bmcsoftware

BMC FootPrints Asset Core - Client Agent Rollout

Version 11.5

BUSINESS RUNS ON I.T.
I.T. RUNS ON BMC™

www.bmc.com

Legal Notices

BMC Software, Inc.

2101 CityWest Blvd, Houston TX 77042-2827, USA

713 918 8800

Customer Support: 800 537 1813 (United States and Canada) or contact your local support center

Contents

Introduction

The BMC FootPrints Asset Core is a unique solution for managing and securing systems that provides a global overview of the complete infrastructure by using its automating administration tools as well as its securization functionalities. Once installed on all systems the Asset Core agents allow the administrator to monitor all devices from the Asset Core administration console.

The BMC FootPrints Asset Core is composed of a master server, a unique agent, installed on all devices and relay agents for an optimized architecture, a database as well as a unique administration console.

Formatting Conventions

Throughout this manual you will encounter elements that stand out in different ways. These elements each have a specific intention and are used consistently, so when you see such an element you immediately know what kind of information to expect.

The following table explains the different formatting conventions:

What you see (Examples)	What it means
1. Select... **2.** Click...	Ordered list of instructions. Execute the steps in the given order.
• Option 1 • Option 2	Enumeration of different options/scenarios to choose from.
Operational Rules	Item of the Graphical User Interface of the software.
Properties	Title of a dialog box/popup window
You need write access to the immediate parent, from which the device or device group is being deleted..	Before a task. Informs you about the prerequisites for the following task.
The **Properties** dialog box appears on the screen.	After a step. Informs you about the immediate result of a step.
The new status has been saved and applied to the selected group.	After a set of instructions. Informs you about the final result of the task.
`MyDevice1,MyDevice1.com,255.255.255.0,"James Kirk",...` `MyDevice2,MyDevice2.com,255.255.255.0,"First Spy",...`	Lines of code.
The new patch group will have the same members as the selected device group.	Additional useful information.

What you see (Examples)	What it means
 To scan every day at 01:00 AM, from the **at** drop-down list select **01:00**.	Example or recommendation from BMC Software for best practice.
 **Note** You can only use ISO-Latin characters even if you are using a Japanese, Greek or Arabic localization.	Simple note or piece of advice.
 **Remember** If you manage your group through a directory server you may not manually create or add objects to this group anymore.	What you are about to do will affect the system behaviour.
 **IMPORTANT** When deleting an administrator you loose all capabilities and access rights accorded to this administrator as well.	What you are about to do will lead to loss of data or settings.
 **ATTENTION** If the original group or "OU" on the directory server was renamed, moved or deleted, the Asset Core group cannot be resynchronized with this group. An error message will be displayed instead.	What you are about to do will lead to partial or entire system failure.

Introduction to Rollouts

BMC FootPrints Asset Core provides you with a rollout mechanism through which you do not have to physically visit each device on your network to manually carry out the install procedure of the Asset Core agent. Asset Core contains a node directly accessible via the Asset Core Console, which will distribute the agents to any number of networked devices. This rollout also enables reinstalling and uninstall if and when required.

The rollout functionality is accessed via the main **Rollout** node which is located under the **Global Settings** top node.

Starting and Logging On

The following paragraphs will guide you through the startup of all parts of the software and through your first logon to the BMC FootPrints Asset Core Console.

Agent Startup

The Asset Core agent installed on the master should start up automatically. To verify this you must proceed as follows, depending on your operating system. If your agent should not be running for any reason you will also find out how to start it. This process is also valid for the startup of the client agents, therefore you will also find a paragraph for MAC, which is not available as a master agent.

Once these agents are running they will fill in their data into the BMC FootPrints Asset Core database on the master.

Windows

The Asset Core agent icon should be displayed in the systray of your master server or client when the agent is running. It can be one of the following colors indicating a specific status:

- The icon is grey during the agent's initialization.
- The icon is blue when the agent is running.
- The icon is green or flashing green when an operation is in progress.
- The icon is red when the agent tries to carry out an unauthorized action or access.
- The icon will turn yellow when the local device is taken over through remote control.
- The blue icon will show a package when packages and operational rules are advertised to the client and are available for download and installation.

If you want to start a stopped agent you need to do so via the Services window of the Control Panel. If you double left click it, a graphic agent interface will open giving the administrator(s) access to various modules and settings related to this agent. The administrator may modify settings and actions via this interface. For more information on this interface, please refer to chapter Agent Configuration in the basic objects manual.

Command Line Options

The agent may also be launched from the command line with the following options:

cmd	cmd long	Description
-v	--version	Returns the version of the agent.
-i	--install	Installs the service. This option must be used in connection with the -sn 'Service Name' option.
-r	--remove	Removes the service. This option must be used in connection with the -sn 'Service Name' option.
-sa	--standalone	Starts the agent as standalone.

cmd	cmd long	Description
-cw	--consolewindow	Starts with popup window (for output text).
-sn	--servicename	Used to install/remove using non-default service name.
-dn	--displayname	Used to install/remove using non-default service display name.

Linux

The Asset Core agent installed on the master should start up automatically. This can be checked by typing `ps -ax | grep mtxagent` and pressing the Enter key. The console or terminal window should return: `/usr/local/numara-software/footprints-asset-core/master/bin/mtxagent` as one of the running processes in the process list that will now be displayed.

To start or stop the agent type the following command into a terminal window:

```
service BMCFootPrintsAssetCoreAgent start
```

```
service BMCFootPrintsAssetCoreAgent stop
```

Command Line Options

The agent may also be launched from the command line with the following options:

cmd	cmd long	Description
-v	--version	Returns the version of the agent.
-sa	--standalone	Starts the agent as standalone.

Mac OS

The Asset Core agent installed on a Mac device should start automatically after a device reboot. This can be checked by typing `ps -eaf |grep mtxagent` and pressing the Enter key. The console or terminal window should return: `/usr/local/numara-software/footprints-asset-core/client/bin/` as one of the running processes in the process list that will now be displayed.

If the agent does not start type the following into a terminal window:

```

SystemStarter start BMCFootPrintsAssetCoreClient
```

then press your Enter key. The agent will start now.

Command Line Options

The agent may also be launched from the command line with the following options:

cmd	cmd long	Description
-v	--version	Returns the version of the agent.

cmd	cmd long	Description
-sa	--standalone	Starts the agent as standalone.

Logging on to the Console

The following paragraphs guide you through your first startup and login of the console according to your operating system and the first preparatory actions to take before you may execute any operations.

Console Startup

As already mentioned the console is a Java application and may thus be launched using the generally available startup options provided by Java, such as -Xmxn to extend the maximum size of the memory allocation (n must be a multiple of 1024, for example: Xmx80m or Xmx81920k). By default the anti-aliasing option is used for the console. To switch it off, open the console shortcut's Properties window and modify the -Dswing.aatext option from true to false.To launch the console with its standard options follow the steps indicated below, depending on the operating system on which your console is installed:

For information on how to start the console via the command line or Java Web Start and possible parameters see the respective chapters in the Customizing and Integrating Asset Core with 3rd Party Applications manual.

Windows

To launch your newly-installed Console, click your Start menu, choose Programs -> BMC Software -> FootPrints Asset Core -> Console or double-click the console desktop icon.

Linux

To start the console you need to type `BMCFootPrintsAssetCoreConsole`, then press your Enter key.

Mac OS

To start the console double-click the icon for the Console Web Start on the desktop.

First Login

When you launch the console for the first time you must use the predefined default administrator login admin as login name. As this login has no password defined a popup window appears on the screen in the language version of the operating system, or in English if it is of a language not supported by Asset Core, requesting you to define it. Once you entered the new password in the respective field and confirmed it, the console opens on the screen.

ATTENTION

Be aware, that if you have installed master and relay agents with the SSL=0 option, you also must use the non secure connection option here to connect the console with the master. If the master and agents are installed with any other SSL option the console will only accept SSL connections.

Note

If you have installed master and relay agents with the SSL=3 option, do not forget to supply the client certificate to the console.

Console installed on Master with Java Web Start support

1. Enter the user name `admin` and no password into the respective fields.
2. The line **Server:Port** displays the name of the database server and its port number to which the console will connect. If the Console is installed on the master server this field will be filled in with the default value `localhost:1610`. If you are connecting via Java Web Start this field will be filled in with the master information (that is, either its name or its IP address).
3. Then click the **Login** button at the bottom of the window.

Master and Console installed on different devices

If your console is on a device other than the master no information is pre-entered.

1. Enter the user name admin and no password into the respective fields.
2. Replace the pre-entered localhost entry with the name of the master server you want to connect to and its port number separated by a colon (:) into the Server:Port field.
3. Then click the **Login**button at the bottom of the window.

Launching the Console from Outside the Company Network

If you need to connect to Asset Core via the Internet and have installed your Console via the .msi file you must provide the public IP address of the master to be able to connect.

1. Enter the user name admin and no password into the respective fields.
2. Replace the pre-entered localhost entry with the public IP address of the master server you want to connect to and its port number separated by a colon (:) into the Server:Port field.
3. Then click the **Login** button at the bottom of the window.

Preparing the Console

Before you may execute any operations in the console such as rolling out the agents across your network, you must provide the license for your system. You can download this license from the BMC Software Web site. If this is not the case, please contact them to provide you with one. However, a basic temporary license will automatically be installed with the software to be able to launch it. This license is limited to 20 managed devices and 15 days. It will be erased and replaced as soon as you import your full license.

The license file contains all the necessary information regarding the purchased product options. After it is installed you may access all of these. Licenses are imported via their files and cannot be added manually. If you have a license excluding some features of the product, you may always acquire an additional license for these and add the license for the new features later on. To follow the exercises in section II of this manual it is sufficient to start with the preinstalled basic license for 20 devices. If your license is expired only the **Licenses** node will be shown in the console to allow you to import a new one.

Specific Considerations for a Super Master Architecture

As with the regular architecture, you must first import the licenses delivered with your software into ALL your masters, including the super master. Be careful to use the correct license for each master device as the contents reflected in the license key will be different for each license:

Super Master

- the global maximum number of all devices (for example, one site has a 50 device license a second one 30, then the super master will have a license for 81 agents),
- the global maximum number of all scans (for example, one site has a 50 scan license a second one 30, then the super master will have a license for 80 scan inventories),
- the global maximum number of all patched devices (for example, one site has a 50 device license a second one 30, then the super master will have a license for 80 patch inventories),
- the Super Master license.

Site Masters

- the total number of devices the respective site will manage (for example, for 50 agents,
- the licenses for all purchased functionalities, such as software distribution, task management, vulnerability management, etc.

Changing the Console Display Language

You may also change the language in which the console is currently displayed, if British English is not your working language. For this proceed as follows:

1. Select the menu option **Tools** > **User Preferences**or click the link **Your Preferences** in the **Welcome** part.

   The window **Preferences**appears on the screen.

   You may change to you required language via the option **Language** in the **General** tab.
2. For this select the language form the drop-down list.
3. Then click the **OK** button to confirm and to close the window.

The console will refresh and be displayed in the selected language.

Importing your License

To import your license proceed as follows:

1. Click on the **Global Settings** node and select from its children the **Licenses** node in the left window pane.
2. Either select **Edit** > **Import License** or the icon in the icon bar.

   A dialog box opens displaying the directory structure in a Windows Explorer like format.
3. Select the file containing your license.
4. With the file selected click the **Open** button at the bottom of the window.

   The information is then read from the file and displayed in the table in the right window pane as follows:

   - **Name**

     The fields in this column display the names of the licenses, which are the following:
   - **Count**

     The number in this field indicates how many agents the license contains (that is, on how many devices you may install clients). If you have a temporary license for testing purposes this number will be 20. For all other licenses this field displays 1, if the license is activated (that is, purchased or 0 if you do not have this license).
   - **Available**

     This column indicates the number of remaining licenses. It is applicable to the Agent, Patch and Vulnerability Management as well as to the number of VM scanners. It displays how many licenses are still free to be used. For all other purchased licenses this field will always display 1.

- **Expiry Date**

  This field is empty if you have an unlimited license for use in your system. If the license is temporary and thus limited this field displays the expiry date of the license, in the default format defined in the user preferences. A temporary license is valid 15 days.
- **Status**

  This field shows the current status of the license. If you are using the test license it will display Expiring.

Now that you have installed your license and thus validated your database and Console, you are ready to start working with the BMC FootPrints Asset Core and proceed to installing a relay and rolling out the agent throughout your network, detailed in the following chapters.

Available Licenses

Following you will find a table with all available licenses explaining which functionalities they include:

License	Description
Application Management	all types regarding the monitoring and prohibiting of applications as well as self-healing functionalities.
Compliance Management	this license activates the device compliance management of the BMC FootPrints Asset Core.
Direct Access	the license providing the direct access features to the remote clients of your installation.
Inventory	the license for the following types of inventory: software, hardware, custom, connectivity, security, and the inventory of unmanaged devices. All other inventory types are part of their respective functionality.
Multicast	activates the multicast transfer option for transferring packages and other information between the Asset Core agents.
Device License	this is the basic license of the product and provides you with the maximum number of agents installed on clients which the database will accept. For the initial and evaluation license this number is fixed at 20. Please note that unconnected devices of which the inventory is integrated will not decrease this value (that is, these devices are not counted for licensing purposes).
Operating System Deployment	this license activates the operating system deployment module which allows you to create OS images and deploy them to any device within your network.
Patch Knowledge Base Update	this license is required to maintain the patch knowledge base up to date.Patch Management - the number of licenses for patches of Windows and other manufacturers and programs, such as Adobe, Mozilla, etc. The number indicates how many devices may be patched at the same time. For the initial and evaluation license this number is fixed at 20. You also need either this license or the Distribution license to access the Operational Rules functionality.
Power Management	activate the Green IT / Power Management feature.
Remote Control	activate the remote control feature.

License	Description
Software Distribution	this license activates all software distribution features of the product such as package generation and scheduling the distribution. You also need either this license or the Patch Management license to access the Operational Rules functionality.
Super Master	this license is required for a super master architecture with a super master and a number of site masters.
Task Management	this license allows you to create tasks to assign and follow the evolution and execution of specific network management tasks via the console.
Topology Graph	activates the graphical display of your network topology.
Vulnerability Knowledge Base Update	this license is required to maintain the vulnerability knowledge base up to date.
Vulnerability Management	this license defines how many devices, with and without installed Asset Core agent may be scanned (that is, may be defined in a target list). Same as with the scanners the devices may be replaced, but never may all defined target lists contain more than the fixed number of members. The evaluation license for example allows you 3 different devices to scan. You may either have this license OR the **Vulnerability Management Scan Pack** license, but not both.
Vulnerability Management Scan Pack	this license defines a number of scans that may be executed on any device in your network. This license is not part of the evaluation. You may either purchase this license OR the **Vulnerability Management** license, but not both.
Vulnerability Management Scanners	this license is always required for the VM module. It defines how many devices may be defined as scanners in your network. You may replace an existing scanner with another device, but you may not have more than the purchased number. The evaluation license for example allows you 2 scanners.
Windows Device Management	this license activates the peripheral device monitoring and controlling functionalities for Windows devices.

Deploying Your First Asset Core Agents

Most management features in Asset Core (patch management, remote control, software distribution, etc.) require that agents are installed on the target machines.

The agent rollout wizard facilitates installation of the Asset Core agent within your environment. The two main components of this process are:

- The **Rollout Server**, a device that generates self-extracting agent installation packages and can push them on the target devices.
- **Rollouts** which include agent installation files, target devices and rollout options.

A typical Asset Core architecture has a smaller number of relays directly under the master and a larger number of clients under each relay. This first section therefore teaches you how to perform the two main types of rollout:

1. Rolling out relay agents (with the master server as their direct parent) and
2. Rolling out final clients (with one of the previously installed relays as their parent).

Prerequisites

Before starting a rollout make sure that the following prerequisites are fulfilled:

- remote shares are accessible from the master device (for example, *ClientMachine1*\C$)
- the RPC service is started
- no NAT-configurations are used
- the remote services are accessible
- for Linux installations make sure that the SSH service is installed and running on the targets
- for Linux installations the root account must be enabled on the targets
- for Mac OS installations make sure that SSH and the root account are enabled on the targets

Configuring the Rollout Server

A Rollout Server is an Asset Core agent used to deploy other agents. To define a device as Rollout Server proceed as follows:

Remember

To remotely deploy agents to Windows targets the Rollout Server MUST also have a Windows operating system.

Note

Any Rollout Server can remotely deploy Asset Core agents to other operating systems (such as Linux/MacOS).

Note

If you have a very heterogeneous and/or distributed environment you may want to define specific Rollout Servers for subnets and/or the different operating system platforms.

To define other Rollout Servers proceed as follows.

1. Click the **Add Rollout Server** icon in the iconbar.
2. Select the new device which is to be *Your Rollout Server* from the list.

3. Then click **OK** to add it and close the window.

Rolling out Relay Agents

- Make sure you already have a rollout server defined. If this is not the case please refer to: *Add Rollout Server*.
- This rollout uses device groups. If you have not yet created a group please do so first. It is also possible to find your rollout targets via other lists, such as the Microsoft Network option or autodiscovered devices.

1. To create a relay agent rollout with the master as its direct parent (only applicable if the master was installed with the default values), launch the rollout creation wizard by selecting the **Wizards** > **Agent Rollout** menu item.

   The **Core Setup Configuration** window appears on the screen.

2. Check the box for **Enable agent as a relay for the other agents**.

   If you want to schedule the rollout at a specific date and time check the box for second last question.

3. Click **Next**.

   The **General Parameters** appears on the screen.

4. Enter the name of the new rollout (for example, *Linux Relay Agents*) into the **Name** field.
5. Enter the name for the rollout package executable that will be created into the **Auto-extractible Name** field (for example, *linuxrelayagent10.sh* or *linuxrelayagent10* for a Linux rollout, or *win7relayagent10.exe* for a Windows 7 installation).
6. Select the operating system group to which the agent is to be rolled out from the drop-down list of the **Operating System** field, for example, *Linux* .
7. Click **Next**.

   The **Targets & Accounts** window appears on the screen.

8. Click the **Select a device** icon.
9. Select the desired group that contains the relay rollout targets of the defined operating system type in the **Available Objects** box.
10. To select individual devices instead of a group click the **All** icon on the left bar and select your devices from the appearing list.
11. Click the **OK** button to add the group and close the window.
12. Now click the **Add Administrator** icon.
13. Enter the required data for the account login into the respective fields.
14. To add a new account click **Add Administrator** in the icon bar.

    The **Properties** dialog box appears on the screen.

15. Enter the following data for a new account login into the respective fields:
    a) Enter the name of the domain to which the rollout is going into the **Administrator Domain** field. You may use an asterisk (*) if the rollout is going to all domains.
    b) Enter the login name of the admin (for when the agent deployment tries to log on to the remote target to install the agent) into the **Administrator Login** field.

    For Windows XP Professional rollouts you MUST enter a valid login and password, and it must be the same for all devices, that is, the rollout server (the master) as well as targets.

    If you are not sure that your local administrator login has the same passwords for all targets, use the domain login. For domain logins to work correctly, the necessary domain trust relationships must already have been set up between the different domain controllers.

c) Enter the password of the above-entered admin into the Password field. For security reasons the passwords will only be displayed in the form of asterisks (*).
d) Confirm the above-entered the password into this field.
e) Click the OK button to confirm the new account and add it.

☞ It will now be shown in the list above.

16. Click the **Verify Rollout** button at the bottom to make sure the credentials are correct.
17. Click **Finish**.
18. In the following **Confirmation** popup window check the **Go to Rollout** radio button to change the focus of the console window to the new rollout. Click **Yes** to confirm the immediate activation.
19. If you have not checked the **Go to Rollout** box at the end of the wizard select the newly created rollout in the left tree hierarchy and then its **Servers** subnode.

    In the **Assigned Schedule** tab you can follow the general progress of the relay rollout assignment
20. Once this value reads `Executing` select the**Targets** tab to follow progress of each individual target through the **Status**column (initial status is `Initial` and final stage should be `Installed`)

✓ To continue installing your architecture with clients below, the relays continue with the next task.

Rolling out Client Agents

Make sure you have executed the rollout in the preceding task to have at least one relay available for this client rollout!

To rollout a client agent proceed as follows:

1. To create a client agent rollout, launch the rollout creation wizard by selecting the > **Wizards** menu item.

   ☞ The **Core Setup Configuration** window appears on the screen.
2. If you want to schedule the rollout at a specific date and time check the box for second last question **Configure a custom schedule for this rollout (default is one immediate execution)** now.
3. Click **Next**.

   ☞ The **General Parameters** appears on the screen.
4. Enter the name of the new rollout, for example, *Windows 32 Bit Clients* into the **Name** field.
5. Enter the name for the rollout package executable that will be created into the **Auto-extractible Name** field, for example, *win32clientagent10.exe* for a Windows 32 bit client rollout.
6. Select the operating system group to which the agent is to be rolled out from the dropdown list of the **Operating System** field, for example, *Windows 2000/XP/... (32 bit)*
7. Click **Next**.

   ☞ The **Communication** window appears on the screen.
8. To find the relay click the **Select a device** icon next to the **Parent Name** field.
9. Click the **All** icon.
10. Select the desired parent device from the appearing list and click **OK**.
11. Click **Next**.

    ☞ The **Targets & Accounts** window appears on the screen.
12. Click the **Select a device** icon.
13. Select the desired group that contains the client rollout targets of the defined operating system type in the **Available Objects** box.

14. To select individual devices instead of a group click the **All** on the left bar and select your devices from the appearing list.
15. Click the **OK** button to add the group and close the window.
16. Now click the **Add Administrator** icon.
17. Enter the required data for the account login into the respective fields.
18. To add a new account click the **Add Administrator** icon.

    The **Properties** dialog box appears on the screen.
19. Enter the following data for a new account login into the respective fields:
    a) Enter the name of the domain to which the rollout is going into the **Administrator Domain** field. You may use an asterisk (*) if the rollout is going to all domains.
    b) Enter the login name of the admin as which the rollout tries to log on to the remote target to install the agent into the **Login** field.

    For Windows XP Professional rollouts you MUST enter a valid login and password, and it must be the same for all devices, that is, the rollout server (the master) as well as targets.

    If you are not sure that your local administrator login has the same passwords for all targets, use the domain login. For domain logins to work correctly, the necessary domain trust relationships must already have been set up between the different domain controllers.

    c) Enter the password of the above entered admin into the Password field. For security reasons the passwords will only be displayed in the form of asterisks (*).
    d) Confirm the above entered the password into this field.
    e) Click the **OK** button to confirm the new account and add it.

    It will now be shown in the list above.
20. Click the **Verify Rollout** button to make sure the entered account data are correct.
21. Click **OK**and then **Finish**.

    The **Confirmation**dialog box appears on the screen.
22. Check the **Go to Rollout** radio button to change the focus of the console window to the new rollout.
23. Click **Yes**to confirm the immediate activation.
24. If you have not checked the **Go to Rollout** box at the end of the wizard select the newly created rollout in the left tree hierarchy and then its **Servers** subnode.

    In the **Assigned Schedule** tab you can follow the general progress of the client rollout assignment.
25. Once this value reads `Executing` select the **Targets** tab to follow progress of each individual target through the **Status** column (initial status is `Initial` and final stage should be `Installed`).

Your first rollout is now completed and your installed base is large enough to execute any other operation.

Rollout Alternatives

In this section you will find alternative ways to roll out your client agent to the target population, such as via the Microsoft Network Neighborhood or to a specific IP address range.

Rolling out Client Agents via the Network Neighborhood

In this example rollout we will roll out the agent to some Windows 7 devices using the Windows network neighborhood.

1. Launch the rollout creation wizard by selecting the **Wizards** > **Agent Rollout**item menu .

   The **Core Setup Configuration** window appears on the screen.

2. Check the box **Configure the relay selection or use master otherwise**.

   If you want to schedule the rollout at a specific date and time check the box for second last question.

3. Click **Next**.

   The **General Parameters** appears on the screen.

4. Enter the name of the new rollout (for example, Windows 7 Client Rollout) into the **Name** field.
5. Enter the name for the rollout package executable that will be created into the **Auto-extractible Name** field (for example, *win7clientagent11.exe*).
6. Select the operating system group to which the agent is to be rolled out from the drop-down list of the **Operating System** field (for example, *Windows 2000/XP/... (64 bit)*.
7. Click **Next**.

   The **Communication** window appears on the screen.

8. To find the relay click the **Import Devices from CSV File** icon next to the **Parent Name** field.
9. Click the **All** icon.
10. Select the desired parent device from the list and click **OK**.
11. Click **Next**.

    The **Targets & Accounts** window appears on the screen.

12. Click the **Import Devices from CSV File** icon.

    The **Select Devices from the List** window appears on the screen. It provides you with the different methods to choose the rollout targets.

13. Select the **Network** tab in the left window bar.

    The field **Available Devices** displays now the Microsoft Windows Network Neighborhood structure on the screen.

14. Open the tree structure under which the target device are located.
15. Select the device/devices to be added to the list by marking the different devices and moving them to the **Selected Devices** list to the right via the **Add** button.

    Be aware that you can select a maximum of 18 devices for your rollout with the evaluation license. The evaluation license allows you to test with a total of 20 devices, and you already installed the master and probably at least one relay.

    Be aware that you cannot add the master as a target device.

16. Click the **OK** button to add the selected devices and close the window.
17. Now click the **Add Administrator** icon.
18. Enter the required data for the account login into the respective fields.
19. Click the **Verify Rollout** button to make sure the entered account data are correct.
20. Click **OK** and then **Finish**.
21. In the following **Confirmation** popup window check the **Go to Rollout** radio button to change the focus of the console window to the new rollout. Click **Yes** to confirm the immediate activation.
22. If you have not checked the **Go to Rollout** box at the end of the wizard select the newly-created rollout in the left tree hierarchy and then its **Servers** subnode.

    In the **Assigned Schedule** tab you can follow the general progress of the client rollout assignment.

23. Once this value reads `Executing` select the**Targets** tab to follow progress of each individual target through the **Status** column (initial status is `Initial` and final stage should be `Installed`).

You have now rolled out the Asset Core client agent to specific devices of your infrastructure that were provided by the Microsoft Network Neighborhood.

Rolling out the Client Agent to Specific IP Address Ranges

To roll the agent out to specific IP address ranges instead of selecting the devices from the network neighborhood, an autodiscovery must be executed before starting the actual rollout procedure.

Executing an Autodiscovery on the IP Address Range

1. In the left window pane of the console select the device which is to execute the autodiscovery of the network; this should be the relay under which the clients are to be located.
2. Then select the node **Agent Configuration** > **Module Configuration** > **AutoDiscovery** .
3. Open the module's parameters by selecting the **Edit** > **Properties** icon.

   The **Properties** dialog box appears on the screen.
4. Enter the indicated values for the following parameters and leave all others as they are:

Options	Description
Timeout (sec)	2
Address Range ;	enter the IP address range to scan
Address Verification Interval (sec)	2
Use Network Neighborhood	Yes

5. Then click **OK** to confirm the new parameters and to close the window.

   The autodiscovery will be launched immediately. You can follow its progress by going to the **Device List** tab.
6. Click the **Refresh** icon from time to time and you will see the list populated with the devices found by the relay.

Rolling out to a Specific IP Address Range

1. Launch the rollout creation wizard by selecting the **Wizards** > **Agent Rollout** item menu .

   The **Core Setup Configuration** window appears on the screen.
2. Check the box **Configure the relay selection or use master otherwise**.

   If you want to schedule the rollout at a specific date and time check the box .
3. Click **Next**.

   The **General Parameters** appears on the screen.
4. Enter the name of the new rollout (for example, Windows 7 Client Rollout) into the **Name** field.
5. Enter the name for the rollout package executable that will be created into the **Auto-extractible Name** field (for example, *win7clientagent11.exe*).
6. Select the operating system group to which the agent is to be rolled out from the drop-down list of the **Operating System** field (for example, *Windows 2000/XP/... (64 bit)*.
7. Click **Next**.

   The **Communication** window appears on the screen.

8. To find the relay click the **Import Devices from CSV File** icon next to the **Parent Name** field.
9. Click the **All** icon.
10. Select the desired parent device from the appearing list and click **OK**.
11. Click **Next**.

    The **Targets & Accounts** window appears on the screen.
12. When selecting the rollout targets from the autodiscovery you have two possibilities to do so:

    You may either select the targets from a general list displaying all autodiscovered devices

    .

    a) The tab is the preselected tab when the window is opened. It displays the list of all devices found by all devices executing autodiscoveries in the network. Select the device/devices to be added to the list by marking the different devices and moving them to the **Selected Devices** list to the right via the **Add** button.

    Be aware that you can select a maximum of 18 devices for your rollout with the evaluation license. The evaluation license allows you to test with a total of 20 devices, and you already installed the master and probably at least one relay.

    Be aware that you cannot add the master as a target device.

    b) Click the **OK** button to add the selected devices and close the window.

    You may make your selection from the autodiscovered list of a specific device.

    a) Select the **AutoDisc Device** tab () in the left window bar.

    The **Select a Device** window appears on the screen.

    b) Click the **All** button and then select the device that carried out the autodiscovery, that is, the parent relay in this example).

    The **Available Devices** field will now display the list of all devices found.

    c) Select the device/devices to be added to the list by marking the different devices and moving them to the **Selected Devices** list to the right via the **Add** button.

    Be aware that you can select a maximum of 18 devices for your rollout with the evaluation license. The evaluation license allows you to test with a total of 20 devices, and you already installed the master and probably at least one relay.

    Be aware that you cannot add the master as a target device.

    d) Click the **OK** button to add the selected devices and close the window.
13. Now click the **Add Administrator** icon.
14. Enter the required data for the account login into the respective fields.
15. Click the **Verify Rollout** button to make sure the entered account data are correct.
16. Click **OK** and then **Finish**.
17. In the following **Confirmation** popup window check the **Go to Rollout** radio button to change the focus of the console window to the new rollout. Click **Yes** to confirm the immediate activation.
18. If you have not checked the **Go to Rollout** box at the end of the wizard select the newly created rollout in the left tree hierarchy and then its **Servers** subnode.

    In the **Assigned Schedule** tab you can follow the general progress of the client rollout assignment.
19. Once this value reads `Executing` select the **Targets** tab to follow progress of each individual target through the **Status** column (initial status is `Initial`and final stage should be `Installed`).

You have now rolled out the Asset Core agent to a specific subnet of your infrastructure.

Making Agent Rollout More Efficient

Rolling out the Asset Core agents consists of first designing your infrastructure, rolling out the agents to the target devices, assigning them their typology type. Beyond that Asset Core offers many possibilities to adapt the agent rollout to your own needs and specifications.In the following chapters you can find out how to schedule the rollout at a given time, install via the Rollout Server Page, etc.

Scheduling the Rollout at a Given Date and Time

In the **Core Setup Configuration** window, make sure the box **Configure a custom schedule for this rollout (default is one immediate execution)**is checked.Then, after the **Targets & Accounts** window another window will be displayed, the **Schedule** window.

1. Select the **Validity** tab.
2. Define in the **Execution Date** box at what moment the rollout, is to be launched for the first time (for example, at the next startup of the device.)
3. Define in the **Termination** box defines when the rollout is to be run for the last time (for example, stop after 5 executions).
4. Select the **Frequency** tab.

   Here you can define the exact day, time and/or frequency at which the rollout is to be launched on the target. To run the rollout more than once only makes sense if you expect that some rollout execution tentatives may not succeed at the first try due to specific reasons.
5. Click the **Finish** button.

The rollout is now defined and scheduled to be executed at the specified time.

Rollout Server Page

The agent running on the rollout server has an additional page, the Rollout Server page. This page is only accessible via a browser through the following address: http://<rollout server name> :<rollout server port number> /rollout. This page can not be access through the regular agent interface. To log on to this page you must either have an admin login, the system login of the master machine, or a login specifically defined by the admin. For our first test this is the master and you may use the predefined login "admin" with no password.

The Rollout Server page provides the following information on all existing rollouts that are defined as being available on the respective rollout server:

Parameter	Description
Rollout Name	The name of the rollout as defined at its configuration in the Console.
Rollout Type	The installation operation executed by the rollout (that is, if it is an agent installation, reinstallation, or uninstall).

Parameter	Description
Operating System	The operating system type and version of the target devices.
Auto-extractible Name	This is the name of the rollout package -- the actual installation package of the agent as defined in the console. This entry is a direct link to the location of the package from which you can download it or launch it through the use of your mouse buttons.
Publication Date	This field displays the date and time at which the package was made available on this page for download.

Downloading and Installing a Rollout from the Rollout Server Page

This page makes all rollout packages on the server available for download by the clients that cannot be accessed directly by the rollout. To download and install proceed as follows:

1. To download a package right click its name and save it on the local client, or launch it directly for installation by double-clicking.
2. Before the actual download or installation process starts you must provide the password for the download a second time.

Uninstalling the Client Agent via Rollout

Agents that were installed via a rollout may also be uninstalled by rollout. The procedure is similar to the installation. The wizard created for this uninstallation uses the Master as the Rollout Server and the default schedule.

Creating the Uninstall Rollout

1. Launch the rollout creation wizard by selecting the **Wizards** > **Agent Rollout** item menu .

   The **Core Setup Configuration** window appears on the screen.
2. Select the **Uninstall** option from the **Select the action to perform for this rollout** drop-down list.
3. Click **Next**.

   The **General Parameters** appear on the screen.
4. Define the following parameters for your new rollout all others leave with their predefined values:
   - Enter the name for the rollout configuration, for example, XP 32-bit Uninstall in the Name field.
   - Enter the name for the auto-extractible file into the **Auto-extractible Name**if the uninstallation is to be also available for download on the Rollout Server agent interface, for example, FPAC_XP32BitUninstall.exe.
   - If the installation is to be executed silently, that is, without any user input on the target, on Windows devices check the **Silent mode Installation** box.
   - In the **Operating System** field select the appropriate operating system group.
   - If the agent was NOT installed in the default directory enter its installation directory in the **Installation Directory** field.
   - If the agent was NOT installed with its default service name enter its name in the **Agent Service Name** field.
5. Click **Next**.

   The **Communication** window appears on the screen. In this window the devices on which the agent is to be uninstalled must be selected as well as the administrator accounts to access them. To select the target devices there are several methods available. Since all targets have an agent installed the easiest method is to select them from the device list.
6. For this select the **Select a device** icon above the **Parent Name** field.

The **Select a Device** window opens on the screen.

7. Select the devices to be uninstalled from one of the tabs of the **Select a Device** dialog box.
8. Click **OK** to confirm and close the window.

   The devices are now added to the list window.
9. Now click the **Add Administrator** icon.
10. Enter the required data for the account login into the respective fields.
11. To add a new account click the **Add Administrator** icon.

    The **Properties** dialog box appears on the screen.
12. Enter the following data for a new account login into the respective fields:
    a) Enter the name of the domain to which the rollout is going into the **Administrator Domain** field. You may use an asterisk (*) if the rollout is going to all domains.
    b) Enter the login name of the admin as which the agent deployment tries to log on to the remote target to install the agent into the **Login** field.

    For Windows XP Professional rollouts you MUST enter a valid login and password, and it must be the same for all devices, that is, the rollout server (the master) as well as targets.

    If you are not sure that your local administrator login has the same passwords for all targets, use the domain login. For domain logins to work correctly, the necessary domain trust relationships must already have been set up between the different domain controllers.

    c) Enter the password of the above entered admin into the Password field. For security reasons the passwords will only be displayed in the form of asterisks (*).
    d) Confirm the above entered the password into this field.
    e) Click the OK button to confirm the new account and add it.

       It will now be shown in the list above.
13. Click the **Verify Rollout** button to make sure the entered account data are correct.
14. Click **OK** and then **Finish**.
15. In the following **Confirmation** popup window check the **Go to Rollout** radio button to change the focus of the console window to the new rollout. Click **Yes** to confirm the immediate activation.
16. If you have not checked the **Go to Rollout** box at the end of the wizard select the newly created rollout in the left tree hierarchy and then its **Servers** subnode.

    In the **Assigned Schedule** tab you can follow the general progress of the client rollout assignment.
17. Once this value reads `Executing` select the **Targets** tab to follow progress of each individual target through the **Status** column (initial status is `Initia` l and final stage should be `Installed`).

You have now uninstalled the Asset Core agent from all the defined target machines.

IMPORTANT

Devices that may not be accessed directly by the rollout because they are in another domain or behind a firewall or for any number of other reasons must download the uninstall package from the Rollout Server page of the server's agent browser interface and execute it. To access the server enter http://<rollout server name> :<rollout server port> /rollout into the browser.

Advanced Rollout

The instructions in the preceding chapters enable you to efficiently use rollout. This section will give you a better understanding of the functionalities and components of the rollout system.

The most important concepts of rollout are explained in this section, including:

- answers and explanations to questions you might have
- flowcharts that illustrate processes
- overviews of where to find the component in the Console
- examples and recommendations
- references to all related tasks

Rollouts

The Rollout includes two separate modes in order to fulfill the maintenance operations. The active mode (Push) prepares and installs Asset Core agents on remote devices while the passive mode (Pull) bundles the Asset Core software so it can be downloaded and installed manually by end users via a specific page on the agent interface.

Rollout folders are created as organizational containers for different types of rollouts. They may contain any number of predefined or custom-made rollouts for the management of the client system.

The Asset Core Rollout makes the installation, reinstallation, or uninstall of the Asset Core agent on your client population a quite simple and quickly executed task. All different installation possibilities are executed through the same operation.

A rollout is configured via the parameters provided by the rollout's subnodes:

- Agent Configuration
- Post-Install
- Servers

Post-Install

The **Post-Install** node allows you to add and edit a script to be executed after the rollout of the agent has terminated and to add files to be installed on the remote client. This may be to finetune agent settings for a specific machine or to simply add some individual configuration files.

The **Post-Install** node has the following tabs:

- **Script**
- **Files**

Script

The **Script** tab allows the administrator to write and edit a script in the Chilli language to be executed after the termination of the rollout process of the agent on the managed device. This script defines the actions to execute after a rollout has successfully taken place and what is to be done with the files that were added with the script. The default location of the script is `[Installation Directory]/data/CoreUtils` on the client device, and it will be created and stored on the master when you leave the **Post-Install** node.

Files

The **Files** tab provides you with the possibility to add files to the rollout package which will be installed or added on the local client after the actual rollout procedure. In which way they are to be treated is defined through the script explained in the preceding tab.

By default the list is empty, however, as soon as the script has been created it will be automatically added to the list. The table displays the following information about the added files:

Parameter	Description
Name	Displays the name of the file to be installed or added on the client machine.
Define the destination path on the client for the selected files:	Shows the path, either full or relative to the agent, where the file is to be installed on the client device.

Servers

The actual rollout is managed and executed by a rollout server. This node provides access to all rollout servers to which the current rollout is assigned to. A rollout may be assigned to more than one server. The table displays the following information about the servers:

Parameter	Description
Name	The name of the rollout server.
IP Address	The IP address of the rollout server.
Operating System	The operating system running on the rollout server.

Servers

Rollouts are managed by authorized Asset Core administrators through the console. When using Push Rollouts, the underlying maintenance operations are delegated to elected Asset Core agents, the Rollout Servers. Hence, any already deployed Asset Core agent may be considered as a possible management point concerning the Asset Core deployment task.

Note

Rollout servers are not limited to executing rollouts to clients of their own operating system family. They may roll out the Asset Core agent to clients of any supported operating system, with the exception of Windows systems: A Windows rollout can only be managed by a Windows Rollout Server.

Adding a Rollout Server

You may directly add a device as a Rollout Server under the **Servers** node. Any device that fulfils the predefined requirements can be a Server in Asset Core . The master is a rollout server by default. To define a device as a rollout server proceed as follows:

1. Go to the **Servers** node in the left window pane.
2. Then select the **Edit** > **Add Rollout Server** icon.

   The **Add a new rollout server** popup window will appear on the screen displaying the list of all devices, that may be a server due to their operating system.
3. Select the device to be added from one of the list boxes.
4. Click **OK** to confirm and close the window.

The device will be added to the table of Servers and its configuration parameter will be updated accordingly.

Rollout Server

The actual providing and sending of installation files and scripts will be managed by the rollout server. The prerequisite for a machine being used as a rollout server is that Windows Installer version 2.0 or later is installed. If the rollout server is on the master, this version will automatically have been installed via the master installation. If the Windows 2000 Service Pack 3 or later has been installed the client will have the correct version.

Assigned Schedule

The **Assigned Schedule** tab displays the execution schedule defined for the selected rollout. It allows you to modify this schedule an/or to reassign the rollout to its targets.

Generating the Rollout Package

If the rollout is to be available on the Rollout Server page of the HTML agent interface for 'pulling' the rollout to the device and then installing it (formerly *Pull Rollout*), a specific self-extracting installation package must be generated.

Select the **Edit** > **Generate Rollout Package** icon.

The package is immediately generated and made available on the Rollout Server and its browser page.

Starting a Rollout

Once all the configuration of a rollout is defined and it is assigned to its targets and its schedule specified, it can be launched:

Select the **Edit** > **Start Rollout** icon in the icon bar.

The rollout will be launched immediately ignoring any schedule that may be defined for it.

Scheduling the Rollout at a Given Date and Time

In the **Core Setup Configuration** window, make sure the box **Configure a custom schedule for this rollout (default is one immediate execution)**is checked.Then, after the **Targets & Accounts** window another window will be displayed, the **Schedule** window.

1. Select the **Validity** tab.
2. Define in the **Execution Date** box at what moment the rollout, is to be launched for the first time (for example, at the next startup of the device.)
3. Define in the **Termination** box defines when the rollout is to be run for the last time (for example, stop after 5 executions).
4. Select the **Frequency** tab.

   Here you can define the exact day, time and/or frequency at which the rollout is to be launched on the target. To run the rollout more than once only makes sense if you expect that some rollout execution tentatives may not succeed at the first try due to specific reasons.
5. Click the **Finish** button.

The rollout is now defined and scheduled to be executed at the specified time.

Targets

The **Targets** tab provides access to all devices which are defined as rollout targets. This list may be filtered according to the device rollout status.

Filtering Rollout Targets

To display only a reduced number of target devices assigned to this rollout you may filter these via their different status values. To do so proceed as follows:

1. Click the **View** dropdown list above the table.

   This list provides you with the following status values according to which you can sort the assigned devices:

Status	Description
All Status	to display the assigned devices of all different types of status
`Initial`	the rollout was not yet launched
`Successful`	the rollout was successfully terminated on the device
`Failed`	the rollout failed to execute successfully on the device
`Processing`	the rollout is still being executed

2. Select the desired status value.

The table will update its contents and display only those devices of which the status value corresponds to the one you selected.

Adding a Device from the List of Autodiscovered Devices

Devices may be added to the list of rollout targets through a number of different ways. One is through different types of lists.

ATTENTION

Be aware that you cannot add the master as a target device.

One of these lists is the list of autodiscovered devices:

The AutoDiscovery module provides a list of all devices of any type found in the network, such as printers or devices with and without the agent installed. This list is also available for the rollout functionality to facilitate the selection of the rollout targets. However, the list displayed in this case will only show all clients of type device and only those with a status of `Verified` or `Learned`, which means that all devices in this list have been verified for existence either by the local client or a neighbor client and exist on the network. To add a device from the list of all autodiscovered devices known to the database proceed as follows:

1. Select the **Edit** > **Import Devices from CSV File** icon.

   The **Select Devices from the List** window opens which provides you with its different methods, with the **AutoDisc Object** tab preselected in the left window bar.

   On the top of the **Available Devices** box there are two drop-down lists which allow you to filter the autodiscovered objects thus reducing the list to your needs. The following filters are available:

- You may filter for the type of the autodiscovered object, that is, if all found devices are to be shown, or only PCs, printers, switches, etc. and you may limit the list to either devices with or without the Asset Core agent already installed.
- The field **Available Devices** displays the list of all available devices.
- Below, the option **Use IP Address** allows you to select the device by IP address. By default this option is not activated, meaning that the device is selected by its name.

2. Select the device/devices to be added as targets from the list
3. Then click the **Add** button to move the selected devices to the list of **Selected Devices**.
4. Click **OK** to confirm the selections and close the window.

The selected device(s) will now be added to the list of targets with the initial status `Initial`.

Adding a Device from the List of Devices Discovered by Another Device

Devices may be added to the list of rollout targets through a number of different ways. One is through different types of lists.

ATTENTION

Be aware that you cannot add the master as a target device.

One of these lists is the list devices discovered by another device:

The tab **AutoDisc Device** allows you to select your target devices from a list of autodiscovered devices by one specific network device.

1. Select the **Edit** > **Import Devices from CSV File** icon.
2. Select the **AutoDisc Device** tab in the left window bar.

   The **Select a Device** window opens on the screen.
3. Select the device of which the autodiscovered list is to be used from one of the tabs of the **Select a Device** dialog box.

   The list of groups and devices provided in this window includes groups and members of synchronised directory servers.
4. Click **OK** to confirm the selections and close the window.

   The field **Available Devices** displays now the list of all devices which were discovered by the selected network device.
5. Select the device/devices to be added as targets from this list
6. Then click the **Add** button to move the selected devices to the list of **Selected Devices**.
7. Click **OK** to confirm the selections and close the window.

The selected device(s) will now be added to the list of targets with the initial status `Initial`.

Adding a Device from the Microsoft Network Neighborhood

Devices may be added to the list of rollout targets through a number of different ways. One is through different types of lists.

ATTENTION

Be aware that you cannot add the master as a target device.

One of these lists is the Microsoft Network Neighborhood:

1. Select the **Edit** > **Import Devices from CSV File** icon.
2. Select the **Network** tab in the left window bar.

The field **Available Devices** displays now the **Microsoft Windows Network Neighborhood** structure on the screen

3. Select the device/devices to be added to the list from one of its groups.
4. Click **OK** to confirm the selections and close the window.

The selected device(s) will now be added to the list of targets with the initial status *Initial*.

Adding a Device from a CSV List

Devices may be added to the list of rollout targets through a number of different ways. One is through different types of lists.

ATTENTION

Be aware that you cannot add the master as a target device.

One of these lists is a CSV list that contains the respective devices.

1. Select the **Edit** > **Import Devices from CSV File** icon.
2. Select the **CSV List** tab in the left window bar.

   A window opens, in which you may choose the file containing the device list.
3. Click the **Open** button at the bottom of the window to open the list.

   The field **Available Devices** displays now the list of all devices contained in the selected CSV list.
4. Check the box **Header**, if your CSV file has a title line which is to be removed.
5. Select the device to be added to the rollout from the list in the window.

   You may also select all devices in the list by using the **Select All** button.
6. Click **OK** to confirm the selections and close the window.

The selected device(s) will now be added to the list of targets with the initial status Initial.

Adding an Existing Device

You may also add a device by directly entering its name. To do so proceed as follows:

ATTENTION

Be aware that you cannot add the master as a target device.

1. Select the **Edit** > **Add Device** icon.

   The **Select a Device** window opens on the screen.
2. Select the device to be added from one of the tabs of the **Select a Device** dialog box.

   The list of groups and devices provided in this window includes groups and members of synchronized directory servers.
3. Click **OK** to confirm the addition and close the window.

Manually Adding Targets

You may also add one or more devices by typing their name or address. To do so proceed as follows:

ATTENTION

Be aware that you cannot add the master as a target device.

1. Select the **Edit** > **Add Existing Device** icon.

   The **Add a Device** dialog box appears on the screen.

2. Enter the name of the device to be added to the list into the respective field. The name may be entered
   - either as its short or long network name, for example, scotty or scotty.enterprise.com or as its IP address, for example, 159.124.5.10,
   - or as a comma separated list of names and/or ranges, for example, scotty;
   - 192.168.4.45-192.168.4.47 which includes machines scotty.enterprise.com, 192.168.4.45, 192.168.4.46 and 192.168.4.47.
   - A range may also be entered as CIDR notation in the form of 192.9.205.22/18.
3. Click **OK** to add the device and close the window.

Verifiying the Rollout

The **Verify Rollout** action verifies the validity of domain/username/password on the rollout server and on the target devices prior to launching a rollout. If no targets have been defined yet, the server account only will be verified. If one or more devices are specifically selected in the table only those are verified. To verify the rollout proceed as follows:

1. Select the target device(s) if specific devices are to be verified or do not make any selection to verify all targets in the table in the right window pane.
2. Then select the **Edit** > **Verify Rollout** icon.

A message box will appear on the screen with the result of the verification for each device.

Displaying the Rollout Log File

Logging of rollout is not included in the general logging in the mtxagent.log file, it is written in its own specific log file, the mtxsetup.log, which is located in the [Installation Directory]\master\data\rollout directory. It is possible to directly access the log file of a specific client assigned to the currently selected rollout. Be aware that this option is only available for devices with an established connection, it is never available for unconnected, retired or unknown devices. To do so proceed as follows:

1. Select the target device in the right window pane.
2. Select the **Edit** > **Display Log** icon.

   A new window will appear on the screen, displaying the contents of the log file of the rollout on the selected client.

   The log displays the date and time at which the action occurred, the name of the operational rule the action executed, a letter(s) that indicates of which type the explanation following is, such as ERR for error or T for trace, etc. as well as the description itself.
3. Click the **Close** button to close the window.

Reassigning a Rollout

If targets failed to install during a rollout, they may be reassigned and thus reexecuted.

1. Select the devices to which the rollout is to be reassigned, or do not assign any device in the table if the rollout is to be reassigned to all targets shown in the table to the right.
2. Select the **Edit** > **Reassign Rollout** icon.

   A confirmation window appears on the screen.
3. Click **Yes** to confirm the reassignment and launch it according to its schedule.

Generating the Rollout Package

If the rollout is to be available on the Rollout Server for "pulling" the rollout to the device and then installing it (formerly Pull Rollout), a specific package must be generated

Select the **Edit Generate Rollout Package** icon.

The package is immediately generated and made available on the Rollout Server.

User Accounts

Specific login accounts may be defined to be used for the rollouts. These logins will then try to log on to the device to execute the rollout in the order in which they are defined. The logins are tried in the order they are defined in the table, and once a login is successful all further accounts will be ignored

Adding an Account to the Rollout Deployment

To add an account to the rollout deployment proceed as follows:

1. In the **User Accounts** tab select the **Edit** > **Add Account** icon.

   The **Properties** dialog appears on the screen.
2. Enter the required data for the new account login.
3. Click the **OK** button to confirm the new account and to close the window.

Automatically Rolling out the Asset Core Agent via the Wizard

The definition and execution of the different rollouts to be executed in the network may be done manually by creating the rollout and then defining all options, or they may be created via the **Agent Rollout** wizard. This wizard creates a new rollout from scratch with all the required settings and sends it to the list of targets. The preentered values are those defined during the installation of the master.

The wizard is available directly on the main **Wizards** menu from anywhere in the Console, or it may be called from specific locations in the console.

1. Select the **Wizards** > **Agent Rollout** menu item from the menu bar.
2. The first wizard window appears on the screen.

Core Setup Configuration

The first step allows you to specify which aspects of an agent rollout require specific configuration and for which the default values may be used.

1. For the first question select the type of rollout to be executed from the drop-down list. Depending on your choice a number of the following questions may be greyed out.
2. Answer the following questions by checking or leaving unchecked the box. Checking the box will add the respective step to the wizard in which you will need to provide information.
3. If you have selected to create a task for this operation, the **Create Task** box appears below and, if tasks of type **Agent Rollout** exist, you may also select to add this rollout to one of the existing tasks by checking the **Use Existing Task** box and selecting it from the drop-down list.
4. Once you have answered all questions click **Next** to start the rollout configuration.

General Parameters

This window is one of the two mandatory wizard steps that will always be part of the rollout configuration, as it defines is basic parameters. The following parameters must be defined for a rollout to work:

1. Enter a name into the respective field.
2. Enter a name for the auto-extractible file, if the rollout is to be made available on the browser interface page of the **Rollout Server**.

   This may be necessary if the rollout is assigned to devices that may not be accessed directly by the rollout. This may be the case if they are in another domain or behind a firewall or for any number of other reasons. For these cases the install package must be downloaded from the Rollout Server page of the server's agent browser interface and executed locally.
3. Select the operating system for which the rollout is to be created.

4. Define the installation directory if another than the default directory is to be used.
5. Define the agent service name if another than the default name is to be used and define its startup type.
6. Click **Next**to go to the following wizard page.

Communication

This window defines the communication settings between the agent to be installed and its parent, such as the parent name and port, the port for inter-agent communication, connection timeout values. and tunnel definitions. The predefined values in this window are the parameter values defined for the master; therefore, if the agents to be rolled out have the master as their parent, no changes are required here.

For any other cases, you have the following options to define the relay:

- Define another static relay,
- Use the automatic relay selection and one or more of its proposed methods to find the relays.

Defining a Static Relay

To define a static relay for the agent targets:

1. Enter the range of ports on which the HTTP server will listen for and send data from into the **Port** field.
2. Enter the number of the port the Console uses for its communication into the **Console Port** field.
3. Enter the name of the direct parent directly into the **Parent Name** field or select it from the list of available devices. The displayed list is pre-filtered to show only those devices for which the *Relay* option is activated. If no value is entered, the master is used by default.
4. Enter the number of the port on which the new agent connects to its parent into the **Parent Port** field.
5. Click **Next** to continue.

Defining Automatic Relay Selection

Automatic relay selection allows the clients to try to find their relay using one ore more specifically selected methods in the order that they are defined. If one method cannot find a relay it returns and the next method in the list will be tried.

1. Select the **Auto-Select Relay** radio button.
2. In the **Available Relay Selection Methods** box select the first method to be used to find the relay.
3. Click the **Add** button.
4. Enter the required parameter values in the **Properties** window.
5. The method will move to the**Selected Methods** box to the right.
6. Repeat these steps for all methods that are to be used for finding a relay.
7. If you want to make changes to the order, select the method to move in the **Selected Methods** box and click the **Move Up** or **Move Down** icons above the box until the method is at the desired place.
8. Click **Next**.

Defining Communication Specific Parameters

If you require specific settings for the agent communication with the relays, you can define these:

1. Select the **Advanced** tab.
2. Make the required changes in the available parameters.
3. Click **Next**.

Security

The parameters in this window define the settings on how the communication between the agents is secured. The preentered default values are those defined for the master. To use those no modifications are required. Otherwise make the necessary changes to the fields of the window.

> **Note**
>
> Don't forget to define the certificates and authorities if you are using secured communication with mutual authentication, otherwise the agents will not be able to communicate.

Click **Next** to continue.

User Interface and Reboot Management

The parameters defined in this window concern the user interface, that is, the information, if any, displayed in the systray and the way rebooting the device is managed by the Asset Core agent. The default settings are:

- **User interface**

  The Asset Core agent icon is displayed in the systray dynamically with all its different possible status and colour changes.
- **Reboot Management**

  A message box is displayed on target device for a reboot request and the reboot waits for a maximum of 5 minutes before executing.

Make any changes as required and then click **Next** to continue.

Logging

The logging parameters define the basic settings for the main agent log file (that is, the values specify the granularity of the contents of the main agent log file, as well as their output location, the amount of information to keep, and the displayed types, for example.)

Make any changes as required and then click **Next** to continue.

Modules

This window provides the list of all available modules that may be installed on the target device and loaded at startup for the selected operating systems according to your licences. The default modules are pre-checked. Modules which are required for the basic functioning of the agent are listed with the mandatory icon (✓) and cannot be unloaded.

1. To load or unload a module for the target device select it in the table.
2. Then either select the **Edit** > **Load Modules** or **Edit** > **Unload Modules** / icon.

   The icon of the selected modules will be automatically changed to indicate its modified loading status via the **Yes**/**No** icon (✓/✗).

Configuring the Modules

It is also possible to directly configure a number of the modules from here. Be aware that not all modules may be preconfigured by the rollout; modules such as OsDeployment may only be configured directly on the device. If a module is specifically configured, the **Customized** icon is displayed in the respective column. The relay module will always be shown as configured, as it was automatically adapted with the parent information.To configure a module proceed as follows:

1. Select the respective module in the table.
2. Then either select the **Edit** > **Properties** icon.

   The **Properties** window appears on the screen.

   It displays all module parameters which are configurable.
3. Make the necessary modifications
4. Click the **OK** button at the bottom of the window to confirm the modifications or click **Cancel** to abandon without modifications and to close the window
5. Click **Next** to continue.

Rollout Server

This window defines the Rollout Server to use for this rollout. By default the Master is defined as Rollout Server. You can either use another already existing server by selecting it in the table or add another one in this step.

1. Select the **Add Device** icon on top of the table.

   The **Add a new rollout server** popup window will appear on the screen displaying the list of all devices, that may be a server due to their operating system.
2. Select the device to be added from one of the list boxes.
3. Click **OK** to confirm and close the window.
4. The device will be added to the table of available servers and selected.
5. Click **Next** to continue.

Targets & Accounts

This window is the second obligatory step of the rollout wizard, as it defines the target devices and the credentials to access them.

Rollout Targets

In the first part of the window the rollout targets are defined. Be aware that you cannot add the master as a target device. Devices may be added to the list of rollout targets through a number of different ways:

Once all devices are added click **Next** to continue.

Rollout Accounts

Specific login accounts may be defined to be used for the rollouts. These logins will then try to log on to the device to execute the rollout in the order in which they are defined. The logins are tried in the order they are defined in the table, and once a login is successful all further accounts will be ignored.

1. Now click the **Add Administrator** icon.
2. Enter the required data for the account login into the respective fields.

   The access to the devices must be defined in the same way as for the installation before you can schedule the rollout.
3. To add a new account click **Add Administrator** .

   The **Properties**dialog box appears on the screen.
4. Enter the following data for a new account login into the respective fields:
   a) Enter the name of the domain to which the rollout is going into the **Administrator Domain** field. You may use an asterisk (*) if the rollout is going to all domains.
   b) Enter the login name of the admin as which the agent deployment tries to log on to the remote target to install the agent into the **Administrator Login** field.

   You may provide the login as one of the following possibilities:

   - as the 'simple' login name of a local user of the remote machine, such as Administrator
   - as .\login for a local login, or
   - as domain\login for a domain login of the administrator, such as LAB\TEST. The domain part may be set to a dot (.) to indicate the local machine.

   For Windows XP Professional rollouts you MUST enter a valid login and password, and it must be the same for all devices, that is, the rollout server (the master) as well as targets.

> If you are not sure that your local administrator login has the same passwords for all targets, use the domain login. For domain logins to work correctly, the necessary domain trust relationships must already have been set up between the different domain controllers.

c) Enter the password of the above entered admin into the Password field. For security reasons the passwords will only be displayed in the form of asterisks (*).
d) Confirm the above entered the password into this field.
e) Click the OK button to confirm the new account and add it.

It will now be shown in the list above.

5. Click the **Verify Rollout** button at the bottom to make sure the credentials are correct.
6. Click **Finish**.
7. Click Next to continue with the wizard.

Post-Install

This window allows you to create a script in the BMC Software proprietary Chilli language after the installation of the agent has finished and/or to add files to the rollout package.

Script

In this box you add and edit a script to be executed after the rollout of the agent has terminated, and add files to be installed on the remote client. This may be to fine-tune agent settings for a specific machine or to simply add some individual configuration files.

> **ATTENTION**
>
> The script must be in the BMC Software proprietary Chilli language and follow all its rules. You can find Information concerning the Chilli programming language in the Chilli manual which is delivered with the Asset Core software.

1. To create a post-installation script enter it into the box below.
2. After you finish the script and click Next button, the agent will try to compile the script to verify it is correct. If it is not correct, an error message will appear on the screen.

Files

The **Files** box allows you to add files to the rollout package which will be installed or added on the local client after the actual rollout procedure. The way they are to be treated is defined through the script defined above.You may define one file to be copied to several different locations on the device by repeating the following procedure for the file and each target location:

1. Select the **Add Postinstall File** icon above the list box.

   The **Add a Postinstall File** window appears on the screen.
2. Select the required file from the file hierarchy displayed in the list window.
3. Click **OK**.
4. Enter its target path in the **Define the destination path on the client for the selected files:** popup window.
5. Click the **OK** button to confirm the addition and to close all windows.
6. Click **Next** to continue.

Schedule

Now that the rollout, as well as the members have been defined, it may be scheduled to execute at a specific time. By default it is scheduled to execute once and immediately. If this is your choice you do not need to make any modifications in this window. To schedule the rollout for a specific moment proceed as follows:

1. Check the **Available on Rollout Server** box, if the rollout is to be made available on the Rollout server (that is, if you have target devices that cannot be reached directly by the rollout).
2. Check the **Allow 32 bit Agent Installations on 64 bit Architecture** box if
3. If the rollout targets are Windows devices select the connection mode that is to be used from the **Windows Connection Mode** drop-down field.
4. In the **Assignment Date** box select at what moment the assignment to the target devices is to be launched. The assignment in this case means that the link between the rollout and the target will be established and the rollout package will be sent.
5. Select the **Validity** tab.
6. Define in the **Execution Date** box at what moment the rollout is to be launched for the first time.
7. Define in the **Termination** box defines when the rollout is to be run for the last time.
8. Select the **Frequency** tab. Here you can define the exact day, time and/or frequency at which the rollout is to be launched on the target. To run the rollout more than once only makes sense if you expect that some rollout execution tentatives may not succeed at the first try due to specific reasons.
9. Click **Next** to continue if you have specified to create a task or click the **Finish** button to confirm all settings, create the rollout as defined and launch its execution.

Task

This step of the wizard allows you to create a task for the rollout defined via this wizard or to assign it to an existing task. This option is only available if you have checked the corresponding box in the first window of the wizard.

1. Define all parameters for the task that is to follow this rollout.
2. When you have made your selections click **Finish** to confirm all choices and launch the process.

Confirmation

A confirmation window appears on the screen. To directly move the focus of the console to the newly created rollout check **Go to Rollout**. If you have also created a task for this operation, this check box will also be available and you may select to move the focus of the console to the task by checking this box.

Click **OK** to confirm all definitions and create and start the rollout.