACCOUNT)

The PATROL Agent must be configured with an agent default account. During application discovery, data collection, menu command or recovery action processing, Knowledge Module program instructions may trigger the agent to start an external command. The agent runs external commands under the context of the agent default account, unless the instructions indicate to use a different account. To run the process as another account, both the name of the account and its system password are required. An incorrect password will generate an error in the agent error log and the external commands will not be executed.

The following window lists sample process information from the Windows Task Manager. The **PatrolAgent.exe** process displays SYSTEM in the Username column. This indicates that the user context for this process is the LocalSystem account. The **MSEXCHE2E.exe** process is a collector defined in PATROL for Microsoft Exchange Servers. It is shown to be running using the *Administrator* account.



On member servers, the agent default account can be either a local or a domain account. During agent installation, the following advanced user rights are automatically added to the account:

- Debug programs
- Increase quotas or Adjust memory quotas for a process
- Logon as a service
- Log on locally
- Profile system performance
- Replace a process level token
- Act as part of the operating system

PATROL for Microsoft Exchange Servers further requires the agent default account to be a local administrator, but only requires a subset of the above user rights as follows:

- Increase quotas or Adjust memory quotas for a process
- Replace a process level token
- Act as part of the operating system

Because of these system requirements, PATROL administrators often choose the scope of the agent default account based on their company's security policies. The following table summarizes how agent-level security is maintained:

Method of Maintaining Security	**How Security Is Established**
User Account	The default account for commands executed by the agent is specified by the */AgentSetup/defaultAccount* variable in the agent's configuration file. The agent cannot run application discovery and parameters properly without a valid user name.
User and Host Names	The Access Control List (ACL), */AgentSetup/accessControlList/* is defined by an agent configuration variable. The ACL specifies which user names can be used with which machines when connecting with an agent.
Directory and File Ownership and Permissions	Agent log and configuration files are created when the PATROL Agent process is executed for the first time. Ownership and permissions of these files is assigned at file creation time. If the PATROL_ADMIN environment variable is set, it specifies the user that owns log and configuration files. If it is not set, then the default account is used as the file owner.

EXCHANGE PERMISSIONS

Microsoft Exchange supports a variety of application-level interfaces used to gain access to system configuration and performance data. Most of these interfaces require the caller to be a domain account that has been granted an Exchange administrative role. Exchange Administrator roles cannot be granted to local user accounts.

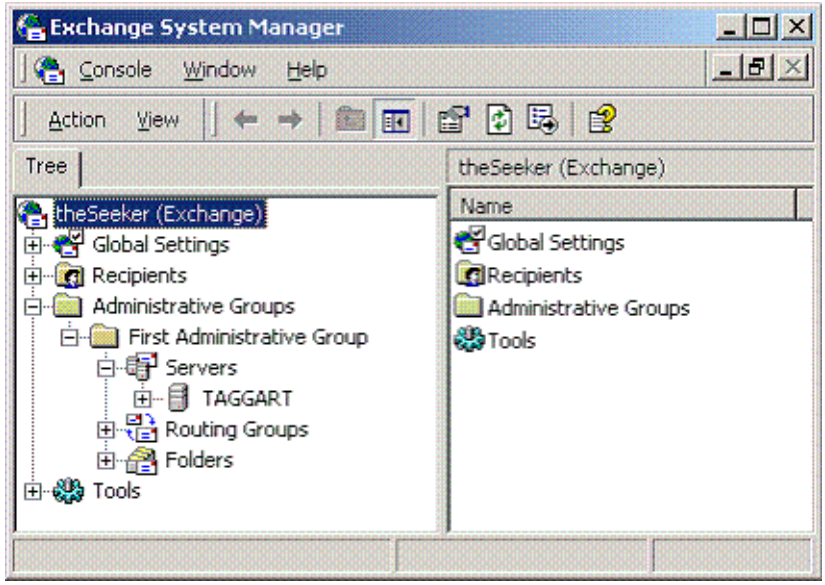
These Exchange permissions requirements add new security considerations for the PATROL administrator, such as how to

- balance a high level of system security against Exchange systems management account constraints
- maintain a separate span of control for the system administrator and the Exchange administrator
- minimize the number of Exchange administrative roles granted for management purposes

Exchange systems management requires performing tasks that simulate user experience. To do this, the systems management tool must be able to access mailboxes on each Exchange server in the configuration.

Microsoft Exchange 2000 Server introduced changes to the relationship between the user account and the Exchange mailbox. Each mailbox must have an owning domain user account; a user account can own only a single mailbox. Exchange systems management tools that simulate user experience typically must use an Exchange mailbox to perform some of their tasks. PATROL for Microsoft Exchange Servers uses a custom mailbox on each managed server for gathering information about the Exchange information store, sending and receiving e-mail messages, and capturing service-level times for various e-mail client operations. For the Exchange administrator who needs to closely manage the delegation of Exchange administrative roles throughout the organization, this can create a formidable challenge.

Example: The window below shows Exchange System Manager with an Exchange 2000 organization named **theSeeker**. The organization has only a single administrative group which is the Exchange default group named **First Administrative Group**. There is only a single back-end server in this Administrative Group named **TAGGART**.



To manage this environment, PATROL for Microsoft Exchange Servers requires:

- A domain account that is the owner of a mailbox that is a member of a storage group owned by **TAGGART**
- The name of the mailbox that the domain account owns
- A domain account that has full access to the mailbox and has *Exchange View Only Administrator* role for **First Administrative Group**

Note: The *Exchange View Only Administrator* role could be explicitly granted at the administrative group level, or it can be inherited from the organization.

The domain account requirements could be satisfied with a single account, or with two accounts with the following delegated roles:

- a mailbox owning account (without any administrative privileges)
- an Exchange administrator account

The default configuration options assume the simplest and quickest approach. This approach is best suited for product trials, and small to medium sized server environments. The default steps include:

- Creating a new Exchange user account for the managed server,
- Mail-enabling the account with a mailbox name matching the account name,
- Adding the user account into the local Administrators Group, and
- Granting *Exchange View Only Administrator* role to the account

To illustrate why this approach might not be well suited for a large scale environment, consider an Exchange organization that contains one hundred Exchange back-end servers defined to four separate Administrative Groups. Assume they are evenly divided with twenty-five servers per Administrative Group.

To manage this environment (assuming the default configuration options) you would end up with a minimum of:

- One hundred mailbox owning user accounts (each is added to the local administrators group on the manged system),
- One hundred mailboxes (one per Exchange server), and
- *Exchange View Only Administrator* role delegated to one hundred user accounts (twenty-five users per Administrative Group)

Additionally, each PATROL Agent would store the name and password of the Exchange user account for the managed system. In a highly secure environment with frequent password changes, this would represent a tremendous challenge. Not only must the system passwords be maintained, but also the corresponding agent configuration settings (saved passwords).

PATROL for Exchange Servers provides the ability to configure with pre-existing accounts and mailboxes, and the ability to limit enterprise-wide Exchange administrative rights to a single account, thereby eliminating the administrative nightmare associated with configuration as in the example above. Information on implementing this type of configuration is provided in the Exchange User Account Role section below.

PATROL FOR MICROSOFT EXCHANGE SERVERS ACCOUNT ROLES

System Access

Software that manages the Exchange environment must have access to many different operating system components and system interfaces including Exchange-specific system files, directory objects, and instrumentation data. PATROL for Microsoft Exchange Servers requires access to each of the following:

- message tracking log files (read access)
- database files and logs (read access)
- PATROL files and directories (read/write access)
- Windows Performance Monitor (read access)
- Windows Registry (read access)
- Windows Win32 APIs
- Microsoft Cluster API
- **mapisvc.inf** file (read/write access)
- Exchange 5.5 Directory Service (read/write access)
- Windows Active Directory (read access)
- Windows Management Instrumentation (read access)
- CDO for Exchange Management (CDOEXM)
- Exchange Mailbox (full access)
- MAPI Subsystem (read access)

System access requirements can be divided into three distinct system roles: local administrator, Exchange administrator, and Exchange user. PATROL for Microsoft Exchange Servers divides the management tasks according to these roles and allows you to control which account and which mailbox to assign to each role. The roles and the system resources they access are as follows:

Agent Account (Agent Default Account) Role

- message tracking log files
- database files and logs
- PATROL files and directories
- Windows Performance Monitor
- Windows Registry
- Windows Win32 APIs
- Microsoft Cluster API

Exchange User Account Role

- **mapisvc.inf** file
- Exchange 5.5 Directory Service
- Windows Active Directory
- Windows Management Instrumentation
- CDO for Exchange Management
- Exchange Mailbox

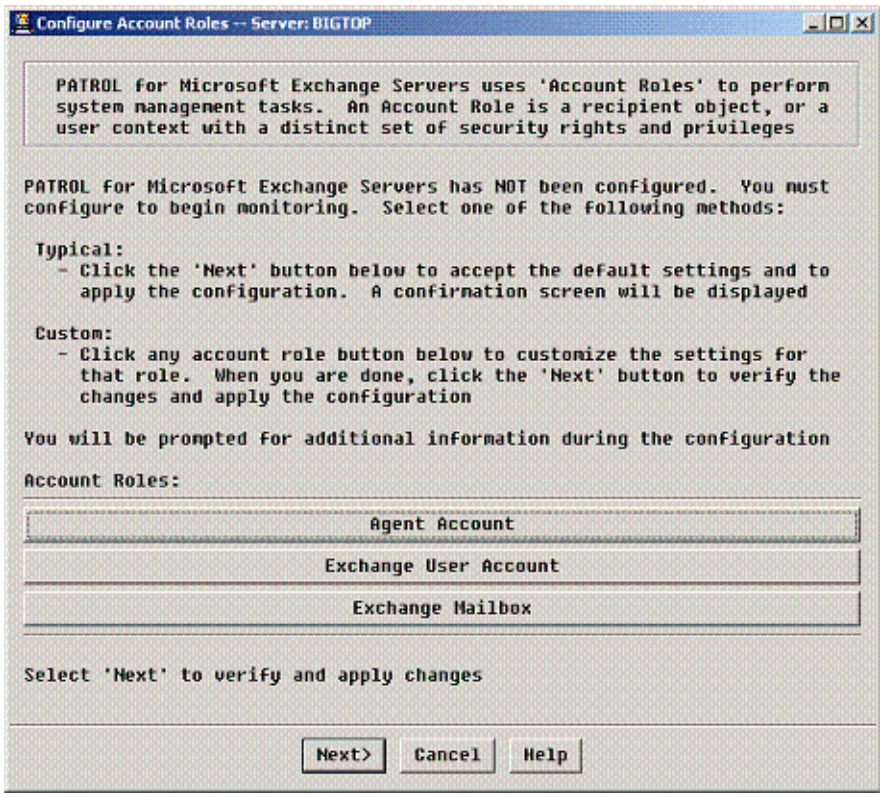
Exchange Mailbox Role

- MAPI subsystem

For each managed node, these roles must be delegated to system accounts used to perform the related functions. Although the Agent Default Account Role is listed in the configuration as a management role, you cannot alter this role through any of the PATROL for Microsoft Exchange Servers dialog boxes. The agent account can be modified through the PATROL Agent Configuration utility or PATROL Configuration Manager (PCM).

Note: If you are licensed for the PATROL consoles, then you also own a license for PCM; PCM is included with, or a component of, the PATROL Central Consoles kit.

The Configure Account Roles dialog box shows the main product configuration dialog box accessed from the PATROL console:



This dialog box is automatically displayed when a PATROL console is connected to an agent with the PATROL for Microsoft Exchange Servers knowledge module loaded, but not yet configured.

The first time configuration is performed on a managed system, the user has the option of an express configuration (**Typical**) or a customized configuration (**Custom**). The Typical configuration type uses default options described in the "Exchange Permissions" section. To perform a Typical configuration, click **Next** after the dialog box is displayed. The Custom configuration type uses options that have

been selected by the user. To perform a Custom configuration, click **Exchange User Account** or **Exchange Mailbox** and make changes on the displayed dialog boxes. The **Agent Account** (Agent Default Account) button displays information about requirements for the role but does not allow you to make changes to the role.

Required Permissions

During PATROL for Microsoft Exchange Servers configuration, each role assignment is validated for required rights and permissions before the configuration can be identified as being valid and complete. Required permissions are described in the following sections.

Agent Account (Agent Default Account) Role

The Agent Account role is used to access system-level files and objects. The following permissions are required:

- *Act as part of the Operating System* advanced user right
- *Replace a process-level token* advanced user right
- *Increase quotas* (Windows NT/2000 advanced user right)
- *Adjust memory quotas for a process* (Windows 2003 advanced user right)
- Member of the local Administrators Group

Exchange User Account Role

The Exchange User Account role is used to access the Exchange environment. The following permissions are required:

- Member of the local Administrators Group
- Full mailbox access permissions to the Exchange Mailbox
- *Admin* or *Permissions Admin* role to the Site (Exchange 5.5)
- *Admin* or *Permissions Admin* role to the Configuration (Exchange 5.5)
- *Exchange View Only Administrator* role at the Administrative Group (Exchange 2000/2003)

Exchange Mailbox Role

No explicit rights are required for the Exchange mailbox. The Exchange User Account must have full mailbox access.

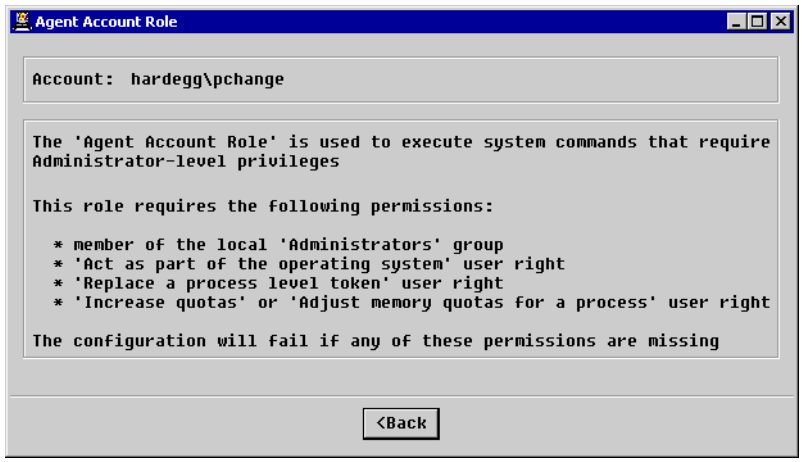
CONFIGURING ACCOUNT ROLES

As mentioned previously, during PATROL for Microsoft Exchange Servers configuration, each role assignment is validated for required rights and permissions before the configuration can be identified as being valid and complete. Configuration options are described in the following sections.

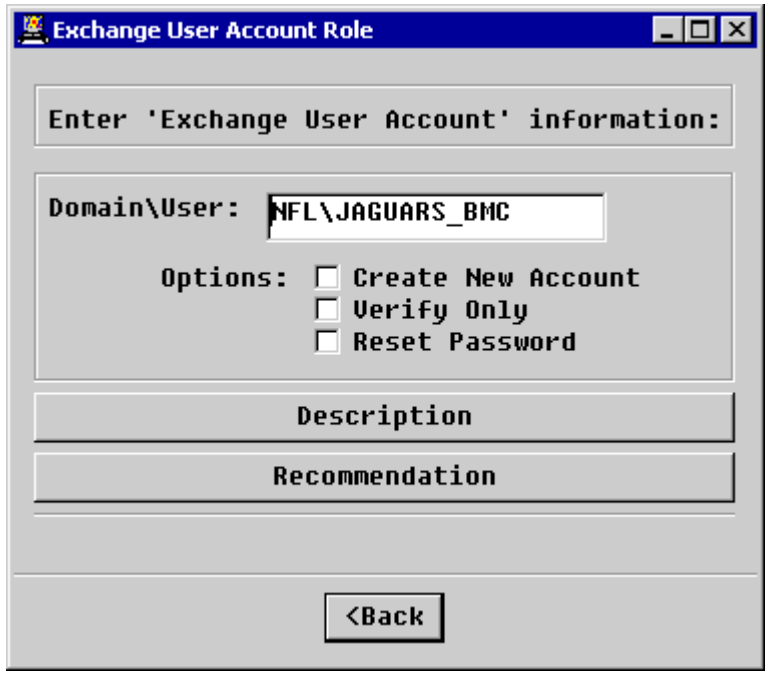
Manual Configuration Process

1. Access the Exchange application class menu, and choose **PATROL Admin => Configure => Account Roles** to display the Configure Account Roles dialog box. **(Note:** This dialog box may look different, depending on whether or not you have configured the accounts previously).

2. To view agent account information, click **Agent Account** to display the Agent Account Role dialog box, which is shown below. Click **Back** to return to the Configure Account Roles dialog box. (**Note**: If you would like to make changes to the Agent Account role assignment you must use either the PATROL Agent Configuration utility or PATROL Configuration Manager).



3. To enter or change Exchange user account information, click **Exchange User Account** to display the Exchange User Account Role dialog box, which is displayed below.



You can modify the following fields:

- **Domain\User:** The fully qualified user account name. To specify an account other than the default, enter the domain and user name in the field.

  Note: If you are configuring a node-level agent in an active-active cluster, BMC Software recommends that you enter the same Exchange user account on both nodes.

- **Create New Account:** Create a new account during configuration. To create the account you may have entered, select this option.

  Note: The account is created only if it does not already exist. Also, if you are configuring a node-level agent in an active-active cluster, BMC Software recommends that you deselect the Create New Account option when you configure the second node.

- **Verify Only**: Verify permissions assigned to the account without attempting to add any missing permissions. The default behavior for this role will add any required permissions that have not already been granted.

  Note: This option is ignored when the Create New Account option has been selected.

- **Reset Password**: Change the configured password for the account. This option is used for applying a password change to a previously configured account setting. Configuration processing also provides an option to change the system password and save it to the configuration.

The **Description** button provides a description of the fields on this dialog box. The **Recommendation** button provides the recommended use of this role.

Note: If you deselect all of the options on this dialog box, PATROL for Exchange Servers will verify the account permissions of the specified account and add permissions, if necessary.

The default configuration options assigned to this role instruct the configuration process to

- create a new account named *host*_BMC (where *host* is the name of the managed system). You will be prompted to enter a new password during configuration processing.
- add the user account to the local Administrators Group
- grant the *Exchange View Only Administrator* role to the account (Exchange 2000/2003 only)
- grant the *Admin* or *Permissions Admin* role at the Site or Organization to the account (Exchange 5.5 only)
- grant the *Admin* or *Permissions Admin* role at the Configuration to the Account (Exchange 5.5 only)

The default option to create a new account assumes you have a configuration model that uses a one-to-one administrative account model. With this model there is one Exchange administrator account per managed system. To implement a one-to-many administrative account model, you must perform the following manual steps prior to configuring the product:

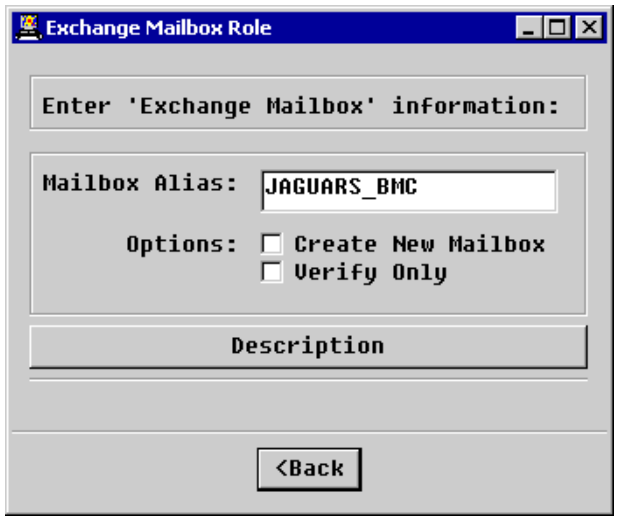
- Create an Exchange User Account.
- Delegate the *Admin* or *Permissions Admin* role at the Site or Organization (Exchange 5.5 only).
- Delegate the *Admin* or *Permissions Admin* role at the Configuration (Exchange 5.5 only).
- Delegate the *Exchange View Only Administrator* role at the Administrative Group or Organization level (Exchange 2000/2003 only).
- Create and mail-enable an account for each managed system (Exchange 2000/2003 only).

To configure using this model, deselect the **Create New** option on the Exchange User Account and Exchange Mailbox dialog boxes. Do not select the **Verify Only** option so that the configuration grants full mailbox access to the Exchange User Account.

Note: You cannot use the PATROL for Microsoft Exchange Servers Configuration Wizard (described later in this whitepaper) to configure a one-to-many model.

4. Click **Back** to return to the Configure Account Roles dialog box.

5. To enter or change Exchange mailbox information, click **Exchange Mailbox** to display the Exchange Mailbox Role dialog box, which is shown below.



You can modify the following fields:

- **Mailbox Alias**: The default is *host*_BMC. To specify a mailbox other than the default, enter the mailbox name in the field.

- **Create New Mailbox**: Create a new mailbox during configuration. To create the mailbox you may have entered, select this option. (**Note**: the mailbox is created only if it does not already exist. The owner will be the user account that was assigned to the Exchange User Account role).

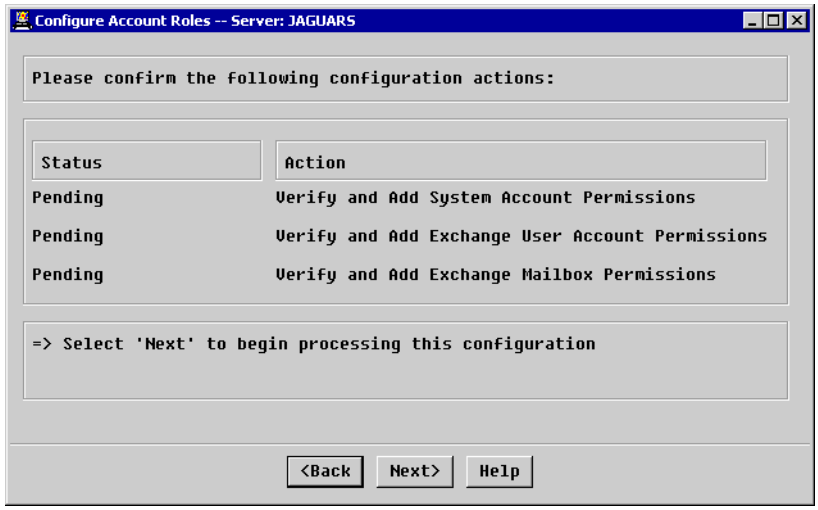
- **Verify Only**: Verify the mailbox access permissions of the Exchange User Account without attempting to add any missing permissions. The default behavior for this role will add any required permissions that have not already been granted to the account.

  Note: This option is ignored when the Create New Mailbox option has been selected.

The **Description** button provides a description of the fields on this dialog box.

6. Click **Back** to return to the Configure Account Roles dialog box.

7. Click **Next** to display a confirmation Configure Account Roles dialog box.



8. Confirm your entries and selections.

   - If you need to change an account setting, click **Back** to return to the Configure Account Roles dialog box.

   - If the settings are correct, click **Next** to make the changes.

   Once all account role options have been specified, a confirmation screen is displayed showing each of the processing steps for the configuration.

   When configuration processing begins, each role assignment is validated for the required rights and permissions before the configuration can be identified as valid and complete. A configuration report is generated showing the results of each processing step and is displayed in a task pop-up window upon completion of the configuration process. A print option is provided for all task pop-ups.

9. Deselect the **View Details** option if you do not wish to review the details of the configuration.

10. Click **Finish**.

Configuration Wizard

The configuration dialog box is designed to configure a single managed system. For environments with many servers, this approach can be very time consuming and tedious. PATROL for Microsoft Exchange Servers includes a configuration wizard for generating agent rulesets used for automatic

configuration. This wizard generates two rulesets:

- Domain ruleset—MSEXCHSetup/AutoConfig/defAccount. This value is assigned a string that contains the username and encrypted password of the configuration account. The format is: *domain\user/password*.

- Modified host mailbox ruleset—MSEXCHSetup/AutoConfig/mailboxAccount. This value is assigned a string that contains the name of the Exchange mailbox and encrypted password. For Exchange 2000 or higher, this also represents the username and password of the account that owns the mailbox. The format is: *user/password*.

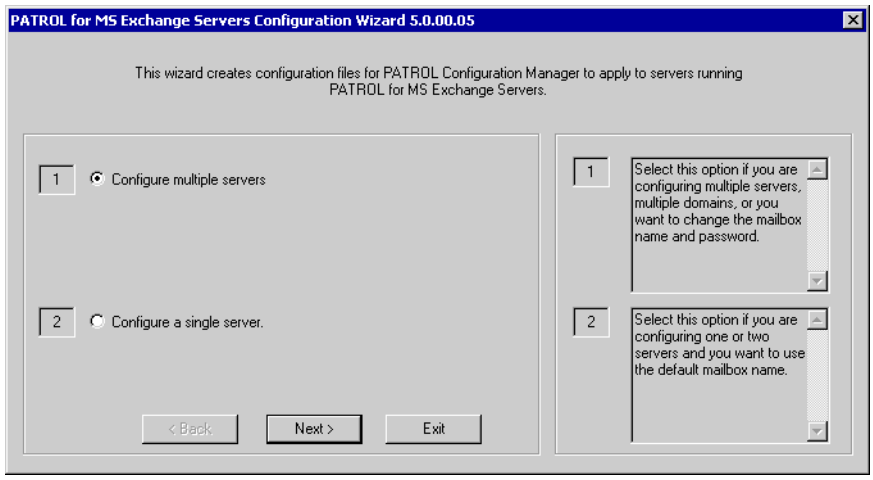
  Note: This ruleset is only generated when the default mailbox name or mailbox password are modified for a host in the Configure multiple servers screen. There is one ruleset for each modified host mailbox.

The PATROL for Microsoft Exchange Servers Configuration Wizard rulesets are imported into PCM (PCM is thus required to use the configuration wizard) and deployed to managed systems. Once deployed, the rulesets trigger PATROL for Microsoft Exchange Servers knowledge modules to process the Exchange User Account and Exchange Mailbox account roles. These rulesets can be incorporated into PATROL Configuration Manager.

The PATROL for Microsoft Exchange Servers Configuration Wizard initial window, shown below, provides two main options:

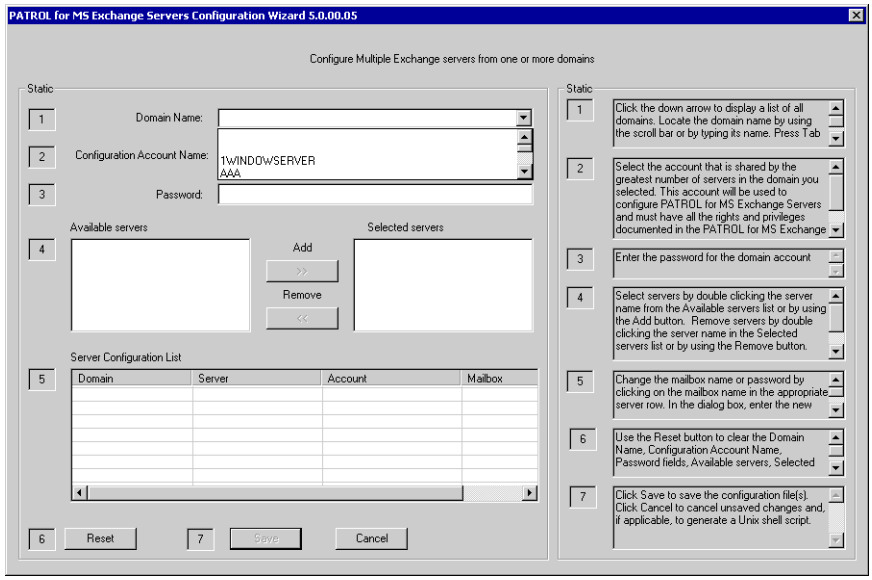
- **Configure multiple servers** - an option for generating rulesets to configure one or more servers discovered in the Windows network. This option will generate one or more rulesets based on the options selected.

- **Configure a single server** - an option for configuring a single server using default options. This option prompts for all user input and does not provide Windows network discovery.

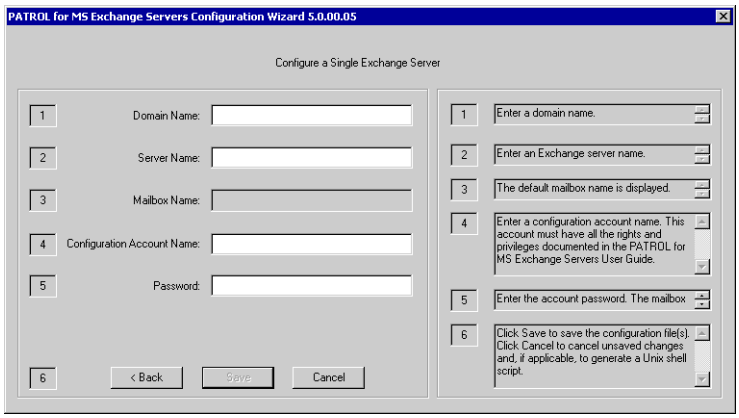


After you have selected a configuration option, you will be prompted to enter the location where you would like to save your rule rulesetssets and if you would like to generate a Unix shell script. Once you have made these selections, click **Next**.

If you select the **Configure multiple servers** option, the next window lists all of the Windows domains it finds using Windows network discovery. Select a domain and configuration account for the domain and enter the configuration account password. From the **Available Servers** list, select the servers to be configured, which are then displayed in the **Selected Servers** list. You can override the Exchange User Account name for a server by clicking in the **Mailbox** field for the server. Click the **Save** button to generate one or more rulesets for the configuration.



If you select **Configure a single server** option, the next window prompts for user input without providing selection lists. The information is validated over the network. If you select this option, the Exchange Mailbox name cannot be changed. The default Exchange Mailbox name is *host*_BMC. Click the **Save** button to generate one ruleset for the configuration.



Ruleset-based configuration is referred to as *automatic configuration.* The processing behavior for this type of configuration is somewhat different than the dialog-based approach.

Automatic Configuration Process

Automatic configuration is performed by PATROL for Microsoft Exchange Servers. The **MSEXCH_Server** application class discovery detects automatic configuration rules and applies those rules to the configuration. All messages are written to the PATROL console system output window.

Automatic configuration does not provide the same flexibility as the PATROL console configuration dialog box. When configuring using rulesets, knowledge module configuration rules use the following implementation scheme:

- The default ruleset, **MSEXCHSetup/AutoConfig/defAccount**, is assigned the credentials for a configuration account which is used to process the configuration. The configuration account ruleset is first validated for required permissions.
- The Exchange Mailbox name (and owning account for Exchange 2000/2003 servers) is read from the **MSEXCHSetup/AutoConfig/mailboxAccount** ruleset. If this ruleset is missing, then the default name, *host*_BMC, is used.
- The Exchange User Account is created (if it does not already exist).
- The Exchange User Account is delegated required Exchange administrative roles.

- The Exchange User Account is mail-enabled and assigned a mailbox alias with the same name (if not already enabled and assigned).

- The configuration is validated and required agent configuration variables are saved indicating the configuration is complete.

This type of configuration allows the PATROL administrator to streamline the configuration process for a large number of managed systems. The configuration process can be distributed to all of the deployed managed nodes concurrently.

CONCLUSION

The PATROL for Microsoft Exchange Servers configuration process provides a means to recognizing the value of Exchange system management. The process needs to be simple, robust, and provide options for all types of users. Configuration features are provided for trial users, custom users, and power users. For the trial user, default options will perform account and mailbox creation and permissions delegation. For the custom user, modifiable options allow the user to setup accounts and permissions prior to configuring and to perform post-configuration actions. For the power user, product configuration can be streamlined by distributing the configuration process to managed systems through the use of automatic processing.

SOURCES

- http://support.microsoft.com
- http://www.microsoft.com
- *PATROL Agent Reference Manual*
- *PATROL 7 Security Implementation: Securing the Data in Your PATROL-Managed Environment*
- *PATROL for Microsoft Windows Server Getting Started*
- *PATROL for Microsoft Exchange Servers Getting Started*
- PATROL for Microsoft Windows Servers
- PATROL for Microsoft Exchange Servers
- PATROL for Microsoft Windows Servers online Help
- PATROL for Microsoft Exchange Servers online Help

HELPING YOU MAINTAIN ADVANTAGE

BMC Software Professional Services helps your company maintain its competitive advantage through a comprehensive suite of services that includes service level management consulting, installation, implementation, configuration, and customization. Our professional services and education offerings are designed to ensure the ongoing availability of critical business applications, maximize product potential, reduce project risk, deliver IT value to your business, and improve your operations. For more information about BMC Software Professional Services, visit http://www.bmc.com/profserv.

About BMC Software

BMC Software, Inc. [NYSE:BMC], is a leading provider of enterprise management solutions that empower companies to manage their IT infrastructure from a business perspective. Delivering Business Service Management, BMC Software solutions span enterprise systems, applications, databases, and service management. Founded in 1980, BMC Software has offices worldwide and fiscal 2003 revenues of more than $1.3 billion. For more information about BMC Software, visit www.bmc.com.

47519

July, 2004