

MID Server

ServiceNow

Introduction

MID Server Plugin



Note: This article applies to Fuji and earlier releases. For more current information, see MID Server^[1] at <http://docs.servicenow.com>. **The ServiceNow Wiki is no longer being updated. Visit <http://docs.servicenow.com> for the latest product documentation.**

Overview

The Management, Instrumentation, and Discovery (MID) Server is a Java application that runs as a Windows service or UNIX daemon. The MID Server facilitates communication and movement of data between the ServiceNow platform and external applications, data sources, and services.

For specific requirements for using the MID Server with Discovery, see MID Server Requirements for Discovery. See the following pages for installation and configuration information:

- MID Server Installation
- MID Server Configuration

The MID Server performs the following tasks:

- Communicates securely with the ServiceNow instance to determine what Discovery probes to run
- Runs Discovery probes on the local network to gather data on network devices
- Sends Discovery probe results back to the ServiceNow instance for processing



Note: MID Server communications are initiated inside the enterprise's firewall and therefore do not require any special firewall rules or VPNs.

Functional Architecture

The MID Server is a Java process that oversees 2 main functional groups of sub-processes, namely *Monitors* and *Workers*. A *Monitor* runs in a separate thread as a timer object and is configured to execute a task periodically, returning its result to ServiceNow's **ECC Queue** (External Communication Channel Queue). A *Worker* is an on-demand thread that executes a task when a corresponding ECC output queue record is read from ServiceNow (The Queue Monitor reads the ECC output queue and triggers a Worker). For example, a **Discovery probe** is a Worker.

Monitors

1. Auto Upgrade
2. Heartbeat
3. Queue Monitor
4. Queue Sender
5. Synchronizers
 - Altiris
 - LanDesk

- Microsoft SMS
- JDBC

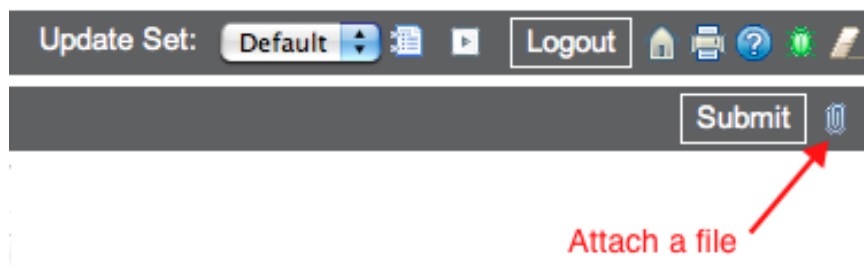
Workers

1. Command Line
2. JDBC
3. File
4. Probes
 - HTTP
 - WMI
 - SNMP
 - SSH

JAR File Synchronization

An administrator can upload a JAR file to an instance and synchronize it to all MID Servers. The administrator can then write custom probes that use the synchronized JAR file. To upload a JAR file to the instance:

1. Navigate to **MID Server > JAR Files**.
2. Click **New**.
3. Complete the following fields:
 - **Name:** A unique and descriptive name for identifying the file in the instance.
 - **Version:** A version number for the file, if one is available.
 - **Source:** Location of the JAR file for reference purposes. Source information is not used by the system.
 - **Description:** Short description of the JAR file and its purpose in the instance.
4. Click the paper clip icon in the banner and attach the JAR file to the record.



5. Click **Submit**.
6. Restart the MID Server service.

The platform makes the JAR file available to any MID Server configured to communicate with the instance.

System Requirements

ServiceNow has tested the MID Server in the following environments:

- Windows Server 2003, 2008, and 2012. All Windows Server 2008 and 2012 editions are supported. Virtual machines and 64-bit systems are supported.
- Linux: Virtual machines and 64-bit systems are supported. On 64-bit Linux systems, you must install the 32-bit GNU C library ^[2] (*glibc*). The installation command for CentOS is: `yum install glibc.i686`

The minimum suggested configuration is:

- 4GB of available RAM per MID Server
- 2+GHZ CPU (Multi-core preferred)

- 500MB of disk space per MID Server
- Can *ride-along* with other services (dependent on server utilization and resource availability)

Java Version Support

The MID Server installs with JRE version 1.8. If you upgrade with a MID Server using JRE 1.6, the system automatically upgrades that MID Server to use version 1.8. Both the 32 bit and 64 bit MID Server use JRE 1.8.

Applications

The MID Server is used by the following applications:

- Discovery
- Orchestration
- Import Sets
- Altiris
- Microsoft SMS / SCCM
- Avocent LANDesk
- HP OpenView Operations
- Microsoft System Center Operations Manager (SCOM)
- Borland Starteam Integration
- Microsoft MIIS

Reports

The following global reports are available for MID Server analytics (starting with the Eureka release).

- MID: Avg Max Memory Percent Use Last 30 Days
- MID Host: Avg CPU Use Percent Per Last 30 Days

MID Servers and System Clones

See KB0547597 ^[3] for a information on what to do with MID servers when you are cloning your instance.

Enhancements

Fuji

- The following records can no longer be modified or deleted:

Table	Record
Public Page [sys_public]	InstanceInfo
Scripted Web Service [sys_web_service]	<ul style="list-style-type: none">• InstanceInfo• GetMIDInfo• MIDAssignedPackages• MIDFieldForFileProvider• MIDFileSyncSnapshot• MIDServerCheck• MIDServerFileProvider

Eureka

- MID Server upgrades support an HTTPS connection over port 443.
- Provides a new SSH client with improved connectivity.
- Provides new reports for MID Server analytics.

Dublin

- Administrators can install a 64-bit MID Server on a 64-bit host system.
- Script File synchronization stores all MID Server scripts in the ServiceNow instance to simplify distribution and security. It is no longer necessary to manually unblock MID Server scripts on the host machine.
- Several new business rules ensure that changing a MID Server's name in the configuration parameter also changes the name in MID Server record. See Available Parameters.
- The first MID server to successfully connect with the ServiceNow instance automatically becomes the default MID Server.

References

- [1] <https://docs.servicenow.com/bundle/jakarta-it-operations-management/page/product/mid-server/reference/r-MIDServer.html>
- [2] <http://www.gnu.org/s/libc/>
- [3] https://hi.service-now.com/kb_view.do?sysparm_article=KB0547597

MID Server Requirements for Discovery



Note: This article applies to Fuji and earlier releases. For more current information, see MID Server^[1] at <http://docs.servicenow.com>. **The ServiceNow Wiki is no longer being updated. Visit <http://docs.servicenow.com> for the latest product documentation.**

Overview

The ServiceNow MID Server is used for enterprise application and service management, Orchestration, and Discovery. The requirements in this page are specifically for the use of MID Servers with the ServiceNow Discovery and Orchestration products.

System Requirements

ServiceNow has tested the MID Server in the following environments:

- Windows Server 2003, 2008, and 2012. All Windows Server 2008 and 2012 editions are supported. Virtual machines and 64-bit systems are supported.
- Linux: Virtual machines and 64-bit systems are supported. On 64-bit Linux systems, you must install the 32-bit GNU C library^[2] (*glibc*). The installation command for CentOS is: `yum install glibc.i686`

The minimum suggested configuration is:

- 4GB of available RAM per MID Server
- 2+GHZ CPU (Multi-core preferred)
- 500MB of disk space per MID Server
- Can *ride-along* with other services (dependent on server utilization and resource availability)

Java Version Support

The MID Server installs with JRE version 1.8. If you upgrade with a MID Server using JRE 1.6, the system automatically upgrades that MID Server to use version 1.8. Both the 32 bit and 64 bit MID Server use JRE 1.8.

External Connectivity Requirements

The MidServer communicates securely on port 443 to the instance and requires *no* inbound connections. In some cases, it might be necessary to allow this communication through the firewall if the MID Server fails to register on the instance. To determine if the application or a network security restriction is to blame for connection failure, attempt to telnet to the instance on port 443 from the server that is hosting the MID Server application. If this connection fails, then the problem could be a web proxy (since 443 is a https connecton) or a Firewall rule preventing external TCP connections from that host. Contact network security personnel for the proxy information to add to the *config.xml* file, or request that the Firewall be configured to allow access using one of the following syntaxes:

- `<source IP> to <any>`
- `<source IP> to <ServiceNow> any established`
- `<source IP> to <instance_name.service-now.com> 443`

Additionally, ensure the MID server can connect to *install.service-now.com* to download and install updates.

Internal Requirements

The three methods used for discovering various devices on a network are SSH, WMI and SNMP. SSH is used for accessing UNIX-like machines. Discovery logs into a machine with SSH and runs commands within an encrypted session to gather system information. Orchestration logs in to UNIX and Linux machines using SSH to perform Workflow activities. WMI is used by Discovery for Windows based machines and is used for querying the remote WMI protocol on targets for gathering of Windows information. Orchestration uses **PowerShell** to run activities on Windows machines. And lastly, SNMP v1/v2c/v3 is used on various network devices (Routers, Switches, Printers) by Discovery and Orchestration. Detailed information is listed below about these methods.

SSH - UNIX

For UNIX-like machines, Discovery and Orchestration use **SSH protocol, version 2** ^[1] to access target machines. SSH is a network protocol that allows data to be exchanged using a secure channel between two networked devices. SSH communicates on port 22 within an encrypted datastream and requires a login to access the targets using two available methods of authentication: a user name and password combination and a user name and shared private key. Specify SSH authentication information and type in the **Credentials** module. If multiple credentials are entered, the platform tries one after the other until a successful connection is established or all are ultimately denied. To provide for application relationships a limited number of SUDO commands must be available to be run. Additional details to these requirements can be found in **UNIX/Linux commands requiring root privileges for Discovery and Orchestration**.

WMI - Windows

For Windows machines, Discovery uses the **Windows Management Instrumentation (WMI)** ^[2] interface to query devices. Due to Microsoft security restrictions for WMI, the MID Server application executing the WMI queries must **run as** a domain user with local (target) administrator privileges. When Discovery detects activity on port 135, it launches a WMI query. The response from the Windows device is sent over a Distributed Component Object Model (DCOM) port configured for WMI on Windows machines. This can be any **port** ^[3]. Ensure that the MID Server application host machine has access to the targets on all ports due to the unique nature of the WMI requirements.

Windows PowerShell

PowerShell ^[4] is built on the Windows .NET Framework and is designed to control and automate the administration of Windows machines and applications. Orchestration uses PowerShell to run **Workflow activities** on Windows machines. PowerShell must be installed on any MID Server that executes these activities. MID Servers using PowerShell must be installed on a supported Windows operating system. ServiceNow supports PowerShell 2.0 and 3.0. Orchestration activities for PowerShell require a **credentials Type** of **Windows**.

SNMP - Network

For network devices, Discovery uses a SNMP scan ^[5] to get device specific MIBs and OIDs. SNMP is a common protocol used on most routers, switches, printers, load balancers and various other network enabled devices. Use a "community string" (password) for authentication when scanning a device via SNMP. Many devices have an out-of-box community string of **public** which Discovery (by default) uses when querying a target. Define additional community strings in the **Credentials** module which are tried in succession, along with **public**, until a successful query returns. In addition to the credentials, the platform also requires the ability to make **port 161** SNMP requests from the MID Server to the target. If Access Control Lists (ACLs) are in place to control the IP addresses that can

make these queries, ensure that the IP address of the MID Server is in the ACL. ServiceNow Discovery supports SNMP versions 1 and 2c ^[6].

The out-of-box Orchestration activity SNMP Query returns the OID of a device and requires SNMP **credentials**.

WBEM

Web-Based Enterprise Management (WBEM ^[7]) defines a particular implementation of the **Common Information Model (CIM** ^[8]), including protocols for discovering and accessing each CIM implementation. WBEM requires either of two ports, 5989 or 5988 and uses the HTTP transport protocol. WBEM supports SSL encryption and uses CIM user name/password credentials. ServiceNow Discovery launches a **WBEM port probe** to detect activity on the target ports and to append gathered data to a classification probe that explores CIM Servers.

References

- [1] http://en.wikipedia.org/wiki/Secure_Shell
- [2] http://en.wikipedia.org/wiki/Windows_Management_Instrumentation
- [3] <http://support.microsoft.com/kb/832017>
- [4] <http://support.microsoft.com/kb/968929>
- [5] <http://en.wikipedia.org/wiki/SNMP>
- [6] http://www.paessler.com/manuals/prtg_traffic_grapher/snmpversion12cand3
- [7] http://en.wikipedia.org/wiki/Web-Based_Enterprise_Management
- [8] [http://en.wikipedia.org/wiki/Common_Information_Model_\(computing\)](http://en.wikipedia.org/wiki/Common_Information_Model_(computing))

Installation

MID Server Installation



Note: This article applies to Fuji and earlier releases. For more current information, see *MID Server Installation* ^[1] at <http://docs.servicenow.com>. **The ServiceNow Wiki is no longer being updated. Visit <http://docs.servicenow.com> for the latest product documentation.**

Overview

The Management, Instrumentation, and Discovery (MID) Server is a Java server that facilitates communication and movement of data between the ServiceNow platform and external applications, data sources, and services.

Video Tutorials

How to Set Up a MID Server	How to Set Up Multiple MID Servers on the Same Host Computer
--	--

Satisfying Connection Prerequisites

You must install a MID Server on a local network resource and configure it to communicate with the machines it will probe. The local network resource must have these network privileges:

- **Firewall access:** Configure any firewalls between the MID Server and the target devices to allow a connection. If your network uses a DMZ ^[2], and if your network security protocols limit port access from within the network to the DMZ, you might have to deploy a MID Server to a machine within the DMZ to probe the devices there.
- **Network access:** Configure target devices to allow the MID Server probe to connect. If network security prevents you from configuring new machines that can connect to the targets, install the MID Server on an existing machine with connection privileges.
- **Network account:** Install the MID Server with the proper account, either local or domain administrator.

Additionally, for the MID Server to access your ServiceNow instance, satisfy these prerequisites:

1. Configure the network to allow MID Server network connectivity to the ServiceNow instance over TCP port 443.
2. Configure basic authentication for SOAP communications with the ServiceNow instance.
3. Navigate to **System Web Services > Scripted Web Services** and confirm that the following web services are active:
 - GetMIDInfo
 - InstanceInfo
 - MIDAssignedPackages
 - MIDFieldForFileProvider
 - MIDFileSyncSnapshot
 - MIDServerCheck
 - MIDServerFileProvider

4. Navigate to **sys_public.list** and verify that the **InstanceInfo** public page is active to allow the MID Server to validate its version.

Setting up MID Server User and Role

The MID Server connects to a ServiceNow instance by using the SOAP web service. To allow authentication with the ServiceNow instance, create a separate user account for each MID Server or share the same account across multiple MID Servers. Each MID Server account must use the `mid_server` role to access protected tables.

To create a MID Server user account on the instance:

1. From the ServiceNow instance, navigate to **User Administration > Users**.
2. Click **New**.
3. Fill in the following:
 - **User ID:** The same user ID that will be specified in the `mid.instance.username` parameter of `config.xml`.
 - **Password:** - The same password that will be specified in the `mid.instance.password` parameter of `config.xml`.
 - **First name:** The user's first name.
 - **Last name:** The user's last name.
4. Right-click the header and select **Save**.
5. Under the **Roles** related list, click **Edit**.
6. Move **mid_server** from the Collection list to the Roles List.
7. Click **Save**.

Verifying the MID Server Account Access

You can confirm that the MID Server account was created successfully and the account has connectivity to the ServiceNow instance.

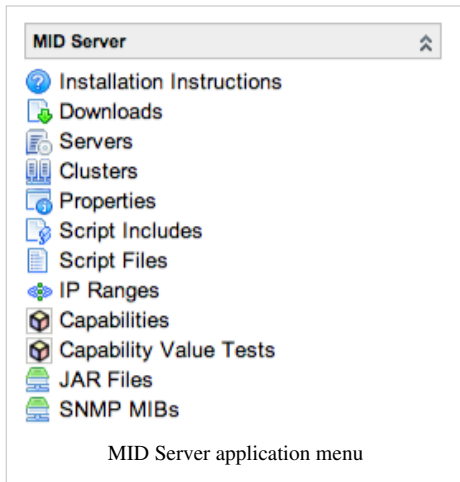


Note: Use a supported browser on the MID Server host to validate connectivity.

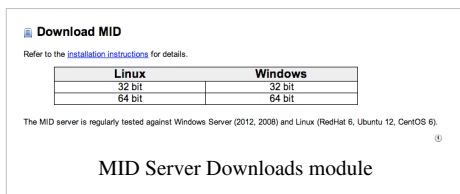
1. On the MID Server host, open a supported web browser.
2. Navigate to the ServiceNow instance.
3. If the account is already logged into the instance, log out.
4. Use the previously created MID Server user credentials and sign in.

Downloading MID Server Files

Enabling Discovery, Orchestration, or any integration that requires the use of the MID Server, automatically activates the MID Server plugin. After activation, the MID Server application menu appears in the application navigator.



To download and install a MID Server, navigate to **Mid Server > Downloads** on your instance. Select and download the MID Server for the appropriate operating system. If the download does not begin immediately, try the download at a later time as the system may be busy.



Installing a MID Server on Linux

1. If you are using a 64-bit operating system with a version of ServiceNow prior to Dublin, you can install a 32-bit MID Server on a 64-bit Linux operating system by installing 32-bit libraries. Run the command for your Linux operating system version:

- **Ubuntu:** `sudo apt-get install ia32-libs ia32-libs-multiarch libgphoto2-2`
- **Red Hat:** `sudo yum -y install glibc.i686`

2. Create the installation directory by running:

```
mkdir -p /servicenow/<mid server name>
```

3. Extract the downloaded MID Server archive file, *mid.<os>.zip* into the */servicenow/<mid server name>* directory.

The resulting directory structure is */servicenow/<mid server name>/agent*.

4. Change to the */servicenow/<mid server name>/agent* directory, and edit the *config.xml* file as follows:

- Find the `<parameter name="url" value=" UNIQ-nowiki-0-11335bd0687cdc6f-QINU //YOUR_INSTANCE.service-now.com"/>` element and change the value to the URL of your instance.
- Enter the MID user credentials in the `mid.instance.username` and `mid.instance.password` parameters. By default, the MID Server, uses basic authentication for SOAP messages. The password value is also encrypted authentication.
- Find the `<parameter name="name" value="YOUR_MIDSERVER_NAME_GOES_HERE"/>` element and change the value for the MID Server name.
- (Optional) Enter connection information for the proxy server. Remove the appropriate comment tags from the proxy configuration information. For example, you can configure the `mid.proxy.use_proxy`, `mid.proxy.host`, `mid.proxy.port`, `mid.proxy.username`, and `mid.proxy.password`.

5. Execute the *start.sh* shell script.

6. Log in to the ServiceNow instance identified in the *config.xml* file.

7. Navigate to **MID Server > Servers**. Alternatively, if Discovery is installed, navigate to **Discovery > MID Servers**.
8. Verify that all MID Servers connected to this instance are listed.

Uninstalling

A MID Server running on Linux operates as a single process. You can end this process to accommodate such tasks as redeploying the MID Server to another host machine or changing the unique name of a MID Server when deploying multiple MID Servers.

1. Stop the MID Server process by executing the *stop.sh* shell script.
2. Verify that the MID Server is running by executing the *bin/mid.sh status* shell script.
3. After the MID Server stops, delete the files in the *agent* directory.

Installing a MID Server on Windows

Use the following procedures to install one or more MID Servers on a single machine.

1. Log in to the host machine where you want to install the MID Server.
2. Create a directory for the MID Server on the top level of the drive, with a distinctive name, such as *ServiceNow\MID Server1*.
3. Move the MID Server archive file into the new directory.
4. Right-click the archive and select **Extract All**.
5. Navigate to the *\agent* directory that was created when the file was extracted.
6. Edit the *config.xml* file with a text editor such as WordPad:
 - Find the `<parameter name="url" value=" UNIQ-nowiki-1-11335bd0687cdc6f-QINU //YOUR_INSTANCE.service-now.com"/>` element and change the value to the URL of your instance.
 - Enter the MID user credentials in the `mid.instance.username` and `mid.instance.password` parameters. By default, the MID Server, uses basic authentication for SOAP messages. The password value is also encrypted authentication.
 - Find the `<parameter name="name" value="YOUR_MIDSERVER_NAME_GOES_HERE"/>` element and change the value to define the name of your MID Server.
 - (Optional) Enter connection information for the proxy server. Remove the appropriate comment tags from the proxy configuration information. For example, you can configure the `mid.proxy.use_proxy`, `mid.proxy.host`, `mid.proxy.port`, `mid.proxy.username`, and `mid.proxy.password`.

NOTE: If this MID Server is installed on a system that contains other MID Servers, edit the *wrapper.conf* file as described in the procedure for installing multiple MID Servers.

Installing the MID Server as a Windows Service

To run a MID Server as a Windows service:

1. Click the **Start** button.
2. In the search box, type **command prompt** or **cmd.exe**.
3. In the results list, right-click **Command Prompt** or **cmd.exe**, and then click **Run as administrator**.

This enables the MID Server to be installed with administrative rights under any Windows User Account Control (UAC) setting.

4. In the command prompt, navigate to *\agent* in the directory you created for the MID Server files. For example, the path might be *C:\ServiceNow\MID Server\agent*.
5. Run *start.bat*.

Configuring MID Server Service Credentials

By default, the MID Server service runs as a local system account. You can perform these steps to configure the service to run as a specific user or domain account.

1. Open the Windows Services console.
2. Double-click the **ServiceNow <MID Server name>** service for each MID Server.
3. To verify that the MID Server service name is correct, review the properties to ensure that the MID server service values match the values from the *wrapper-override.conf* file. The **Service name** value should match the **wrapper.name** value and the **Display name** value should match the **wrapper.displayname** value.
4. Select the **Log On** tab, and then do one of the following:
 - Select the **Local System Account** to assign the Windows system account. This account has account privileges to modify files in MID server agent folder.
 - Select **This account** and assign a local or domain admin account credentials. Use Windows Explorer to grant write permissions to the MID Server agent folder.
5. In the General tab, set **Startup type** to **Automatic**.
6. Click **OK**.
7. Restart the **ServiceNow <MID Server name>** service, and make sure that *ServiceNow\<MID Server name>\agent\logs\agent0.log* does not have error messages.
8. On the instance this MID Server is connected to, navigate to **MID Server > Servers**. Alternatively, if Discovery is installed, navigate to **Discovery > MID Servers**.
9. Verify that all MID Servers connected to this instance are listed.

Uninstalling

The MID Server runs as a standalone service. It can be removed easily to accommodate such tasks as redeploying the MID Server to another host machine or changing the unique name of a MID Server when deploying multiple MID Servers.

1. Stop the running MID Server service.
2. Open a command window (**Start > Run > cmd**).
3. Do one of the following:
 - From the Dublin versions and newer, navigate to the *\agent\bin* directory in the MID Server installation directory and double-click the *UninstallMID-NT.bat* file.
 - For versions prior to Calgary, navigate to the *\agent\bin* directory in the MID Server installation directory and double-click the *uninstall.bat* file.

Installing Multiple MID Servers on a Single System

You can install multiple MID Servers on a single host or on a virtual machine using either Linux or Windows. Installing multiple MID Servers may involve other setup steps depending on your network configuration. See Deploying Multiple MID Servers for other considerations. For instances using a version prior to Calgary, see the previous version information.

1. Log in to the host system or virtual machine where you want to install multiple MID Servers.
2. Create a directory for each MID Server on the top level of the drive.

Make sure you create a unique and descriptive name for each MID Server, such as *MIDServer_SMS_Int* or *MIDServer_Disc1*.

3. Extract the downloaded MID Server archive file into each MID Server directory.

When this is complete, there should be the a directory path that resembles the following for each MID Server:

`\ServiceNow\<MID Server name>\agent.`

4. Using a text editor such as WordPad, edit the *config.xml* file in each MID Server *\agent* directory, as follows:

- Find the `<parameter name="url" value=" UNIQ-nowiki-2-11335bd0687cdc6f-QINU //YOUR_INSTANCE.service-now.com" />` element and change the value to define the name of your MID Server.
- If basic authentication is enabled, as it is by default behavior, enter the user credentials in the `mid.instance.username` and `mid.instance.password` parameters.
- Find the `<parameter name="name" value="YOUR_MIDSERVER_NAME_GOES_HERE" />` element and change the value to define the name of your MID Server.
- Enter connection information for any proxy server used and remove the comment tags from the proxy configuration information.

5. For each Windows MID Server, edit the *\agent\conf\wrapper-override.conf* file with a text editor such as WordPad. Use the *wrapper-override.conf* configuration file to enter all configuration information. Do not edit the *wrapper.conf* file, which contains the default configuration for the MID Server. Any future ServiceNow upgrades overwrite the contents of the *wrapper.conf* file, but do not modify the *wrapper-override.conf* file.

- **wrapper.name** ^[3]: [Required] This name identifies the MID Server process, maps to the **Service name** and must be unique. The default value is **snc_mid**.
- **wrapper.displayname** ^[4]: [Required for Windows] This value maps to the **Display name** in the Windows Services console. For example, you might enter **ServiceNow DevMID01**. The default value is **ServiceNow MID Server**.
- **wrapper.java.command** ^[5]: [Optional] This property defines the path to the java bin directory, either relative to the agent directory or absolute. The default value is *jre/bin/java*.
- **wrapper.java.initmemory** ^[6]: [Optional] This property defines the initial Java heap size ^[7] in MB. The default value is **10**.
- **wrapper.java.maxmemory** ^[8]: [Optional] This value defines the maximum Java heap size in MB. The default is **512**.

Note: These values **cannot** be edited while the MID Server is running.

6. Confirm that the MID Server is running.

7. (Optional) Configure MID Server clustering for load balancing or failover as necessary.

Versions Prior to the Calgary Release

MID Servers in versions prior to Calgary

- Log in to the host machine or virtual machine where you want to install multiple MID Servers.
- Create a directory for each MID Server on the top level of the drive.

Make sure you create a unique and descriptive name for each MID Server, such as *MIDServer_SMS_Int* or *MIDServer_Disc1*.

- Extract the downloaded MID Server zip file into each MID Server directory.

When this is complete, you should have the a directory that resembles the following for each MID Server:

`\ServiceNow\<MID Server name>\agent.`

Using a text editor such as WordPad, edit the *config.xml* file in each MID Server *agent* directory, as follows:

- Find the element `<parameter name="url" value=" UNIQ-nowiki-3-11335bd0687cdc6f-QINU //YOUR_INSTANCE.service-now.com" />` and change the value to the URL of your instance.
- For basic authentication, which is the default, enter the MID user credentials in the `mid.instance.username` and `mid.instance.password` parameters. Set up additional

authentication for SOAP messages.

- For encrypted authentication, enter the MID user credentials in the `mid.instance.username` and `mid.instance.password` parameters.
- Find the element `<parameter name="name" value="YOUR_MIDSERVER_NAME_GOES_HERE" />` and change the value to define the name of your MID Server.
- Enter connection information for any proxy server used. Be sure to remove the comment tags from the proxy configuration information.
- Edit the `wrapper.conf` file for each MID Server with a text editor such as WordPad. By default, this file is located here:

`\ServiceNow\<MID Server name>\agent\conf`

- **wrapper.console.title=<MID Server name>:** This is the title to use when running the MID Server as a console.
- **wrapper.ntservice.name=<MID Server name>:** This is the internal Windows name for the service and is not displayed. This name must be unique. For example, example: **snc_agent2**.
- **wrapper.ntservice.displayname=<MID Server name>:** This is the name that is displayed to the user in the Windows Services console. For example, you might enter **ServiceNow MID Server1**.
- **wrapper.ntservice.description=<New Custom Description>:** This is the optional long description of the service that appears in the Services console.

NOTE: These values *cannot* be edited in this file after you create the service. Make sure you name and describe the services correctly before continuing to the next step.

- Install the MID Server as a Windows service:
 - a. For Windows XP, Windows 2000 Server, or Windows Server 2003:
 1. Open the `\agent` folder in the directory you created for the MID Server installation files. For example, the path might be `C:\ServiceNow\MID Server\agent`.
 2. Double-click the `start.bat` file to install the Windows service.
 - b. For Vista, Windows 2008 Server, or Windows 7:
 1. Click the **Start** button.
 2. In the search box, enter **command prompt** or **cmd.exe**.
 3. In the results list, right-click **Command Prompt** or **cmd.exe**, and then click **Run as administrator**.
 This enables the MID Server to be installed with administrative rights under any Windows User Account Control (UAC) setting.
 4. In the command prompt, navigate to `agent` in the directory you created for the MID Server files. For example, the path might be `C:\ServiceNow\MID Server\agent`.
 5. Run `start.bat`.
- Edit each MID Server's credentials.
 - a. Open the Windows Services console.
 - b. Double-click the **ServiceNow <MID Server name>** service for each MID Server.
 - c. In the properties dialog box, select the Log On tab.
 - d. Set **Log on as** privileges with Domain User or Local Admin credentials.
 - e. In the General tab, set **Startup type** to **Automatic**.
 - f. Click **OK**.
- Restart each ServiceNow MID Server service and make sure that `\ServiceNow\<MID Server name>\agent\logs\agent0.log` does not have error messages.

- In each instance these MID Servers are connected to, navigate to **MID Server > Servers**. If Discovery is installed, navigate to **Discovery > MID Servers**.

All MID Servers connected to this instance are listed.

Confirming Connectivity

Use the following procedures to verify that each MID Server service instance has started properly with network connectivity.

1. Verify that the MID Server service is running:
 - **Windows:** In the Windows Services console, locate the **ServiceNow <MID Server name>** and confirm that each MID Server has the **Started Status**.
 - **Linux:** Ensure that the *agent0.log.0.lck* file appears in the */servicenow/<mid server name>/agent* folder.
2. After each ServiceNow MID Server restart, open the *agent0.log.0* file and address all error messages.
3. Confirm network connectivity by pinging the instance URL, executing a telnet to instance URL at port 443, and/or performing a traceroute to the instance URL.
4. From the ServiceNow instance, navigate to **MID Server > Servers**.
5. Review and verify that all MID Servers that are connected to the ServiceNow instance are listed.
6. Verify that the **Status** is **Up** for the MID Servers.

Upgrading and Testing

The MID Server is configured to check with the ServiceNow instance hourly to determine whether it needs to upgrade. This configurable behavior allows the MID Server to upgrade automatically when the instance upgrades. The system that hosts the MID Server must be able to access one of these URLs to automatically upgrade (starting with the Eureka release):

- **HTTPS:** <https://install.service-now.com> on the default HTTPS port (443)
- **HTTP:** <http://install.service-now.com> on the default HTTPS port (80)

The MID Server automatically tests connectivity through a public scripted web service.



Note: *In versions prior to Eureka, the MID Server upgrade URL was only available on the default HTTP port (80).*

Upgrade Error Messages

The MID Server can display the following upgrade error messages.

Message	Description
Unable to refresh packages	The MID Server displays this as a generic error when the error is not handled by a defined error message.
Failed to query instance for MID Server buildstamp	Instance is offline or there is a major version mismatch between the MID Server and the instance.
Not a valid package buildstamp	InstanceInfo returned an assigned buildstamp that was not in the correct format, such as a version mismatch.

Using Basic Authentication

You can enforce basic authentication on each request. Basic authentication requires each SOAP request to contain an Authorization header as specified in the Basic Authentication ^[9] protocol.

To set basic authentication for SOAP messages:

1. Navigate to **System Properties > Web Services**.
2. Select the check box for **Require basic authorization for incoming SOAP requests**.
3. Click **Save**.

Supplying basic authentication information, regardless of whether it is required, has an added advantage. The web service invocation creates or updates data using the supplied credentials. As an example, when you create an incident record, the journal fields have the user id of the basic authenticated user instead of the default Guest user. This behavior allows you to identify data added by a specific MID Server.

To provide basic authentication credentials for a MID Server, navigate to *C:\Program Files\ServiceNow\MID Server name\agent* and edit the *config.xml* file, as follows:

- Find the element `<parameter name="mid.instance.username" value="" />` and enter your instance's administrator user name as the value. For example, you might enter `<parameter name="mid.instance.username" value="admin"/>`.
- Find the element `<parameter name="mid.instance.password" value="" />` and enter the configured password for this instance as the value. For example, you might enter `<parameter name="mid.instance.password" value="abc123"/>`.



Note: The setting for enforcing strict security controls how ServiceNow uses the credentials you provide for the MID Server. When the setting is enabled, you must provide a user ID with access to the tables the MID Server is trying to access. When the setting is disabled, any valid user ID allows the MID Server to access to all tables.



Note: The MID Server is not able to communicate through a proxy server if the proxy server supports only NTLM authentication. You can use basic authentication with a proxy server or create an exception for the MID server host.

Monitoring Your MID Server

Use the following procedures to monitor each Windows or Linux MID server:

1. For **Windows**, navigate to the Windows Services console, locate the service name that matches the name that appears from the *wrapper-override.conf* file. If the MID Server process is the only Java process running on the host, monitor the memory used by *java.exe* and alert on *less* than the maximum configured memory defined in *~\agent\conf\wrapper-override.conf*.

2. Ensure that the *agent0.log.0.lck* file appears in the *~\agent\logs* folder to confirm that the MID Server running and logging system activity in the *agent0.log.0* file.
3. Review the following logs for warning, critical, and severe errors:
 - *~\agent\logs\agent0.log.0*
 - *~\agent\logs\wrapper.txt*
4. Confirm network connectivity.
5. From the MID Server instance, navigate to the **MID Servers** page, and review the status of the MID Server. For additional information, click a **Name**.
6. Use Windows or Linux tools to monitor:
 - CPU
 - Memory
 - Disk utilization
 - Event logs
 - syslog
7. Set up Email and SMS notifications to alert you when issues occur with MID servers. The MID Server Down Notification is enabled by default.

References

- [1] https://docs.servicenow.com/bundle/jakarta-it-operations-management/page/product/mid-server/concept/c_MIDServerInstallation.html
- [2] [http://en.wikipedia.org/wiki/DMZ_\(computing\)](http://en.wikipedia.org/wiki/DMZ_(computing))
- [3] <http://wrapper.tanukisoftware.com/doc/english/prop-name.html>
- [4] <http://wrapper.tanukisoftware.com/doc/english/prop-displayname.html>
- [5] <http://wrapper.tanukisoftware.com/doc/english/prop-java-command.html>
- [6] <http://wrapper.tanukisoftware.com/doc/english/prop-java-initmemory.html>
- [7] http://publib.boulder.ibm.com/infocenter/javasdk/tools/index.jsp?topic=%2Fcom.ibm.java.doc.igaa%2F_1vg00014884d287-11c3fb28dae-7ff6_1001.html
- [8] <http://wrapper.tanukisoftware.com/doc/english/prop-java-maxmemory.html>
- [9] <http://www.w3.org/Protocols/HTTP/1.0/draft-ietf-http-spec.html#BasicAA>

Deploying Multiple MID Servers



Note: The latest release this documentation applies to is Fuji. For the Geneva release, see MID Server^[1]. Documentation for later releases is also on docs.servicenow.com^[2].

Overview

Depending upon how you use the MID Server (for an external integration, Discovery, or Orchestration) and the load placed on it, you might find it necessary to deploy multiple MID Servers in your network. You can install each MID Server on a separate machine or install multiple MID Servers on a single machine (including virtual machines). For instructions on installing the MID Server on multiple machines, see MID Server Installation.

Integrations

Factors determining the number of MID Servers your network will require to support external applications that integrate with ServiceNow include the following:

- The security constraints in your network
- The amount of traffic between ServiceNow and the integrations
- The reliability of the MID Server machines.

Security

Security policies in your network (firewalls between network segments, for example) might make direct communication impossible between your instance and an integration's data source (JDBC, LDAP, etc.). To retrieve data for the instance, you can install a MID Server that has access to both the data source and the instance.

Load balancing

In some cases, a single MID Server can handle all the transactions that occur between an instance and an external integration. However, in a high volume environment, it might be necessary to deploy multiple MID Servers as load balancers for certain transactions. For example, JDBC data transfers can tie up the resources of a MID Server, making it unable to respond to other requests. The following operations between an integration might require separate MID Servers in a busy network:

- File exports
 - Running scripts
 - JDBC data sources
 - Reading files
-

High availability model

Avoid installing MID Servers for critical integrations on a machine that might experience any type of planned outage or an outage caused by overloaded processes. If necessary for reliability, consider deploying these types of MID Servers to dedicated machines for high reliability.



Warning: Do not integrate with an external application on a MID Server provisioned for ServiceNow Discovery or Orchestration.

Discovery

When determining if you need multiple MID Servers to discover the configuration items in your network efficiently, the following factors must be considered:

- **WAN deployment:** When determining where to deploy MID Servers in a WAN, consider the bandwidth available between your local area networks. In most cases, the best practice is to install a MID Server on each LAN to probe devices locally, rather than deploying MID Servers that must probe devices across slow WAN connections. An alternative to this type of deployment is to install MID Servers that probe other LANs via VPN connections that take advantage of fast Internet connections. If the bandwidth of your WAN connections is comparable to that of your Internet connection, then there is no performance impact in running MID Server probes across WAN connections.
- **DMZ:** Your network policy might require you to install one or more MID Servers in your DMZ to probe the devices there. This is common in networks that tightly regulate the ports that are opened on the inside firewall.
- **High capacity:** Deploy multiple MID Servers where capacity is an issue, as when Discovery has to gather information about thousands of configuration items quickly.
- **Security:** If your security policy controls access to network devices (e.g. switches and routers) with an *access control lists (ACL)*, it might be necessary to install one or more MID Servers on a machine in the network that is already on the ACL.
- **Probe types:** If you are conducting probes of different operating systems, your network policy might require a separate MID Server for each type of probe (e.g., one MID server for Windows WMI probes and another for SSH probes on UNIX)

Orchestration

When determining if multiple MID Servers are necessary to execute Orchestration activities, consider the following factors:

- **WAN deployment:** When determining where to deploy MID Servers in a WAN, consider the bandwidth available between your local area networks. In most cases, the best practice is to install a MID Server on each LAN to probe devices locally, rather than deploying MID Servers that must probe devices across slow WAN connections. An alternative to this type of deployment is to install MID Servers that probe other LANs via VPN connections that take advantage of fast Internet connections. If the bandwidth of the WAN connections is comparable to that of the Internet connection, then there is no performance impact in running MID Server probes across WAN connections.
- **DMZ:** Network policy might require the installation of one or more MID Servers in the DMZ to probe the devices there. This is common in networks that tightly regulate the ports that are opened on the inside firewall.
- **Security:** If a security policy controls access to computers with an *access control list (ACL)*, it might be necessary to install one or more MID Servers on a machine in the network that is already on the ACL.

- **Probe types:** If Orchestration launches probes for different operating systems, network policy might require a separate MID Server for each type of probe (e.g., one MID server for Windows PowerShell and another for SSH probes on UNIX).

References

[1] https://docs.servicenow.com/bundle/geneva-it-operations-management/page/product/mid_server/concept/c_MIDServer.html

[2] <http://docs.servicenow.com>

Configuration

MID Server Configuration



Note: This article applies to Fuji and earlier releases. For more current information, see *MID Server Configuration* ^[1] at <http://docs.servicenow.com> **The ServiceNow Wiki is no longer being updated. Visit <http://docs.servicenow.com> for the latest product documentation.**

Overview

Administrators must configure a MID Server to ensure that it has access to sufficient system resources, probes the proper data sources, and communicates with the instance as expected. You must complete all the steps in MID Server Installation before attempting any of the configuration steps explained here.

You must restart a MID Server after any configuration change for the changes to take effect.



Note: Using special characters in an XML configuration file requires you to encode them.

Available MID Server Setting Types

You can configure the following setting types on a MID Server. The setting type determines what components are affected by the MID Server setting. Choose a MID Server setting type that matches the scope you want the setting to affect.

Type of setting	Components affected	Overrides
MID Server Property	Either: <ul style="list-style-type: none"> The behavior of all MID Servers The behavior of a particular MID Server 	MID Server properties override MID Server parameters
MID Server parameter	The behavior of a particular MID Server	None

Setting MID Server Properties

Use a MID Server property to control either the behavior of all MID Servers or a particular MID Server. Configure MID Server properties in the MID Server plugin. Do not configure MID Server properties in the **glide.properties** file that is located in the *properties* folder of the agent. The **glide.properties** file gets overwritten during the upgrade process.

1. Navigate to **MID Server > Properties**.
2. Click **New**.
3. Fill in the fields, as appropriate (see table).

Field	Description
Name	Enter the property name. See the Name(s) column in Required Parameters or Optional Configuration parameters for a list of parameter and property names.
Value	Enter the value you want the property to have.
MID Server	Leave this field blank to set a MID Server property that affects all MID Servers. To set a MID Server property for a particular MID Server, select the MID Server.

Setting MID Server Parameters

Use a MID Server parameter to control the behavior of a particular MID Server. Set MID Server configuration parameters in either of the following places:

- From the **Configuration Parameters** related list in the MID Server record.
- From the `config.xml` file in the `\agent` directory of your MID Server installation.



Note: *Changes to parameters only take effect when the MID Server is started (or restarted).*

Setting Parameters from the ServiceNow Instance

You can view and manage MID Server configuration from the ServiceNow instance.

1. Navigate to the list of MID Servers using one of the following paths:
 - **MID Server > Servers**
 - **Discovery > MID Servers**
 - **Orchestration > MID Servers** (starting with Dublin)
 - **Runbook Automation > MID Servers** (versions prior to Dublin)
2. From the list of MID Servers, select a MID Server to configure.

The **Configuration Parameters** related list shows all the parameters currently in the MID Server's configuration file. If there are any passwords, they are displayed in asterisks for security reasons.

Configuration Parameters (9) | IP Ranges | Capabilities | Logs (15) | Threads (12) | Properties

Configuration Parameters

New

Go to

Param name

1 to 9 of 9

MID Server = Surfplot-MID1

Param name	Value
<input type="checkbox"/> url	http://10.0.4.176:8080/glide/
<input type="checkbox"/> mid.shazzam.chunk_size	10
<input type="checkbox"/> mid.shazzam.regulator.interval_ms	25
<input type="checkbox"/> mid.instance.password	*****
<input type="checkbox"/> threads.max	25
<input type="checkbox"/> mid.shazzam.regulator.packets_per_interval	1
<input type="checkbox"/> mid_sys_id	99c9f8d6a9fee3d2787bf0f01e6dcc6e
<input type="checkbox"/> mid.instance.username	admin
<input type="checkbox"/> name	Surfpilot-MID1

Actions on selected rows...

1 to 9 of 9

3. To add parameters, click **New**, and then complete the form.

After the form is submitted, the configuration file for that MID Server is modified to include the new parameter. Changes to existing parameters are reflected in the MID Server configuration file as well. Changes made to the MID Server configuration file do not take place immediately, but rather the next time the MID Server is restarted. The MID Server form has a related link for restarting the MID Server.



Note: ServiceNow prevents you from saving changes, such as modifying or deleting parameters, that would cause the MID Server to lose communications with the instance. For example, you cannot change the url parameter. Any changes to these protected properties must be made directly in the config.xml file for that MID Server.

Setting Parameters from the config.xml File

MID Server configuration is controlled by an XML file called *config.xml*. This file is located in the *\agent* directory, immediately under the directory where the MID Server is installed. Edit this file directly to make any configuration changes to protected parameters. Many configuration changes, such as those that do not disrupt communication between the MID Server and the ServiceNow instance, may also be made from the instance.

The structure of the *config.xml* file is simply an outer parameters tag and a series of inner parameter tags. Each parameter tag has name and value attributes.

- To change the value of a parameter, edit the value attribute.
- To add a parameter, add another parameter tag with its name and value.
- To delete a parameter, delete the entire parameter tag.

The order of the parameters within the file is not important. Notice the green comment sections in the sample. Use these elements to add useful comments to the configuration file.



Note: When configuring the MID Server for use with a proxy server, be sure to remove the comment tags around the proxy sections that you configure.

```
--<parameters>
  <!-- MID Server Configuration -->
  <parameter name="url" value="https://example.service-now.com"/>
  <parameter name="refresh_rate" value="65"/>
  <parameter name="name" value="Super Duper MID Server #1"/>
  <parameter name="mid_sys_id" value=""/>
  <!-- MID Server Threads -->
  <parameter name="threads.max" value="25"/>
  <!-- MID Server proxy configuration -->
  <parameter name="mid.proxy.host" value=""/>
  <parameter name="mid.proxy.port" value=""/>
  <parameter name="mid.proxy.username" value=""/>
  <parameter name="mid.proxy.password" value=""/>
--</--

  MID Server to instance configuration options

  mid.instance.use_proxy
    - when talking to instance, should we use the proxy config?

  mid.instance.username
  mid.instance.password
    - supply username and password if instance has basic authentication enabled

  ==>
  <parameter name="mid.instance.use_proxy" value="true"/>
  <parameter name="mid.instance.username" value=""/>
  <parameter name="mid.instance.password" value=""/>
--</--

  MID Server upgrade options

  mid.upgrade.use_proxy
    - when talking to upgrade server, should we use the proxy config?

  mid.upgrade.branch
    - define a branch our MID Server is pinned to

  -->
  <parameter name="mid.upgrade.use_proxy" value="true"/>
  <parameter name="mid.upgrade.branch" value=""/>
</parameters>
```



Note: The sample file here is from Firefox. Conventional text editors, such as Notepad, Wordpad, or TextEdit, do not display colors and variable fonts.

Required Configuration

All MID Servers require the following configuration settings.

Setting up MID Server User Credentials

Each MID Server must have a set of ServiceNow user credentials with the mid_server role. Any change to user credentials or roles used by the MID Server user requires a restart of the MID Server service.

Required Parameters

The following parameters are required for all MID Servers.



Note: Using special characters in an XML configuration file requires you to encode them.

Label	Names	Description
Instance URL	url	<p>Specifies the URL to the associated ServiceNow instance. Normally the URL is similar to https://instance.service-now.com, where you replace <i>instance</i> with the instance name. If you host your own ServiceNow instance, use the URL set by your organization.</p> <ul style="list-style-type: none">• Type: string• Default value: none
MID Server ID	mid_sys_id	<p>Records the MID Server record's unique identifier. This parameter should be empty when you initially configure a MID Server. Do not change the value.</p> <ul style="list-style-type: none">• Type: string• Default value: automatically set (GUID)
MID Server name	name	<p>Use this parameter to supply a name that is meaningful for you. If you do not supply this parameter, the MID Server uses the default value. A set of business rules synchronizes the name in the configuration file with the name in the MID Server record (starting with the Dublin release). The business rules ensure that changing the name in one location also changes the name in the other location.</p> <ul style="list-style-type: none">• Type: string• Default value: YOUR_MIDSERVER_NAME_GOES_HERE
Instance user name	mid.instance.username or glide.glidesoap.username	<p>If the ServiceNow instance has authentication enabled, as it is by default, set this parameter to define the user name the MID Server should use to log in to the instance. This user should have the mid_server role on the ServiceNow instance in order to access necessary tables and fields.</p> <ul style="list-style-type: none">• Type: string• Default value: none
Instance password	mid.instance.password or glide.glidesoap.password	<p>If your ServiceNow instance has authentication enabled, as it is by default, set this parameter to define the password the MID Server should use to log in to the instance.</p> <ul style="list-style-type: none">• Type: string• Default value: none

Optional Configuration

The following configuration settings are optional. While a MID Server should start with the default settings, you may want to change the default values to improve performance or follow your organization's business practices.

Setting MID Server Memory Size

In the base ServiceNow system, the MID Server memory is set to 512MB, which can be configured in the `\agent\conf\wrapper.conf` file in the MID Server installation directory. This setting might not be appropriate for the way your organization uses the MID Server. If you want the MID Server to work harder, allocate more resources to it. Or perhaps the MID Server is located in a small branch office with very few devices, and runs in an environment where memory allocation is shared between a print server, mail server, or web proxy server. In this situation, the MID Server memory allocation might have to be reduced.

To edit the memory allocation:

1. Navigate to `\ServiceNow\<MID Server name>\agent\conf` and open the `wrapper-override.conf` file in a text editor.

For more information about this file, see [Installing Multiple MID Servers on a Single System](#).

2. Locate the following lines in the file:

```
# OPTIONAL: Maximum Java Heap Size (in MB)
# wrapper.java.maxmemory=512
```

3. Edit the memory allocation.
4. Remove the comment tag (#) from the memory allocation parameter.
5. Save the file.
6. Restart the MID Server service.

Setting MID Server Thread Use

By default, the MID Server uses a maximum of 25 threads. If the MID Server is running on a host containing many other programs that must compete for CPU time, fewer threads than the default of 25 might be necessary. You can set the MID Server to use as few as 5 threads without issues. If the MID Server needs more speed, and the host is powerful enough or lightly loaded with other programs, raise the thread setting. The thread limit depends on the hardware and the operating system of the host. You might have to experiment to find the optimal value for your situation. The following general observations may be useful:

- Most MID Server tasks require *file handles* to do their job.
 - **Windows:** On the Windows operating system, file handles are available in a fixed quantity. If you configure too many MID Server threads on a Windows host, the MID Server can consume all the file handles before approaching maximum CPU usage. This situation appears as an **Out of file handles** error in the MID Server log and indicates that the MID Server is trying to use too many threads.
 - **Unix and Linux:** UNIX and Linux hosts have a much different scheme for allocating file handles. Generally, you can increase MID Server thread use on these operating systems until the CPU of the host is overloaded. See your OS documentation for monitoring CPU usage.
- Each thread on the MID Server requires some memory. Exactly how much memory varies considerably from task to task and depends on the equipment being discovered. To increase the number of threads, you might have to increase the amount of memory that Java uses. If you configure insufficient memory, an **Out of memory** error appears in the MID Server log.

To edit the maximum number of threads allowed for the MID Server:

1. Open the `\agent\config.xml` file using any text editor.
2. Locate the following lines:

```
<!-- MID Server Threads -->
<parameter name="threads.max" value="25"/>
```

3. Edit the value. Keep in mind the cautions described above.
4. Save the record.
5. Restart the MID Server service.

Enabling Script File Synchronization for Windows Enhanced Security

Windows Internet Explorer enhanced security blocks downloaded files that it determines are potentially dangerous. Without script file synchronization, Internet Explorer blocks files downloaded for use by the MID Server, forcing ServiceNow administrators to unblock each file manually. File synchronization creates the files on the MID Server rather than downloading them, which does not trigger security blocking. Also, file synchronization between script records on the instance and the MID Server protects any customer updates in those records from being overwritten during a ServiceNow upgrade.

Script file synchronization is available starting with the Dublin release. If you are using an older version, see the previous version information.

How File Synchronization Works

Script files synchronized with the MID Server are stored on the ServiceNow instance in the MID Server Script File [ecc_agent_script_file] table (**MID Server > Script Files**). When the MID Server first connects to the instance, ServiceNow creates a directory called `\scripts` in the MID Server root. The instance then creates a parent directory in the path `\scripts\<parent name>` using definitions from the ecc_agent_script_file table. Finally, the instance creates the script files themselves inside the parent directory using the records from the ecc_agent_script_file table.

The record for the parent directory looks like this:

MID Server Script File [Update] [Delete] [Refresh] [Help]

Name: PowerShell

Description: Holds PowerShell script files for use by the MID Server

Parent: [Search]

Active: ☒

Directory: ☒ Creates a parent directory inside the MID Server /scripts directory

[Update] [Delete]

MID Server Script Files [New] Go to [Name] [Search]

Parent = PowerShell

Name	Description	Active	Directory
Credentials.psm1	Manages credential testing to see if the...	true	false
LaunchProc.psm1	Launches a process and fetches the output...	true	false
PSScript.ps1	Main wrapper script for all PowerShell s...	true	false
WMIFetch.psm1	Collection of functions used to fetch da...	true	false
XMLUtil.psm1	Collection of methods for managing XML c...	true	false

Actions on selected rows... [1] to 5 of 5

The instance creates each script file in the parent directory on the MID Server using the record **Name** from the ecc_agent_script_file table as the file name and the **Script** field payload as the file contents. A script file record looks like this:

MID Server Script File

Name: Credentials.psm1

Description: Manages credential testing to see if there is proper access to a target system

Parent: PowerShell

Active: ☒

Directory: ☐

Script:

```
<#####>
# Turn user/password into a credential object for use in cmdlets that take a credential
#####>
function getCredential {
    param([string]$user, [string]$password)

    if ($password) {
        $passwordSecure = convertto-securestring -string $password -asplaintext -force;
    } else {
        # If no password was supplied, use an empty instance of SecureString
        $passwordSecure = new-object System.Security.SecureString;
    }

    $cred = new-object -typename System.Management.Automation.PSCredential -argumentlist "$user",$passwordSecure;

    return $cred;
}
```

Update Delete

Unblocking PowerShell Scripts Prior to the Dublin Release

Click the plus for previous version information

Enhanced security on the Windows operating systems can block PowerShell from working with Discovery and Orchestration. If PowerShell does not run with Discovery or Orchestration, *unblock* the MID Server archive:

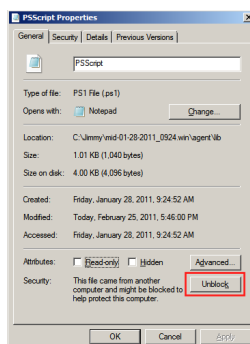
- **MID Server archive:** mid.<build date>.<operating system>.<system bit>.zip

If you do not unblock the archive, unblock each individual file:

- Credentials.psm1
- LaunchProc.psm1
- MSSqlAuth.ps1 (Removed in the Calgary release)
- MSSqlWinAuth.ps1 (Removed in the Calgary release)
- PSScript.ps1
- WMIFetch.psm1
- XmlUtil.psm1

Perform this procedure on *each* MID Server machine:

1. Navigate to the MID Server archive file.
2. Right-click the first file in the list and select **Properties** from the menu.
3. In the Properties dialog box, click **Unblock**.
4. Repeat the procedure for each of the remaining files, if necessary.



Adding SSL Certificates

You can configure the MID Server to connect over SSL by adding the following certificates to the cacerts keystore file:

- Signing Certificate Authority (CA) certificate
- MID Server certificate

To add a certificate to a MID Server:

1. Open a command prompt and navigate to the folder containing the JRE keytool ^[2]. For example:
`cd C:\Program Files (x86)\ServiceNow\<MidServer(s)>\agent\jre\bin`
2. Enter the following keytool command to import a certificate into the MID Server's cacerts keystore:
`keytool -import -alias <certificate alias> -file "<path to certificate>" -keystore "<path to MID Server(s)>\agent\jre\lib\security\cacerts"`

For example:

```
keytool -import -alias MyCA -file "C:\myca.cer" -keystore "C:\Program Files (x86)\ServiceNow\MIDserver\agent\jre\lib\security\cacerts"
```



Note: Keytool prompts for a certificate password. If the certificate is for a CA, keytool also asks whether to trust the certificate authority.

To add a certificate to an instance, see [Uploading a Certificate](#).

MID Server Properties

Use the following properties to control the behavior of all probes on a MID Server or all probes on all MID Servers. See [Setting MID Server Properties](#).

Label	Names	Description
Max length of a payload that a MID Server will return	mid.discovery.max_payload_size	<p>Specifies the maximum string length of Discovery probe results that the MID Server will send to the instance. The MID Server verifies the size of the Discovery probe results before sending them to the instance. If the Discovery probe results exceed the limit, the MID Server discards them and returns a warning message. This applies only to probes where the Used by Discovery field is true. Set the value to any negative number to disable the payload limit and allow Discovery payloads of any size to be sent to the instance. For example, -1. This parameter is available starting with the Eureka release.</p> <ul style="list-style-type: none"> • Type: integer (bytes) • Default value: 5000000
Max length of an ECCQ payload XML that a MID Server will send to the instance	mid.eccq.max_payload_size	<p>Specifies the maximum string length of a payload that the MID Server will send to the instance. The MID Server verifies the size of the payload before sending it to the instance. If the payload size exceeds the limit, the MID Server saves a copy of the payload to the filesystem on the MID Server host, and returns an error message that contains the location of the file.</p> <ul style="list-style-type: none"> • Type: integer (bytes) • Default value: 20000000

CIM Parameters

This parameters determine how a MID Server conducts CIM Discovery.

Label	Names	Description
Interval to wait between requests to the same CIMOM (ms)	mid.cim.request.interval	<p>Specifies the number of milliseconds to wait between requests to the same Common Information Model Object Manager (CIMOM). This parameter is available starting with the Eureka release.</p> <ul style="list-style-type: none"> • Type: integer (milliseconds) • Default value: 0
The maximum amount of simultaneous connections allowed per CIMOM	mid.cim.host.connection.limit	<p>Specifies the maximum number of simultaneous connections to each Common Information Model Object Manager (CIMOM). A value of zero disables simultaneous connections. This parameter is available starting with the Eureka release.</p> <ul style="list-style-type: none"> • Type: integer (number of connections) • Default value: 0

Connection Parameters

Label	Names	Description
The maximum amount of standard messages to queue in memory for processing	mid.max.messages	<p>Specifies the maximum number of messages to hold in memory for processing. The default value is computed from the <code>threads.max</code> parameter.</p> <ul style="list-style-type: none"> • Type: integer • Default value: <code>[10 * threads.max]</code>
Instance date format	instance.date.format	<p>Specifies the format the instance uses for dates and times. The primary impact of setting this parameter is to allow the MID Server to correctly refresh its start and stop times on the MID Server record in ServiceNow. The format of this date/time string is identical to that used by the Java SimpleDateFormat class, documented here ^[3] in the section titled <i>Date and Time Patterns</i>.</p> <ul style="list-style-type: none"> • Type: string (Date format) • Default value: <code>yyyy-MM-dd HH:mm:ss</code>
MID Server immediate response enable	glide.mid.fast.responses	<p>Instructs the MID Server to try sending messages to the instance as soon as they are ready. Normally the MID Server sends message to the ServiceNow instance <i>serially</i> (that is, one message at a time). Since many probes can be run in parallel, there can be multiple messages simultaneously transmitted to the instance. Setting this parameter to true may decrease the time between a probe's completion and its response arriving at the instance. However, the multiple simultaneous messages consume resources, decreasing the overall instance responsiveness. If there are communications problems, this parameter's value can also cause a <i>logjam</i> on the MID Server, as threads normally used for running probes may become consumed for sending messages. Generally, leave this parameter out of your configuration. Setting it to true is meaningful only under very special circumstances.</p> <ul style="list-style-type: none"> • Type: <code>true false</code> • Default value: <code>false</code>
MID Server JMX enable	mid.jmx.enabled	<p>Enables a JMX server on the MID Server, which exposes some management information to JMX consoles. Implementing JMX requires additional configuration of the Java runtime environment. Setting this parameter to true is only recommended for those with detailed knowledge of the Java security architecture and a specific need for JMX.</p> <ul style="list-style-type: none"> • Type: <code>true false</code> • Default value: <code>false</code>

MID Server max transmission queue size	glide.mid.max.sender.queue.size	<p>Places an upper limit on how large the queue is allowed to get. The MID Server starts deleting queued messages if this limit is exceeded. When the MID Server generates messages to the ServiceNow instance faster than it can send them, it queues them temporarily on the file system of the MID Server's host. This queue is normally quite small, and is completely emptied as soon as the MID Server processing slows for a short period. However, this queue can grow in size when there are communication problems between the MID Server and the instance, and especially if there is an integration running on the MID Server, .</p> <p>The parameter is of the form {number}{multiplier}, where {number} is any positive decimal number including non-integers, and the optional multiplier is any spelling of <i>bytes</i>, <i>kilobytes</i>, <i>megabytes</i>, <i>gigabytes</i>, or <i>terabytes</i> (only the first character is tested, and the test is case-insensitive). The default multiplier is bytes. White space is liberally tolerated. The following strings all represent valid parameters: "1000000000", "0.5m", "5 GB", "7.67gigas", "145.69392 meg", and "1.1 terra".</p> <ul style="list-style-type: none"> • Type: string • Default value: 0.5g
MID Server maximum number of probe threads	threads.max	<p>Controls the number of execution threads (simultaneous work) that probes may use. This parameter provides direct control over what CPU resources the MID Server consumes on the computer that hosts it. To decrease the MID Server's CPU consumption, lower the number of threads. To make the MID Server work faster, increase the number of threads. See Setting MID Server Thread Use.</p> <ul style="list-style-type: none"> • Type: integer (threads) • Default value: 25
MID Server poll time	mid.poll.time	<p>Sets the MID Server polling interval (in seconds).</p> <ul style="list-style-type: none"> • Type: integer (seconds) • Default value: 15

Credentials Parameters

Label	Names	Description
Credentials provider	mid.credentials.provider	<p>Specifies the Java class name of the credentials provider.</p> <ul style="list-style-type: none"> • Type: string • Default value: com.service_now.mid.creds.standard.StandardCredentialsProvider

Debug Parameters

Label	Names	Description
Debug logging enable	debug.logging	<p>Specifies whether to enable logging of MID Server events and messages (both sent and received). Normally this parameter is only used by developers, but it is occasionally useful when troubleshooting a problem. Be aware that setting this parameter to true causes intensive logging on the MID Server, potentially using considerable disk space.</p> <ul style="list-style-type: none"> • Type: true false • Default value: false
Debug mode enable	debug	<p>Specifies whether to enable debug logging on the MID Server. Normally this parameter is only used by developers, but it is occasionally useful when troubleshooting a problem. Be aware that setting this parameter to true causes intensive logging on the MID Server, potentially using considerable disk space.</p> <ul style="list-style-type: none"> • Type: true false • Default value: false

Enables debug logging for CIM / WBEM / SLP / SMI-S	mid.cim.debug	<p>Specifies whether to enable debug logging for CIM, WBEM, SLP, or SMI-S.</p> <ul style="list-style-type: none"> • Type: true false • Default value: false
Enable debug logging for ServiceNow SSH Client	mid.ssh.debug	<p>Enables SSH debug information in the log file. The parameter usage depends on whether the ServiceNow SSH client is enabled (starting with the Eureka release).</p> <p>When the ServiceNow SSH client is enabled, the parameter functions as follows:</p> <ul style="list-style-type: none"> • Type: string • Default value: false <p>The following string values are valid for the ServiceNow SSH client:</p> <ul style="list-style-type: none"> • true: Enables SSH debug information in the log file. • false: Disables SSH debug information in the log file. • <IP Addresses>: Specify which IP ranges to enable SSH debug information in the log file. You can enter IP addresses in the following formats: <ul style="list-style-type: none"> • An IP range defined by a slash and the number of bits in the subnetmask ^[4]. For example, the string <code>10.10.10.0/24</code> scans 24 bits of IP addresses from <code>10.10.10.0</code> to <code>10.10.10.254</code>. • An IP range defined by a dash. For example, the string <code>10.10.11.0-10.10.11.165</code> scans the IP addresses from <code>10.10.11.0</code> to <code>10.10.11.165</code>. • A comma-separated list of specific IP addresses. For example the string <code>10.10.11.200,10.10.11.235</code> scans the IP addresses <code>10.10.11.200</code> and <code>10.10.11.235</code>. • deferred: Logs SSH debug information in memory unless an error or warning occurs. If an error or warning occurs, the platform publishes the debug information to the log file. This ensures that only the part of the log file pertaining to the error or warning is recorded. If no error or warning is detected, the platform deletes the unused log data from memory when the session closes. Each session stores up to 1000 log messages. If the session exceeds 1000 log messages, the deferred log discards the oldest log message to make room for the newest log message. <p>When the ServiceNow SSH client is disabled, the parameter enables or disables SSH debug information in the log file:</p> <ul style="list-style-type: none"> • Type: true false • Default value: false

DNS Parameters

Label	Names	Description
DNS scanning regulator interval (ms)	mid.dns_scan.regulator.interval_ms	<p>Specifies the interval between DNS scans in milliseconds.</p> <ul style="list-style-type: none"> • Type: integer • Default value: 10
DNS scanning regulator packets per interval	mid.dns_scan.regulator.packets_per_interval	<p>Specifies the number of regulator packets per DNS scan.</p> <ul style="list-style-type: none"> • Type: integer • Default value: 1
DNS scanning default name servers	mid.dns_scan.default_name_servers	<p>Specifies the host names or IP addresses of the default name servers.</p> <ul style="list-style-type: none"> • Type: string • Default value: none
DNS scanning additional name servers	mid.dns_scan.additional_name_servers	<p>Specifies the host names or IP addresses of any additional name servers.</p> <ul style="list-style-type: none"> • Type: string • Default value: none

DNS scanning load balancing enable	mid.dns_scan.load_balancing_enable	Specifies whether to enable load balancing of name servers.
		<ul style="list-style-type: none"> • Type: true false • Default value: false

ECC Queue Parameters

Label	Names	Description
The amount of time to look-behind on the ECCQ when querying for more work (s)	mid.eccq.monitor.window	Specifies the time period to look behind on the ECC Queue in seconds. The default value is 30 minutes. <ul style="list-style-type: none"> • Type: integer • Default value: 1800 seconds
MID Server ECC query interval	query_backoff	Allows the interval at which the MID Server queries the ECC Queue to lengthen if the MID Server is idle. By default, the MID Server queries the ECC Queue for work every 15 seconds. In a system that employs a large number of MID Servers, these queries can produce unnecessary traffic during periods of light MID Server activity. When the <code>query_backoff</code> parameter is set to true , the query interval slowly lengthens for an idle MID Server. Eventually, the interval slows to one query every four minutes and holds at that rate until the MID Server has a job to do. When the MID Server starts work again, the query interval for that MID Server immediately increases to once every 15 seconds and continues at that rate until the demand on the MID Server backs off again. <ul style="list-style-type: none"> • Type: true false • Default value: false

Logging Parameters

Label	Names	Description
Disable monitor checking	disable_monitors	Specifies whether to disable the MID Server from actively checking for monitors on the instance. <ul style="list-style-type: none"> • Type: true false • Default value: false
Query logging enable	mid.show.queries	Instructs the MID Server whether to log details about every query it makes to the ServiceNow instance. Typically this parameter is only used by developers, but it is occasionally useful when troubleshooting a problem. Be aware that setting this parameter to true causes intensive logging on the MID Server, potentially using considerable disk space. <ul style="list-style-type: none"> • Type: true false • Default value: false
Remote logging disable	disable.remote.logging	Prevents the MID Server from logging any information to the MID Server log on the ServiceNow instance. Relatively little information is logged on the instance in any case, but setting this parameter to true eliminates all logging to the instance. <ul style="list-style-type: none"> • Type: true false • Default value: false
Status sending disable	disable.status	Prevents the MID Server from sending a status report to the ServiceNow instance every 10 minutes. <ul style="list-style-type: none"> • Type: true false • Default value: false

Proxy Server Parameters

Use these parameters to configure how your MID Server communicates through a proxy server to access the ServiceNow instance.

Label	Names	Description
Instance proxy enable	mid.instance.use_proxy or mid.proxy.use_proxy	<p>If your MID Server must go through a web proxy to access the ServiceNow instance, set this parameter to true to instruct the MID Server to use the proxy. You must also set the proxy server's host and port, and perhaps the user name and password as well.</p> <ul style="list-style-type: none"> • Type: true false • Default value: false
Instance proxy host	mid.proxy.host	<p>If your MID Server must go through a web proxy to access the ServiceNow instance, set this parameter to define the proxy's host.</p> <ul style="list-style-type: none"> • Type: string • Default value: none
Instance proxy password	mid.proxy.password	<p>If your MID Server must go through a web proxy to access the ServiceNow instance, and your proxy requires a password, set this parameter to define that password.</p> <ul style="list-style-type: none"> • Type: string • Default value: none
Instance proxy port	mid.proxy.port	<p>If your MID Server must go through a web proxy to access the ServiceNow instance, set this parameter to define the proxy's port.</p> <ul style="list-style-type: none"> • Type: integer (0-65535) • Default value: 80
Instance proxy user name	mid.proxy.username	<p>If the MID Server must go through a web proxy to access the ServiceNow instance, and the proxy requires a user name, set this parameter to define that user name.</p> <ul style="list-style-type: none"> • Type: string • Default value: none

Shazzam Parameters

Label	Names	Description
Port probe packet interval	mid.shazzam.regulator.interval_ms	<p>Sets the interval, in milliseconds, in which Shazzam can launch packets. This parameter works with the <code>mid.shazzam.regulator.packets_per_interval</code> parameter to set the number of packets allowed in this interval. By default, Shazzam launches one packet each millisecond.</p> <ul style="list-style-type: none"> • Type: integer • Default value: 1
Port probe packets launched per regulator interval	mid.shazzam.regulator.packets_per_interval	<p>Sets the number of packets that Shazzam can launch in the configured time interval. This parameter works with the <code>mid.shazzam.regulator.interval_ms</code> parameter, which sets that interval. By default, Shazzam launches one packet each millisecond.</p> <ul style="list-style-type: none"> • Type: integer • Default value: 1
Shazzam chunk size	mid.shazzam.chunk_size	<p>Specifies the maximum number of IP addresses that Shazzam scans in parallel. This parameter primarily controls outbound port consumption.</p> <ul style="list-style-type: none"> • Type: integer • Default value: 100

SNMP Discovery Parameters

Label	Names	Description
Enable automatic inclusion of SNMP public community string	mid.snmp.enable_auto_public	Specifies whether to enable the SNMP public community string ^[5] . <ul style="list-style-type: none"> • Type: true false • Default value: true
Timeout to wait for a response for each OID request (ms)	mid.snmp.request.timeout	Specifies the timeout value for each SNMP OID ^[6] request. The default is 1.5 seconds. <ul style="list-style-type: none"> • Type: integer • Default value: 1500 milliseconds
Inactivity timeout for an established session - after the first response is received (ms)	mid.snmp.session.timeout	Specifies the timeout value for existing SNMP connections. The default is 0.5 seconds. <ul style="list-style-type: none"> • Type: integer • Default value: 500 milliseconds

SSH Discovery Parameters

Label	Names	Description
MID Server connection cache	mid.connection_cache	Specifies whether to cache connections. Set to false to disable connection caching. This parameter applies to SSH connections only. <ul style="list-style-type: none"> • Type: true false • Default value: true
Decide if the PATH environment variable should be set for SSH commands	mid.ssh.set_path	Specifies whether to set the PATH environment variable for SSH commands. <ul style="list-style-type: none"> • Type: true false • Default value: true
Process commands against localhost via SSH rather than console	mid.ssh.local	Specifies whether to execute commands for the MID Server host machine (localhost) via SSH rather than from a console. This allows long-running commands to execute properly. This parameter applies to the legacy SSH client only. <ul style="list-style-type: none"> • Type: true false • Default value: false
MID Server SSH connection per host	mid.ssh.connections_per_host	Controls the number of concurrent probes the MID Server can run against a given host. Lowering the number of concurrent connections can slow Discovery. <ul style="list-style-type: none"> • Type: integer • Default value: <ul style="list-style-type: none"> • 7 for the ServiceNow client • 3 for the legacy SSH client
Enable (or disable) sudo to preserve environment (-E) for SSH	mid.ssh.sudo_preserve_environment	Specifies whether to use sudo ^[7] to preserve the environment for SSH. <ul style="list-style-type: none"> • Type: true false • Default value: false

Set the PATH environment paths for SSH commands

mid.ssh.path_override

Overrides the default paths set before executing a command. Enter one or more override paths delimited by a colon (:). The default path is `/usr/sbin: /usr/bin: /bin: /sbin`.

The ServiceNow SSH client accepts the following prefixes in front of the `path_override` value.

- **append:** Appends the override path to the end of the host's path. This is the default behavior.
- **replace:** Replaces the host path with the `path_override` value.
- **prepend:** Appends the override path to the front of the host path.
- **Type:** string (a colon-separated list of directories)
- **Default value:** None

Enable ServiceNow SSH Client

mid.ssh.use_snc

Enables the ServiceNow SSH client (SNCSSH), which is a ServiceNow implementation of an SSH client. SNCSSH is active by default on new instances starting with the Eureka release. Customers upgrading to Eureka or a later release can manually switch to the ServiceNow SSH client with this parameter. Enabling the ServiceNow SSH client disables the legacy SSH client. This parameter is available starting with the Eureka release.

- **Type:** true | false
- **Default value:** false

The maximum number of times to retry an SSH operation after a timeout

mid.ssh.max_retries

Specifies the maximum amount of times to retry an SSH operation after a time-out. The system sleeps two seconds between each connection attempt. By default, the MID Server retries once only. Set the parameter to **0** to disable retries.

- **Type:** integer
- **Default value:** 1

Sets a different remove file command to replace the default `/bin/rm -f`

mid.ssh.alt_rm

Sets a different SSH remove file command.

- **Type:** string
- **Default value:** none

Delay sending any SSH commands to a server after connecting

mid.ssh.initial_delay_ms

Delays sending any SSH probe commands to a server after connecting to the target for the time specified, in milliseconds. This parameter is available starting with the Calgary release. This parameter applies to the legacy SSH client only.

- **Type:** integer (milliseconds)
- **Default value:** 0

Suppress history file generation for SSH

mid.ssh.suppress_history

Suppresses the generation of the SSH history file. This parameter applies to the legacy SSH client only.

- **Type:** true | false
- **Default value:** false

Timeout in ms for SSH socket read

mid.ssh.socket_timeout

Specifies the timeout value for the SSH socket to prevent issues created by a socket timeout. Some devices, such as systems with embedded controllers like UPSs and PDUs, that have SSH enabled require more time to respond to an authentication request. The default value of 2 minutes ensures such requests do not timeout prematurely.

In versions prior to Fuji, the default value is 60000 (1 minute).

- **Type:** integer (milliseconds)
- **Default value:** 120000 (2 minutes)

Timeout in ms for SSH channel activity

mid.ssh.channel_timeout

Specifies the amount of time that the MID Server waits for activity on the SSH socket before closing the connection. If there has been no activity on the SSH socket for the specified timeout value, the MID Server closes the connection. Some devices, such as systems with embedded controllers like UPSs and PDUs, that have SSH enabled may require more time to respond to an authentication request. This parameter is available starting with the Eureka release.

- **Type:** integer (milliseconds)
- **Default value:** 120000 (2 minutes)

Timeout in ms for SSH socket read	mid.ssh.session_timeout	<p>Specifies the amount of time that a cached session remains in memory after last use. Excessively small values tend to decrease performance. This parameter applies to the ServiceNow SSH client only.</p> <ul style="list-style-type: none"> • Type: integer (milliseconds) • Default value: 300000 (5 minutes)
Timeout for SSH command execution (ms)	mid.ssh.command_timeout_ms	<p>The timeout duration, in milliseconds, for the execution of an SSH command.</p> <ul style="list-style-type: none"> • Type: integer (milliseconds) • Default value: 300000 (5 minutes)
Use keyboard interactive authentication for SSH	mid.ssh.use_keyboard_interactive	<p>Uses the <i>keyboard interactive</i> authentication mode ^[8] in SSH daemons on which it is activated.</p> <ul style="list-style-type: none"> • Type: true false • Default value: false
Min size of DH group in bits	mid.ssh.dh_group_length_min	<p>Specifies the minimum group length in bits used for generating a "shared secret" key in Diffie-Hillman key exchange ^[9]. The larger the key the more secure the SSH connection is but at the cost of performance. This parameter is available starting with the Eureka release.</p> <ul style="list-style-type: none"> • Type: integer (bits) • Default value: 1024
Max size of DH group in bits	mid.ssh.dh_group_length_max	<p>Specifies the maximum group length in bits used for generating a "shared secret" key in Diffie-Hillman key exchange ^[9]. The larger the key the more secure the SSH connection is but at the cost of performance. This parameter is available starting with the Eureka release.</p> <ul style="list-style-type: none"> • Type: integer (bits) • Default value: 2048

Default Paths for SSH Commands

By default, the MID Server is configured to search for SSH commands in the following paths and the logged-on user's default paths:

- /usr/sbin
- /usr/bin
- /bin
- /sbin


Upgrade Parameters

Label	Names	Description
Fixed MID Server version	mid.pinned.version	<p>Name of the version to which this MID Server is pinned.</p> <ul style="list-style-type: none"> • Type: string • Default value: build timestamp
Upgrade branch	glide.mid.autoupgrade.branch <i>or</i> mid.upgrade.branch	<p>Defines a <i>branch</i> (a directory on the distribution server) the MID Server should download its upgrades from. This might be set if you had a special MID Server version for some reason. Consult with ServiceNow <i>before</i> adding this parameter to your configuration.</p> <ul style="list-style-type: none"> • Type: string (path) • Default value: none

Upgrade proxy enable	mid.upgrade.use_proxy	<p>If your MID Server must go through a web proxy to access the upgrade URL, set this parameter to true to instruct the MID Server to use the proxy. You must also set the proxy server's host and port. If the instance proxy user name and password are set, they are used for the upgrade proxy as well.</p> <ul style="list-style-type: none"> • Type: true false • Default value: false
Upgrade proxy host	glide.mid.autoupgrade.proxy_host <i>or</i> glide.gldessoap.proxy_host	<p>If your MID Server must go through a web proxy to access the upgrade URL, define the proxy's host here. You must restart the instance after changing this property to apply the change in versions prior to Calgary Patch 6.</p> <ul style="list-style-type: none"> • Type: string (URL) • Default value: none
Upgrade proxy port	glide.mid.autoupgrade.proxy_port <i>or</i> glide.gldessoap.proxy_port	<p>If your MID Server must go through a web proxy to access the upgrade URL, define the proxy's port here. You must restart the instance after changing this property to apply the change in versions prior to Calgary Patch 6.</p> <ul style="list-style-type: none"> • Type: integer (0-65535) • Default value: 80
Upgrade proxy user	glide.mid.autoupgrade.proxy_user	<p>If your MID Server must go through a web proxy to access the upgrade URL, define the proxy's user name here.</p> <ul style="list-style-type: none"> • Type: string (URL) • Default value: none
Upgrade proxy password	glide.mid.autoupgrade.proxy_password	<p>If your MID Server must go through a web proxy to access the upgrade URL, define the proxy's password here.</p> <ul style="list-style-type: none"> • Type: string • Default value: none
Upgrade URL	glide.mid.autoupgrade.host	<p>Controls where the MID Server downloads its upgrades from. Normally, you should not set this parameter.</p> <ul style="list-style-type: none"> • Type: string (URL) • Default value: [10]

Windows Discovery Parameters

Label	Names	Description
Enable or Disable the enforcement of UTF-8 for command output	mid.powershell.enforce_utf8	<p>Enable this parameter to force commands on a target Windows system to return UTF-8 encoded output. Disabling it allows the target system to use its default encoding. This parameter is only valid when PowerShell is enabled. Setting this value to false may result in incorrect values in the CMDB when non-ASCII characters are returned by a probe.</p> <ul style="list-style-type: none"> • Type: true false • Default value: true
Enable PowerShell for Discovery	mid.use_powershell	<p>Specifies whether to enable PowerShell for Discovery. The MID Server requires PowerShell version 2 to operate. If the MID Server cannot find the correct version of PowerShell, it uses WMIRunner instead.</p> <ul style="list-style-type: none"> • Type: true false • Default value: true

Enable/Disable automatically falling back to the MID Server service user credential if all other credentials fail	mid.powershell.local_mid_service_credential_fallback	<p>Specifies the login credentials the MID Server uses if all other credentials fail. This parameter is available starting with the Calgary release.</p> <ul style="list-style-type: none"> • Type: true false • Default value: true
Timeout for Windows probes	mid.windows.probe_timeout	<p>Specifies the timeout value for the Windows probe, in seconds. The default value is 5 minutes.</p> <ul style="list-style-type: none"> • Type: integer • Default value: 300 seconds
MSSQL credentials for PowerShell	mid.powershell.use_mssqlauth	<p>Determines whether PowerShell should use Integrated Windows Authentication ^[11], also known as Windows Integrated Security, or SQL authentication when attempting to log into the MSSQL instance. PowerShell uses Windows Integrated Security by default.</p> <p>Note: This parameter is obsolete starting with the Calgary release and has been removed from the platform. Microsoft SQL Server discoveries use the PowerShell probe, which uses the MID Server's credentials. The Calgary upgrade removes any MSSQL credentials from the Credentials [discovery_credentials] table.</p>  <ul style="list-style-type: none"> • Type: true false • Default value: false
Powershell use credentials table	mid.powershell.use_credentials	<p>Specifies whether PowerShell Discovery should use the Windows credentials from the credentials table. To use PowerShell Discovery on a single domain, set this parameter to false, and then restart the MID Server. In this case, the MID Server runs the probes with the credentials of the user for the MID Server process.</p> <ul style="list-style-type: none"> • Type: true false • Default value: true
Path to Powershell executable	mid.powershell.path	<p>Enables an administrator to point to a specific PowerShell on a MID Server in cases where more than one PowerShell is installed. Supply the path to the directory containing the PowerShell executable, for example, <i>C:\mypowershell</i> or <i>C:\mypowershell\</i>. ServiceNow automatically appends the string <i>powershell.exe</i> to the path.</p> <p>This parameter might be necessary when both 32-bit and 64-bit PowerShells are active on the same MID Server, and it becomes necessary to launch the correct PowerShell for the context. Note that 64-bit Windows employs file system redirection and the MID Server runs as a 32-bit application. If the path is in <i>%WinDir%\System32</i>, Windows automatically redirects to <i>%WinDir%\SysWOW64</i>. To avoid redirection, specify the path as <i>%WinDir%\Sysnative</i>. An example would be to specify <i>C:\WINDOWS\sysnative\WindowsPowerShell\v1.0\</i> instead of <i>C:\WINDOWS\system32\WindowsPowerShell\v1.0\</i>.</p>



Note: *On a 64-bit version of Windows Server 2003 or Windows XP, a Microsoft hotfix^[12] may be required to enable this capability.*

To discover applications running on a 64-bit Windows machine in the Calgary release, the MID Server must be running on a 64-bit Windows host machine. For MID Servers installed on 32-bit hosts to discover 64-bit Windows applications, you must add the `mid.powershell.path` parameter to the MID Server and define the `C:\WINDOWS\system32\WindowsPowerShell\1.0\` path.

- **Type:** string (path)
- **Default value:** none

Timeout for all
Windows probes
on a MID Server

`windows_probe_timeout`

Sets the timeout interval for all Windows probes on a specific MID Server. This value is overridden by the values configured for individual probes with the `wmi_timeout` probe parameter.

- **Type:** integer
- **Default value:** none

References

- [1] https://docs.servicenow.com/bundle/jakarta-it-operations-management/page/product/mid-server/concept/c_MIDServerConfiguration.html
- [2] <http://docs.oracle.com/javase/1.3/docs/tooldocs/win32/keytool.html>
- [3] <http://java.sun.com/j2se/1.4.2/docs/api/java/text/SimpleDateFormat.html>
- [4] <http://en.wikipedia.org/wiki/Subnetwork>
- [5] http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol#Security_implications
- [6] http://en.wikipedia.org/wiki/Object_identifier
- [7] <http://en.wikipedia.org/wiki/Sudo>
- [8] http://en.wikipedia.org/wiki/Secure_Shell#Architecture
- [9] http://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange
- [10] <http://install.service-now.com/glide/distribution/builds/mid/>
- [11] [http://msdn.microsoft.com/en-us/library/aa292114\(VS.71\).aspx](http://msdn.microsoft.com/en-us/library/aa292114(VS.71).aspx)
- [12] <http://support.microsoft.com/kb/942589>

Controlling the MID Server Version



Note: The latest release this documentation applies to is Fuji. For the Geneva release, see MID Server^[1]. Documentation for later releases is also on docs.servicenow.com^[2].

Overview

ServiceNow MID Servers are configured to check the instance for the correct MID Server version once every hour. If the version has changed since the last check-in, the MID Server upgrades or downgrades itself accordingly. An administrator might want to edit the MID Server version to enable a new feature or get a fix for a defect. There are two properties that control how and when the MID Server can change its version:

- **mid.buildstamp**
- **mid.version.override**



Note: Downgrades are only possible within the same release family. For example, you can downgrade from Dublin Patch 3 to Dublin Patch 2, but not from Dublin to Calgary.

mid.buildstamp

The **mid.buildstamp** property identifies the MID Server version with an identifier based on the date of the build. This property uses a date and time format of `yyyy-mm-dd-hhmm`.

The MID Server checks for version information hourly. If no override version is configured, the MID Server looks at the *mid.buildstamp* property for the version to use. This property resets itself to the default version (the version that matches your instance version) when the instance is restarted or upgraded, so any user changes are lost at that time.

mid.version.override

Use this property to set an override condition for the current MID Server version. When the MID Server checks the version each hour, it looks at the *mid.version.override* property first. If this property is empty, the MID Server will get its version information from the *mid.buildstamp* property. If an override version is configured, the MID Server uses this value and ignores the version information in the *mid.buildstamp* property. This override value remains when the instance is restarted and is passed to the MID Server at check in. However, the version in the *mid.version.override* property is deleted during an upgrade, allowing the MID Server to reset itself to the version in the *mid.buildstamp* property.

Create the property and then set the value.

1. In the Navigation pane filter, type **sys_properties.list**.

The list of system properties appears.

2. Click **New**.
3. Type **mid.version.override** in the **Name** field.
4. Enter a description, such as, **Set an override value for the current MID Server version**.
5. Enter a version for the MID Server to use that is different from the version ServiceNow has selected in the *mid.buildstamp* property.

The date and time format is `yyyy-mm-dd-hhmm`.

6. Click **Submit**.

MID Server Heartbeat



Note: This article applies to Fuji and earlier releases. For more current information, see *MID Server Heartbeat*^[1] at <http://docs.servicenow.com> **The ServiceNow Wiki is no longer being updated. Visit <http://docs.servicenow.com> for the latest product documentation.**

Overview

The ServiceNow platform checks the MID Server for a response every 5 minutes, using a synthetic transaction monitoring system. When the MID Server changes status (from **Up** → **Down** or from **Down** → **Up**), a system event is triggered which can be used for **script actions** or to send **notifications**.

Checking for a Heartbeat

ServiceNow instances send a synthetic transaction via the **Heartbeat** probe to every MID server every 5 minutes. The Heartbeat probe functions exactly as a normal probe does and is sent by writing an output record to the **ECC queue**. A MID Server retrieves the record when it queries the ECC queue for work. The MID Server processes the probe just as it would any other probe and responds back to the instance. If the instance does not detect a response from a MID Server, the instance marks that MID Server as **Down**. If the MID Server responds, the instance considers the MID Server to be **Up**.

System Events

When a MID Server transitions from one state to another, one of these events is triggered:

- **mid_server.up:** The MID Server goes from a status of **Down** to a status of **Up**.
- **mid_server.down:** The MID Server goes from a status of **Up** to a status of **Down**.

Scheduled Job

To change the trigger interval for the Heartbeat probe, navigate to *System Scheduler > Scheduled Jobs > Scheduled Jobs*. Open the **MID Server Monitor** record and edit the interval.

Schedule Item

UpdateDelete

Name:MID Server Monitor

Job ID:RunScriptJob

Next action:2010-11-08 09:04:00

State:Ready

Calendar:

System ID:

Job context: #Mon Nov 08 08:59:09 PST 2010
fcScriptName=in the schedule record

Script:
var m = new MonitorMIDServer();
m.monitor();

Trigger type:Interval


Repeat:Days0Hours00:05:00

UpdateDelete

References

[1] https://docs.servicenow.com/bundle/jakarta-it-operations-management/page/product/mid-server/reference/r_MIDServerHeartbeat.html

MID Server User Security



Note: The latest release this documentation applies to is Fuji. For the Geneva release, see MID Server^[1]. Documentation for later releases is also on docs.servicenow.com^[2].

Overview

The **strict SOAP security** feature, enabled by default for any instance that uses **basic authentication**, protects all tables with Access Control Lists (ACL). The tables that the ServiceNow MID Server must access are protected by these ACLs and are unavailable to the MID Server unless the MID Server user has specific roles.

The mid_server Role

The mid_server role allows the MID Server to access protected tables when strict SOAP security is in place. Add this role to the MID Server user for any instance on which basic authentication is enabled. The system adds the necessary SOAP roles automatically with the mid_server role.

User

UpdateDelete

User ID:MyMIDServerUser

First name:MID

Last name:Server

Title:

Department:

Password:

Password needs reset:

Locked out:

Active:

Email:

Notification:Email

Calendar integration:Outlook

Time zone:System (America/Tijuana)

Business phone:

Mobile phone:

Photo:Click to add...

UpdateDelete

Related Links

[Notification Preferences](#)

Roles (8)GroupsDelegates

RolesNewEdit...Go toRole

1 to 8 of 8

User = MID Server

Role	State	Granted by	Inherited
<input type="checkbox"/> mid_server	Active		false
<input type="checkbox"/> soap	Active		true
<input type="checkbox"/> soap_create	Active		true
<input type="checkbox"/> soap_delete	Active		true
<input type="checkbox"/> soap_ecc	Active		true
<input type="checkbox"/> soap_query	Active		true
<input type="checkbox"/> soap_script	Active		true
<input type="checkbox"/> soap_update	Active		true

MID Server Autofinder for Orchestration

Discovery

Orchestration

Related Topics

- Cloud Provisioning
- Help the Help Desk
- Help the Help Desk Login Script
- ECC Queue
- Useful Related Lists in CI Forms
- Creating a Workflow
- Using Workflow Activities

Get the Book



Discovery



Data Collected by Discovery



Orchestration for VMWare

Overview

MID Servers are associated with IP address ranges, enabling Orchestration to select the correct MID Server to use for an Orchestration activity based on the IP address of the target machine. This functionality ensures that a MID Server with proper privileges is available wherever Orchestration probes need to operate in a network. Autofinder also enables administrators to define specific **capabilities** for each MID Server within an IP address range.

Mapping IP Addresses to DNS Names

If the MID Server manages resources within defined IP ranges, all host servers must have their DNS names mapped to an IP address. This ensures that the appropriate MID Server is selected based on the IP Address range configuration. If this is not done, Orchestration reverts to the default MID Server. If Discovery cannot discover the server and resolve the DNS name to an IP address, you must perform this task manually.

1. Enter **cmdb_ci_dns_name.list** in the navigation filter.

A list of DNS names appears.

2. Check the list for your host server.

If it does not appear in the list, continue with this procedure to create the relationship between the DNS name and the IP address manually.

3. Click **New**.
4. Enter the fully-qualified domain name (FQDN) of the host server in the **Name** field.
5. Right-click in the form header and select **Save** from the context menu.
6. In the **IP Address** related list, click **New**.
7. In the **IP Address** field, enter the IP address of your host server.
8. In the **Nic** field, select **eth0** or your preferred network interface controller.
9. Leave the **Netmask** field blank.
10. Click **Submit**.

Configuring a MID Server for an IP Address Range

1. Navigate to **MID Server > IP Ranges**.

2. Click **New**.

3. Type a unique name for this MID Server Autofinder IP address range.

This name is for reference only and is not used in any processing.

4. Define the IP addresses for this range, using one or more of the following formats in a comma-delimited list.
 - IP Address Ranges
 - IP Networks
 - IP Address Lists

For additional details about these formats, see **Configuring IP Addresses**.

5. In the **Type** field, select whether to **Include** or **Exclude** these addresses.

← MID Server IP Range

Submit

Name:

SDSales

Range:

10.10.11.8/24,10.10.10.0-10.10.10.255,10.10.8.45,10.10.8.68

Type:

Include

Submit

6. Click **Submit**.
7. Reopen the form and click **Edit** in the **MID Servers** Related List.
8. Select one or more MID Servers to use for this IP address range.

← MID Server IP Range

UpdateDelete

Name:

SDSales

Range:

10.10.11.8/24,10.10.10.0-10.10.10.255,10.10.8.45,10.10.8.68

Type:

Include

UpdateDelete

MID Servers

NewEdit...

Go to MID Server

IP Range = SDSales

MID Server

Surfpilot-MID1

Actions on selected rows...

The IP address ranges defined here also appear in a Related List in the MID Server's record (*Orchestration > MIDServers*).

MID Server [Update] [Delete]

Name: Surfpilot-MID1

Status:

Version: 09-22-2010_1640

Last refreshed:

Started: 2010-11-11 08:36:46

Stopped:

Host name: swood1.service-now.com

IP address: 10.0.7.148

Router: 10.0.6.1

Network: 10.0.6.0/23

Host OS: Windows

Windows domain: SERVICE-NOW

[Update] [Delete]

Related Links

[Grab MID Logs](#)

[MID Stats](#)

[Refresh SNMP MIBs](#)

[Restart MID](#)

[Upgrade MID](#)

[Configuration help](#)

Configuration Parameters (9) **IP Ranges (1)** Capabilities (1) Logs (6) Threads (12) Properties

IP Ranges ▾ [New] [Edit...] Go to IP Range [] Q

▸ MID Server = Surfpilot-MID1

IP Range	Range	Type
<input type="checkbox"/> SDSales	10.10.11.8/24, 10.10.10.0-10.10.10.255, 10...	Include

Actions on selected rows... []

1 to 1 of 1

MID Server Capabilities

MID Server *capabilities* define the specific functions of a MID Server within an IP address range. At least one capability is required for each MID Server used by Orchestration. The base functionality enables an administrator to select specific capabilities for the probes launched by each MID Server. You can assign multiple MID Servers to the same IP address range and give them different capabilities, or assign a MID Server with specific capabilities to more than one IP address range. When Orchestration initiates a Workflow activity, Orchestration uses the IP address of the target machine to locate the MID Server assigned to that network segment that has the necessary capabilities to execute the activity.

The following capabilities are available for Orchestration:

- SSH
- SNMP
- VMware
- PowerShell
- WMI
- SOAP
- REST
- Resolve DNS

Values

Capabilities provided in the base system do not have a defined **Value** string. A MID Server configured to use a capability that has no **Value** can locate any device using that capability's protocol. If a capability has a defined value, the MID Server using that capability finds only those devices using that protocol that match the value string *exactly*. The exception to this is the **Resolve DNS** capability, which is configured to resolve any DNS name into an IP address using a partial string match.

Scripted Value Matching

A module called Capability Value Tests, enables administrators to create capabilities that find devices using values that do not require exact string matching. Action on these values is controlled by a user-defined script. The Resolve DNS capability is provided in the base system and is configured to resolve DNS names into IP addresses for devices whose names *end* with a specified domain name. The capability **Value** entered is automatically prefaced with a dot during processing to match domain syntax. This value can contain one or more sub-domains, but must include the end of the domain string. Matching devices must end with the identical syntax. The script for the Resolve DNS capability determines if a device name matches the criteria defined by **Value**. If a match exists, the platform performs the address resolution automatically. For example, if the value for the Resolve DNS capability is **service-now.com**, the MID Server with this capability finds *lnxlab01.sandiego.service-now.com* and *dbsrv101.sanjose.service-now.com*. If the value is changed to **sandiego.service-now.com**, then the MID Server finds only *lnxlab01*.



Note: If **Value** in the Resolve DNS capability is blank, then all domains match.

To view the script for evaluating this capability, navigate to *MID Server > Capability Value Tests* and select **Resolve DNS** from the list.

```

1 function(capability_value, requested_value) {
2   if (JSUtil.nil(capability_value)) {
3     return true;
4   }
5   var i = requested_value.lastIndexOf(capability_value);
6   if (i < 0) {
7     return false;
8   }
9   if (i == 0) {
10    return true;
11  }
12  if (requested_value.length != i + capability_value.length) {
13    return false;
14  }
15  return (requested_value.charAt(i - 1) == '.') && (i > 1);
16 }

```

At the bottom of the script area, there are 'Update' and 'Delete' buttons.

Configuring Capabilities

1. Navigate to **MID Server > Capabilities**.
2. Select an existing capability or click **New** to create one.

NOTE: At least one capability is required for each MID Server. Ensure that each IP address range has MID Servers with the necessary capabilities to complete the Orchestration activities on that network segment.

3. Configure the value for a custom capability.

An example is a capability for **DOMAIN**, with a value of **service-now**.

4. Click **Submit**.
5. Reopen the record and click **Edit** in the MID Servers Related List.
6. Select one or more MID Servers for this capability from the slushbucket.

MID Server Capability

Capability: DOMAIN

Value: service-now

Update Delete

MID Servers New Edit... Go to MID Server

Capability = DOMAIN

MID Server

Surfpilot

Actions on selected rows...

The capability defined here also appears in the primary record for this MID Server.

MID Server Update Delete

Name: Surfpilot Host name: sandb01.service-now.com

Status: Up IP address: 10.10.10.3

Version: 11-07-2010_2100 Router: 10.10.10.1

Last refreshed: 2010-11-15 14:14:18 Network: 10.10.10.0/23

Started: 2010-11-11 09:11:14 Host OS: Windows

Stopped: Windows domain: SERVICE-NOW

Update Delete

Related Links

[Grab MID Logs](#)

[MID Stats](#)

[Refresh SNMP MIBs](#)

[Restart MID](#)

[Upgrade MID](#)

[Configuration help](#)

Configuration Parameters (6) IP Ranges **Capabilities (1)** Logs (7) Threads (14) Properties

Capabilities New Edit... Go to Capability 1 to 1 of 1

MID Server = Surfpilot

Capability	Value
DOMAIN	service-now

Actions on selected rows...

1 to 1 of 1

MID Server Selection Criteria

If Orchestration finds multiple MID Servers in the target IP range with appropriate capabilities, it selects one of these at random. If no MID Servers are found with the necessary capabilities, Orchestration uses the MID Server defined in Orchestration MID Server properties. For this reason, it is very important to define a default MID Server in the properties that can fulfill this function.

To set the default Orchestration MID Server, navigate to **Orchestration > MID Server Properties** and type the name of the MID Server into the **Default MID Server to use for Orchestration Activities** property field.


MID Server

Default MID Server to use for Orchestration Activities

DevDoc1

With the Dublin release, the instance does not select a MID Server at random if no default is specified. The first MID Server to connect to the instance becomes the default MID Server.

You can set a MID Server as the default by clicking the **Set as default** related link on the MID Server form.

 MID Server

Name:	lsh30	Host name
Status:	Up	IP address
Version:	2013-10-08-2230	Router:
Last refreshed:	2013-10-09 16:34:07	Network:
Started:	2013-10-09 15:21:27	Host OS:
Stopped:	2013-10-09 10:18:38	Windows d

Update

Delete

Related Links

[Grab MID logs](#)

[Set as default](#)

[MID Statistics](#)

[Restart MID](#)

[Upgrade MID](#)

Article Sources and Contributors

MID Server Plugin *Source:* <http://wiki.servicenow.com/index.php?oldid=89866> *Contributors:* Aburruss, Bow, CapaJC, Cheryl.dolan, Christen.mitchell, Chuck.tomasi, Dan.sherwin, David Loo, David.Bailey, Dawn.bunting, Doogiesd, Fuji.publishing.user, G.yedwab, Guy.yedwab, Jeremiah.hall, John.andersen, John.ramos, John.roberts, Joseph.messerschmidt, Mark.odonnell, Neola, Phillip.salzman, Publishing.user, Rob.woodbyrne, Steven.wood, Tom.dilatush, Vaughn.romero, Vhearne

MID Server Requirements for Discovery *Source:* <http://wiki.servicenow.com/index.php?oldid=67960> *Contributors:* Bow, CapaJC, David Loo, Dawn.bunting, Doogiesd, Fuji.publishing.user, Gadi.yedwab, Guy.yedwab, John.ramos, Joseph.messerschmidt, Phillip.salzman, Rob.woodbyrne, Steven.wood, Valor, Vaughn.romero, Vhearne, Virginia.kelley

MID Server Installation *Source:* <http://wiki.servicenow.com/index.php?oldid=250732> *Contributors:* John.ramos, Joseph.messerschmidt, Katharine.sohler, Mary.stromberg, Phillip.salzman, Publishing.user, Rachel.sienko, Steven.wood, Vaughn.romero, Virginia.kelley

Deploying Multiple MID Servers *Source:* <http://wiki.servicenow.com/index.php?oldid=249565> *Contributors:* CapaJC, Chuck.tomasi, Joseph.messerschmidt, Peter.smith, Phillip.salzman, Steven.wood

MID Server Configuration *Source:* <http://wiki.servicenow.com/index.php?oldid=250729> *Contributors:* Aleck.lin, Bow, Cheryl.dolan, David.Bailey, Dawn.bunting, Emily.partridge, Fuji.publishing.user, Guy.yedwab, Jim.holthaus, John.ramos, Joseph.messerschmidt, Phillip.salzman, Publishing.user, Steven.wood, Tom.dilatush, Vaughn.romero, Vhearne, Virginia.kelley, Voytek.blonski

Controlling the MID Server Version *Source:* <http://wiki.servicenow.com/index.php?oldid=249563> *Contributors:* Dawn.bunting, Emily.partridge, Joseph.messerschmidt, Phillip.salzman, Rachel.sienko, Steven.wood

MID Server Heartbeat *Source:* <http://wiki.servicenow.com/index.php?oldid=250730> *Contributors:* John.ramos, Joseph.messerschmidt, Phillip.salzman, Steven.wood, Tom.dilatush

MID Server User Security *Source:* <http://wiki.servicenow.com/index.php?oldid=249566> *Contributors:* Cheryl.dolan, Joseph.messerschmidt, Neola, Phillip.salzman, Steven.wood

MID Server Autofinder for Orchestration *Source:* <http://wiki.servicenow.com/index.php?oldid=248932> *Contributors:* Joseph.messerschmidt, Steven.wood

Image Sources, Licenses and Contributors

Image:Warning.gif *Source:* <http://wiki.servicenow.com/index.php?title=File:Warning.gif> *License:* unknown *Contributors:* CapaJC

Image:JAR_File_Sync.png *Source:* http://wiki.servicenow.com/index.php?title=File:JAR_File_Sync.png *License:* unknown *Contributors:* Steven.wood

Image:mid server menu.png *Source:* http://wiki.servicenow.com/index.php?title=File:Mid_server_menu.png *License:* unknown *Contributors:* Vaughn.romero

Image:MID_Server_Download_Dublin.png *Source:* http://wiki.servicenow.com/index.php?title=File:MID_Server_Download_Dublin.png *License:* unknown *Contributors:* Vaughn.romero

Image:Caution-diamond.png *Source:* <http://wiki.servicenow.com/index.php?title=File:Caution-diamond.png> *License:* unknown *Contributors:* John.roberts, Publishing.user

Image:MID config.png *Source:* http://wiki.servicenow.com/index.php?title=File:MID_config.png *License:* unknown *Contributors:* Steven.wood, Tom.dilatush

Image:MID config xml.png *Source:* http://wiki.servicenow.com/index.php?title=File:MID_config_xml.png *License:* unknown *Contributors:* Tom.dilatush

Image:MID_Server_Script_File_Sync.png *Source:* http://wiki.servicenow.com/index.php?title=File:MID_Server_Script_File_Sync.png *License:* unknown *Contributors:* Steven.wood

Image:MID_Server_Script_File_Sync2.png *Source:* http://wiki.servicenow.com/index.php?title=File:MID_Server_Script_File_Sync2.png *License:* unknown *Contributors:* Steven.wood

Image:MID_Server_Unblock_Config.png *Source:* http://wiki.servicenow.com/index.php?title=File:MID_Server_Unblock_Config.png *License:* unknown *Contributors:* Steven.wood

Image:MID_Server_Monitor_Interval.png *Source:* http://wiki.servicenow.com/index.php?title=File:MID_Server_Monitor_Interval.png *License:* unknown *Contributors:* Steven.wood

Image:MID_Server_Roles.png *Source:* http://wiki.servicenow.com/index.php?title=File:MID_Server_Roles.png *License:* unknown *Contributors:* Steven.wood

Image:Knowledge.gif *Source:* <http://wiki.servicenow.com/index.php?title=File:Knowledge.gif> *License:* unknown *Contributors:* G.yedwab, Joseph.messerschmidt, Publishing.user

Image:MID_Server_IP_Range1.png *Source:* http://wiki.servicenow.com/index.php?title=File:MID_Server_IP_Range1.png *License:* unknown *Contributors:* Steven.wood

Image:MID_Server_IP_Range2.png *Source:* http://wiki.servicenow.com/index.php?title=File:MID_Server_IP_Range2.png *License:* unknown *Contributors:* Steven.wood

Image:MID_Server_IP_Range3.png *Source:* http://wiki.servicenow.com/index.php?title=File:MID_Server_IP_Range3.png *License:* unknown *Contributors:* Steven.wood

Image:MID_Server_Resolve_DNS.png *Source:* http://wiki.servicenow.com/index.php?title=File:MID_Server_Resolve_DNS.png *License:* unknown *Contributors:* Steven.wood

Image:MID_Server_Capability2.png *Source:* http://wiki.servicenow.com/index.php?title=File:MID_Server_Capability2.png *License:* unknown *Contributors:* Steven.wood

Image:MID_Server_Capability3.png *Source:* http://wiki.servicenow.com/index.php?title=File:MID_Server_Capability3.png *License:* unknown *Contributors:* Steven.wood

Image:RBA_MID_Server_Property.png *Source:* http://wiki.servicenow.com/index.php?title=File:RBA_MID_Server_Property.png *License:* unknown *Contributors:* Joseph.messerschmidt, Steven.wood

Image:MID_SetDefault.png *Source:* http://wiki.servicenow.com/index.php?title=File:MID_SetDefault.png *License:* unknown *Contributors:* Joseph.messerschmidt