Architecture

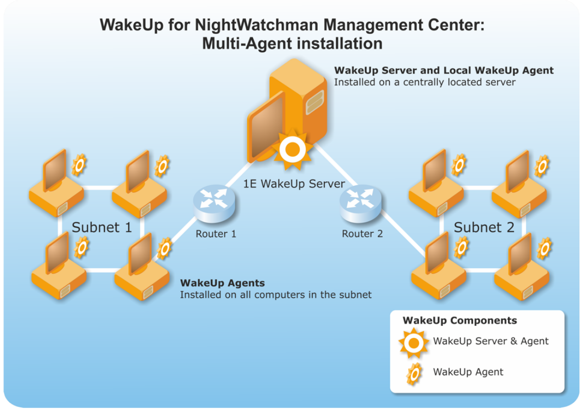
If you use WakeUp, you must either integrate WakeUp Server with NightWatchman Management Center or with Microsoft's System Center Configuration Manager (ConfigMgr or SCCM).

If you integrate WakeUp Server with NightWatchman Management Center, only one WakeUp Server installation is required as it is registered with NightWatchman Management Center as the master wake up service. As the WakeUp Server acts as the conduit for all wake ups, install it on a centrally located and well connected server.

The 1E WakeUp agent module in the Tachyon Agent is installed on every computer. The centrally located WakeUp Server communicates with the remote subnet, dynamically selecting agents to distribute wake ups locally on their subnets. Using the Last Man Standing feature, WakeUp agents collaborate to ensure that there is always one agent awake per subnet to receive wake up list instructions.

On this page:

> In this and the following diagrams, "WakeUp Agent" refers to the WakeUp agent module in the Tachyon Agent.



WakeUp for NightWatchman Management Center:
Multi-Agent installation
WakeUp Server and Local WakeUp Agent
Installed on a centrally located server
1E WakeUp Server
Subnet 1
Router 1
Router 2
Subnet 2
WakeUp Agents
Installed on all computers in the subnet
WakeUp Components
WakeUp Server & Agent
WakeUp Agent

Secure communications

WakeUp supports encryption for the packets used for communications between the WakeUp Server and agents. You can choose the level of security at installation.

- Full – all communications are encrypted and any unencrypted packets are ignored. If used then all WakeUp Servers and agents must used this option.
- Partial – both encrypted and unencrypted communications are allowed by the server. This can be a useful half-way solution to a fully encrypted configuration that caters for the scenario where you are upgrading an existing WakeUp installation to use encryption and you do not want to re-install every single component in one go. Unencrypted packets sent by the previous version clients can be used by the server. However, the upgraded server will only send out encrypted packets and therefore previous-version clients cannot be used as Primary or Alternate Agents
- None – all packets are unencrypted

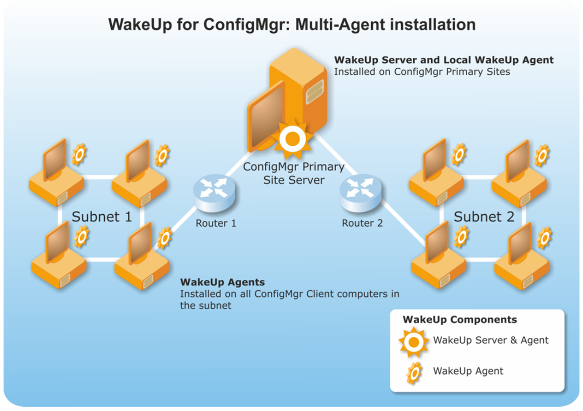
Alternatively you can enable FIPS-compliant encryption, but this is used for all communication between agents and WakeUp Server, and between agents and NightWatchman Management Center. If used, then all NightWatchman and WakeUp components must have FIPS enabled.

Multi-Agent mode

This is the recommended installation mode providing the most flexibility and functionality. Install the WakeUp agent on all target computers in your environment.

The features that come with this configuration are:

- Last Man Standing
- Network wake state reporting
- NightWatchman auto shutdown – NightWatchman will shutdown after being woken up by a Configuration Manager scheduled job
- Configuration Manager acceleration – policy refresh and hardware inventory refresh



WakeUp for ConfigMgr: Multi-Agent installation
WakeUp Server and Local WakeUp Agent
Installed on ConfigMgr Primary Sites
ConfigMgr Primary
Site Server
Subnet 1
Router 1
Router 2
Subnet 2
WakeUp Agents
Installed on all ConfigMgr Client computers in the subnet
WakeUp Components
WakeUp Server & Agent
WakeUp Agent

When using multi-agent mode, deploy the 1E Wakeup agent module in the Tachyon Agent to all systems in the environment. While technically each subnet requires only one system with the Wakeup agent powered on and running, delays and unexpected failures can occur when attempting to wake-up collections of machines where not all the systems have the WakeUp agent installed.

Dedicated Agent mode

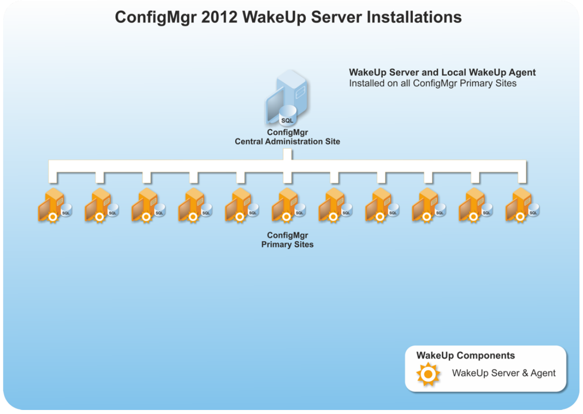
This mode is not generally recommended as it does not support Last Man Standing, wake state reporting or NightWatchman auto-shutdown – it is only for backward compatibility. In this mode, a single machine on each remote subnet is identified as an agent. The WakeUp Server communicates only with this agent and it means that the dedicated agent machine must remain on at all times in order to be able to process server communications.

In order to reduce the size of the agent package, run the installation on the nominated dedicated agent with a Tachyon client installation command-line with the AGENTTO and REPORTINGSERVER parameters. AGENTTO specifies the FQDN or NetBIOS name for the server where WakeUp Server is installed and REPORTINGSERVER specifies the FQDN or NetBIOS name for the server where the NightWatchman Management Center Web service is installed. There are other parameters you can set at installation.

No other action is required as the agent automatically registers with the controlling Primary Site once the service starts. It is also possible to install an alternate dedicated agent to provide redundancy if one of the agents needs to be taken offline. Simply install it using the command-line above.

Although you can configure a second host as dedicated agent on a subnet, the last dedicated agent host to start up on that subnet becomes the primary agent for that subnet. There is no alternate agent under these conditions and therefore no Last Man Standing feature.

Integration with Microsoft System Center Configuration Manager


ConfigMgr 2012 WakeUp Server Installations
WakeUp Server and Local WakeUp Agent
Installed on all ConfigMgr Primary Sites
SQL
ConfigMgr
Central Administration Site
SQL
ConfigMgr
Primary Sites
WakeUp Components
WakeUp Server & Agent

If you integrate with Configuration Manager, the WakeUp Server must be installed on all Primary Sites. Although it is possible, we do not recommend installing the WakeUp Server on the Central Administration Site (CAS) as it provides no advantage because the CAS does not have any clients reporting to it directly. WakeUp Server will monitor Configuration Manager for pending advertisements and send out wake up requests before they are due. You can also right-click on a collection of machines or a single machine to wake it up immediately.

Configuration Manager acceleration provides the option of combining a wake up with a Policy Refresh, so that any machines already awake will process the advertisement at the same time. You can also perform Policy Refresh without wake up.

You will need the following:

- Installation account – must be a domain user account with local admin rights on the server where the WakeUp Server is installed and read-rights to the Site object in Configuration Manager. It is used to install, configure and integrate WakeUp Server with Configuration Manager.
- The Hardware Inventory client agent must be enabled
- The Advertised Program client must be enabled
- Machine must be a Configuration Manager client
- NightWatchman Management Center 7.1 or later must already be installed if you are using Web WakeUp or integrating with NightWatchman Management Center.

Non-administrator account requirements

Users with local administrator rights on the server automatically have the ability to send wake-ups or make changes in the WakeUp console, either locally or remotely. In order for a non-administrator to send wake-ups or make changes to the WakeUp Server**,** their account requires full permissions on the WakeUp Server WMI namespace and for remote access, remote DCOM rights.

The WakeUp Server installation automatically configures the necessary WMI and DCOM rights for the AD account or group specified in the NightWatchman Management Center Configuration installer screen (Apply WMI Namespace). Installation automatically grants WMIACCOUNT full permissions on the root\N1E namespace and adds it to the Distributed COM Users local group.

As best practice, we recommend that you create an AD group for all the accounts that need to use WakeUp Server, who are not already local administrators of the server, and specify this group as WMIACCOUNT during installation. Typically, this AD group will contain the following AD accounts and groups:

- The service account for the NightWatchman Management Center console service, if using NightWatchman Management Centea with or without Web WakeUp

- Configuration Manager administrator accounts and groups, if using remote Configuration Manager consoles with WakeUp extensions
- WakeUp Server administrators and operators, if using remote WakeUp Server consoles

In addition to WMIACCOUNT, other accounts and groups can be manually granted remote administration rights to the WakeUp Server by granting full rights on the N1E namespace and adding the same accounts and groups to the Distributed COM Users local group on the server. We provide a free tool called `WmiConfigPerms` which is available on our website.

To add an additional AD group or local groups such as SMS Admins to the N1E namespace, use:

```
WmiConfigPerms.exe /A:ADD /N Root\N1E /M "<domain>\<group>":"
EXEC_METHODS|FULL_WRITE|ENABLE_ACCOUNT|REMOTE_ENABLE" /R
```

Configuration Manager administrative users

Configuration Manager administrator accounts and groups are all members of the SMS Admins local group on the server. Its membership is automatically managed from the Configuration Manager Console when creating and deleting administrative users. It is possible to specify WMIACCOUNT as SMS Admins, and the installer will grant this local group full WMI rights on the N1E namespace. This enables all Configuration Manager administrators to send wake-ups using WakeUp extensions and also make changes in the WakeUp Server console.

However, if SMS Admins is specified, the WakeUp Server installer adds this local group to the Distributed COM Users local group. Nesting of local groups is not technically supported, and SMS Admins can be safely left or removed. The SMS Admins group is created and configured with remote WMI and DCOM rights during the installation of the Configuration Manager Site role SMS Provider, therefore there is no requirement for it or its members to also be members of the Distributed COM Users local group.

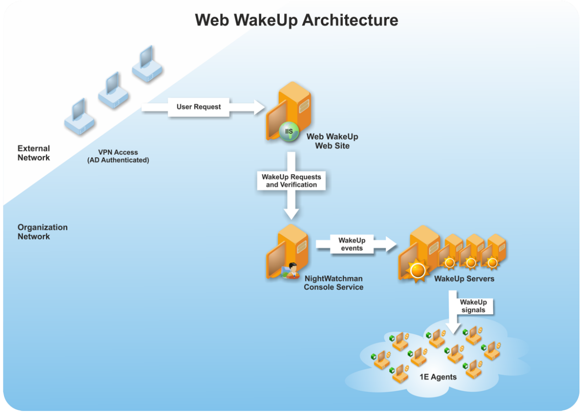
By default, the Distributed COM Users local group has COM Security that allows local and remote access, launch and activation. If the default rights have been modified, it may be necessary to manually configure DCOM security using `dcomcnfg.exe` to grant remote access, launch and activation rights to WMIACCOUNT and other WakeUp Server administrator accounts.

Web Wakeup architecture

The Web WakeUp architecture illustrates how its components interact with each other and other objects in your network. Web WakeUp uses:

- The Web WakeUp Website – the interface to the application and communicates with the NightWatchman Console service.
- The NightWatchman Console service – retrieves computer details from the NightWatchman Management Center database and sends wake-up events to the WakeUp Servers.
- The WakeUp Server – distributes wake-ups to target computers, typically through its WakeUp agents. This includes the WakeUp provider that enables wake-ups to be configured using WMI.

The Web WakeUp website and the NightWatchman Console service may be located on different servers as long as the Web WakeUp application pool has access to the network. You must carry out post-installation configuration on both the Web WakeUp website and the NightWatchman Console service computer.


Web WakeUp Architecture
User Request
IIS
Web WakeUp Web Site
External Network
VPN Access (AD Authenticated)
WakeUp Requests and Verification
Organization Network
WakeUp events
NightWatchman Console Service
WakeUp Servers
WakeUp signals
1E Agents