# SmartSpace®

## SmartSpace Using Unicast Cluster Setup Guide

From version 3.5.2

Ubisense Limited, St Andrew's House, St Andrew's Road, Cambridge CB4 1DL, United Kingdom.

Telephone: +44 (0)1223 535170. Website: https://www.ubisense.com

Ubisense Limited
St Andrew's House
St Andrew's Road
Cambridge CB4 1DL
United Kingdom

Tel: +44 (0)1223 535170

WWW: *https://www.ubisense.com*

# Contents

# Overview of Smart Space Using Unicast Cluster

This document explains how to set up Ubisense SmartSpace to run with services distributed across multiple machines without multicast. This makes use of the unicast cluster support in the Ubisense platform.

# Motivation

Ubisense protocols make use of multicast to communicate between all relevant machines on the network. When multicast is not available, the system must know in advance the addresses of the other machines running Ubisense services. The following sections outline how to set up a cluster of Ubisense server machines operating in unicast to implement a SmartSpace system.

# Configuring the platform

The basic cluster configuration involves specifying, on each server, the IP addresses of the other servers in the cluster, and then installing a Service Controller on each server.

## Deploy controllers

On each machine in the cluster, install UbisenseServers. Each machine must run a multicast proxy, which is started by the UbisenseServiceController service if the configuration requires it. The proxy forwards the platform messages sent by other servers to all the local services and clients that require them. As such, all servers in the cluster must run a local controller. Your system should still only have one core server. This means that UbisenseCoreServer should be disabled on all but the core server, so that it cannot be started by accident.

## Configure machine-specific cluster parameters

To enable unicast mode, the following local configuration parameters must be set on each server machine:

- **no_multicast_mode** – set this to 1 to disable use of multicast protocols and ensure the multicast proxy is started.
- **server_unicast_addresses** – a comma-separated list of IP addresses of the other server machines. The addresses should be in standard dotted address form (or DNS name if required and DNS is available).
- (Optional) **high_bandwidth_server_unicast_addresses** – a comma-separated list of IP address of other server machines running high bandwidth services (location cell data and presence association services). This only needs to be set on machines running these services. Set this to 0 to restrict high bandwidth service communications to the local machine only. Setting this will reduce unnecessary network to machines not requiring high bandwidth service data. When not set, the value of **server_unicast_addresses** is used instead.

Local configuration parameters are set either via the registry keys **HKEY_LOCAL_MACHINE/SOFTWARE/Wow643** on a Windows machine, or in the file **/etc/ubisense/platform.conf** on a Linux machine.

NOTE: On Windows, be careful not to add spaces in the registry parameter names as they will not be recognized by the platform.

After changing the value of a local configuration parameter, the service controller and (where applicable) the core server on that machine must be restarted before it will take effect.

# Configure system-wide cluster parameters

## Enabling the multicast proxy

To enable the multicast proxy, the following global configuration variable must also be set by running the **ubisense_configuration_client** command-line utility on the core server machine:

- **multicast_proxy_port** – the port that the server machines will use to communicate between one another. This should be a port number that is free on all server machines.

When this global configuration parameter is set, all local controllers and the core server should be restarted. The server machines should all be running in unicast mode now and able to communicate with one another.

## Specifying logging parameters

To ensure monitor messages are sent to the correct server for logging, use the **ubisense_configuration_client** to set the following parameters:

- **unicast_monitor_address** – the IP address of the logging server
- **unicast_monitor_port** – the port used for logging, defaults to 0, but should be set to a port outside the reserved and dynamic ranges on your server. For example, on Windows, use a unassigned port in the range 1024 to 49151

For further information on distributed logging, see Distributed Logging (UDP Multicast or UDP Unicast) in Ubisense Protocol Addresses and Port Ranges on the Ubisense Documentation Portal.

# Example

We have two servers in the cluster, one for the core platform and location system support, and the other for the web site and Visibility. The server IP addresses are 10.1.16.1 (Linux) and 10.1.16.2 (Windows).

On server 10.1.16.1, we have:

- A core and controller both running.

In **platform.conf**:

- no_multicast_mode: 1
- server_unicast_addresses: 10.1.16.2

On server 10.1.16.2, we have:

- A core and controller, with the core disabled and the controller running.

In registry **HKLM/SOFTWARE/Wow6432node/Ubisense2.1/Platform/Config** the following string values:

- no_multicast_mode: 1
- server_unicast_addresses: 10.1.16.1

On 10.1.16.1, the following command has been executed:

```
ubisense_configuration_client set multicast_proxy_port 24301
```

Now all core and controllers have been restarted. On 10.1.16.2, Service Manager can now be run and will show both controllers as present.

# Visibility and cluster mode

If you have licensed Visibility, one of your cluster machines will be used to run the SmartSpace web site under IIS. There are two configurations necessary to get this to work:

## Firewall exceptions for IIS on Windows

### Firewall exception for w3wp.exe

*Applies to SmartSpace Web on a Windows server for versions of SmartSpace except 3.4 and 3.5*

In cluster mode, the web site executable must be allowed to listen for UDP packets from other machines in the cluster. To do this, it is recommended to add a firewall exception for **w3wp.exe**, the IIS executable. On a 64-bit machine this is located in **%SystemRoot%\SysWOW64\inetsrv\w3wp.exe**. This executable should be allowed to listen for UDP on non-private ports, i.e. 1025-65535. For extra security, this rule can be allowed only for remote addresses in the cluster by setting the scope in Windows Firewall With Advanced Security.

To configure the scope of a rule to only allow traffic from the rest of the unicast cluster, follow these steps:

1. In the Windows Firewall With Advanced Security snap-in, create a new Inbound rule.
2. Select Custom as the rule type and **%SystemRoot%\SysWOW64\inetsrv\w3wp.exe** for the specific program path.
3. Select the UDP protocol and enter the local port range you require.
4. In the Scope tab, in the Remote IP Address group, select These IP Addresses and add the IP addresses of each of the other machines in the cluster.
5. Give the rule a name and save the rule definition.

### Firewall exception for dotnet.exe

*Applies to SmartSpace Web on a Windows server for SmartSpace version 3.5 using Microsoft .NET Core 2.2* ***only***

For Microsoft .NET Core 2.2, the runtime required for SmartSpace 3.5, the website on Windows runs in a separate **dotnet.exe** sub-process under IIS. So the exception for these versions is required for **dotnet.exe** instead of **w3wp.exe**. **dotnet.exe** is located at **%ProgramFiles%\dotnet\dotnet.exe**. Because opening a firewall exception for **dotnet.exe** is a

security risk, when creating a firewall exception for **dotnet.exe** you can define a firewall rule to further restrict the scope so that packets can only be received from specific addresses, such as the other machines in the unicast cluster.

To configure the scope of a rule to only allow traffic from the rest of the unicast cluster, follow these steps:

1. In the Windows Firewall With Advanced Security snap-in, create a new Inbound rule.
2. Select Custom as the rule type and **%ProgramFiles%\dotnet\dotnet.exe** for the specific program path.
3. Select the UDP protocol and enter the local port range you require.
4. In the Scope tab, in the Remote IP Address group, select These IP Addresses and add the IP addresses of each of the other machines in the cluster.
5. Give the rule a name and save the rule definition.

## Migrating web interface services to the same machine

It is recommended that the following services should be deployed onto the machine running IIS:

- Ubisense Visibility Auto association client interface
- Ubisense Visibility HMI client interface
- Ubisense Visibility Roles client interface
- Ubisense Visibility Sensor status client interface
- Ubisense Visibility Shifts client interface
- UbisenseVisibility Tag status client interface
- Ubisense Visibility Web forms client interface
- UbisenseVisibility Web map client interface

Use the Service Manager to drag these services onto the IIS server controller, and they should deploy automatically into that server.

# Connecting clients

To connect to the Ubisense services from a client machine outside of the cluster, you will need to first connect to the server using Site Connector. The use of Site Connector is outlined in Introduction to Site connector on the Ubisense Documentation Portal.