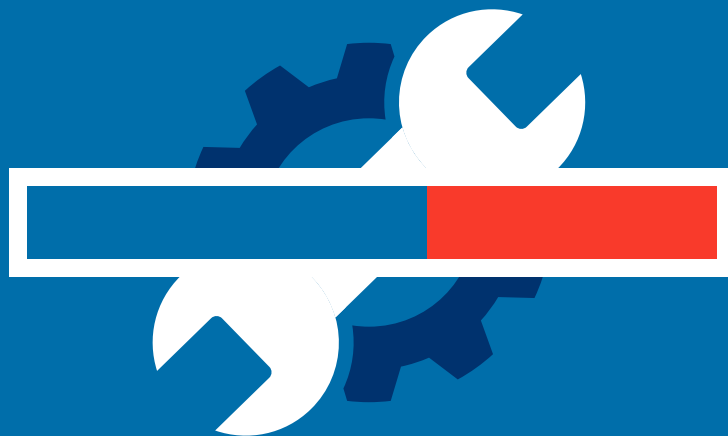




Anti-Virus for SAP Solutions

v 3.1

Installation and Configuration Guide



Anti-Virus for SAP solutions

Installation and Configuration Guide

Table of contents

bowbridge Anti-Virus for SAP solutions	3	Logging content scan activity	27
Product Overview	3	Implementing Content Scanning in the Java Environment	28
Content filter overview	4	Defining a Scanner Group.....	28
Installation on UNIX/Linux	5	Defining a Virus Scan Provider (Adapter)	30
Content filter overview	6	Defining Virus Scan Profiles	32
Installation on Microsoft Windows Server	7	Advanced Content Scanning - Java Configuration	34
Silent and unattended installation	9	File extension blacklist	34
SAP-side configuration	10	File extension whitelist	35
Understanding the SAP NetWeaver Virus Scan Service	10	MIME-type blacklist	36
Configuring Content Scanning in an ABAP environment	11	MIME-type whitelist	37
- Defining Scanner Groups	11	Content validation.....	38
- Defining Virus Scan Providers	14	Blocking active content	39
- Defining Virus Scan Profiles.....	17	Logging Scan Activity	40
Advanced Content Scanning - ABAP	21	Configuring ICAP-based virus scanning	41
File extension blacklist	21	Configuring ClamAV-based virus scanning	43
File extension whitelist	22	Preloading configuration parameters from configuration files	44
MIME-type blacklist	23	Controlling automatic updates	45
MIME-type whitelist	24	Integration with McAfee ePO	46
Content validation	25	Integration with OS-level anti-virus updates	49
Blocking active content	26	McAfee Virus Scan Enterprise (Windows)	49
		McAfee Endpoint Security (Linux)	49
		Parameter reference	51



Anti-Virus for SAP solutions

Installation and Configuration Guide

Product Overview

bowbridge Anti-Virus is an integrated content security solution for SAP®-based applications. NetWeaver application servers. The product secures file transfers from or into SAP applications, leveraging advanced content filters and built-in or external virus scan products from leading vendors.

bowbridge Anti-Virus utilizes SAP's NetWeaver Virus Scan Interface (NW-VSI) to seamlessly and easily enable content scanning.

In addition to virus scanning, bowbridge Anti-Virus supports filtering by file extensions and true content-based MIME-type filters. It further detects and blocks various types of active content and malformed or maliciously embedded files.

bowbridge Anti-Virus offers flexibility and choice when it comes to virus scanning by integrating two industry leading virus scan engines from McAfee and SOPHOS and by providing an industry-standard ICAP-interface, permitting the use of external virus scanners from virtually any security vendor offering and ICAP interface. Lastly, the integration with opensource virus scanner ClamAV allows for cost-effective integration of content scanning functionality.

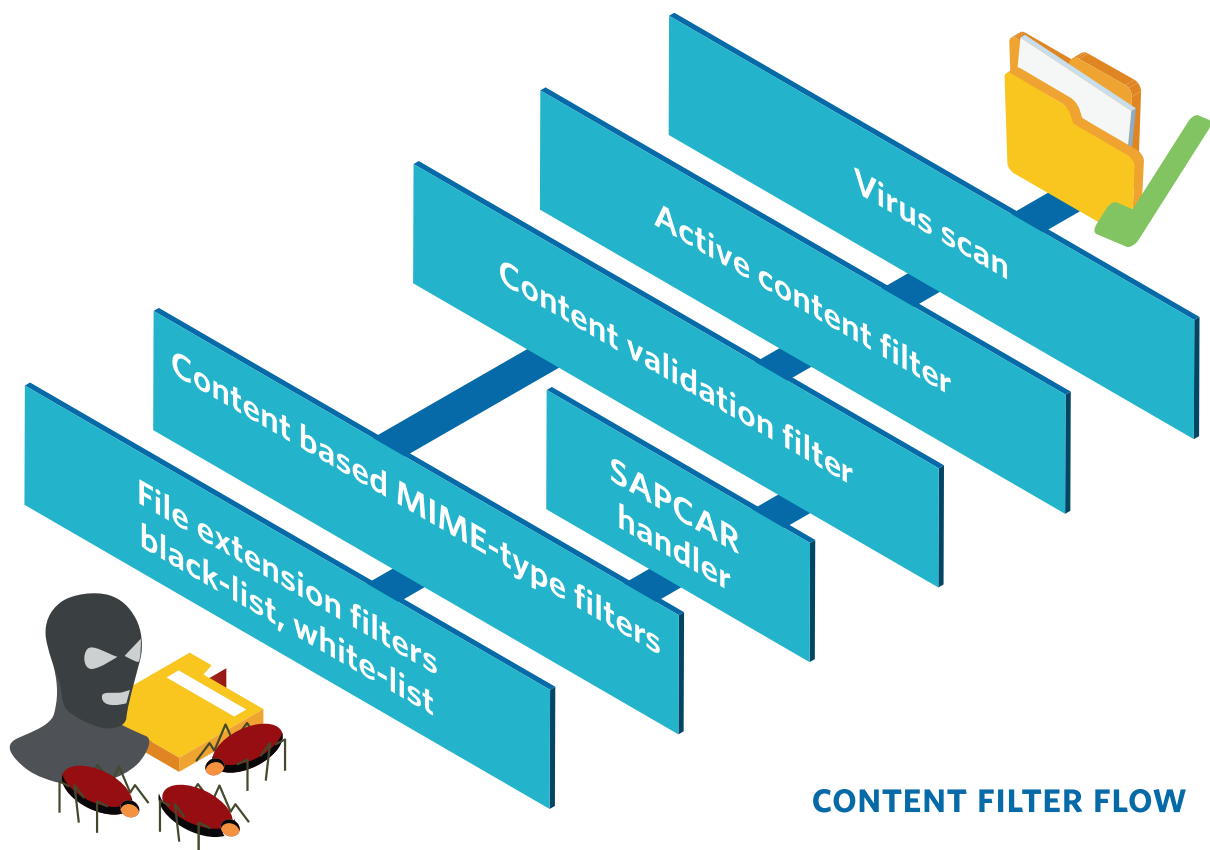
bowbridge Anti-Virus integrates seamlessly into the SAP management infrastructure. For standard operation, it does not require any operating system level configuration, but is fully customizable from within the SAP management and customization infrastructure.

Anti-Virus for SAP solutions

Installation and Configuration Guide

Content filter overview

Each object passed to Anti-Virus is examined through a series of content filters, controlled by parameters set either at the SAP-system level or in individual application content scanning policies.



Anti-Virus for SAP solutions

Installation and Configuration Guide

Installation on UNIX/Linux

The installation process is virtually identical on all UNIX/Linux platforms, however the screen output on your machine may differ slightly from the screen-shots provided in this documentation.

bowbridge Anti-Virus for SAP solutions for UNIX/Linux is delivered as a gzip-compressed installation shell-script which self-extracts the binaries to be installed. Please copy the file to a location where the current user has write privileges. Extract the file with:

```
gunzip ./install-bowbridge-[version]_[build]_[platform].sh.gz
```

Executing the resulting installer script with

```
./install-bowbridge-[version]_[build]_[platform].sh
```

will start the installation process:



The installer is a menu-driven, interactive application guiding you through the installation process during which you will be required to provide the following information:

- ⤴ Agree to the bowbridge Software End User License Agreement
- ⤴ the SIDadm user ID (when installing as root)
- ⤴ the installation target directory
- ⤴ Activation/choice of services to run
- ⤴ a license to be installed (optional)

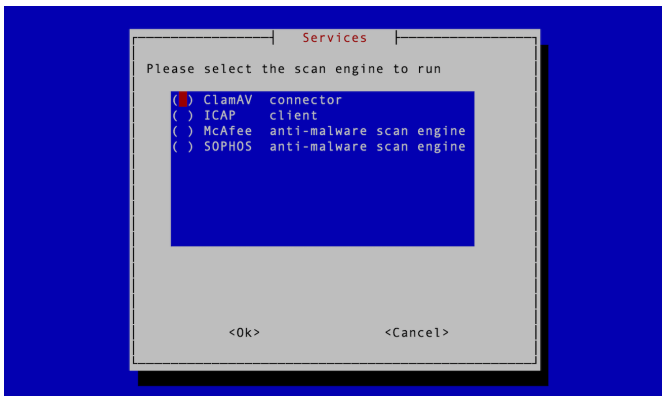
Service Mode:

Starting with version 3.1.13 "Service Mode", in which the virus scan engine and other supporting processes are no longer controlled by the starting and stopping of virus scan providers in the SAP processes but are started and monitored by the operating system's system daemon (**systemd**) is recommended.

Service Mode streamlines internal synchronization and locking and results in improved stability, better performance and much faster initialization and re-initialization times. On older Linux releases, controlling services with **initd** instead of **systemd** is possible. Please contact bowbridge technical support for assistance with that, if required.

Installation/Activation:

In order to install and benefit from Service Mode, the installation must be performed with root privileges. In interactive mode, the installer prompts the admin for the activation of Service Mode (see page 9 for silent installation options). After completing the initial installation/upgrade, the admin is prompted for the service to start:



The installer registers the systemd service unit, starts the selected service and enables it for automatic startup at system boot time.

Controlling bowbridge services in Service-Mode

bowbridge services may be controlled using the regular **systemctl** suite of commands:
systemctl start/stop/restart/enable/disable/status <servicename>

The registered service names are **bowbridge-clamav.service**, **bowbridge-icap.service**, **bowbridge-mcafee.service** and **bowbridge-sophos.service**.

Because the service run before the SAP processes start, initialization parameters INITDIRECTORY, INITENGINES, and, when needed, INITSERVERS and INITTEMP_PATH must be configured in the bbvsa31.cfg configuration file.

Anti-Virus for SAP solutions

Installation and Configuration Guide

Interactive Installation on Windows Server

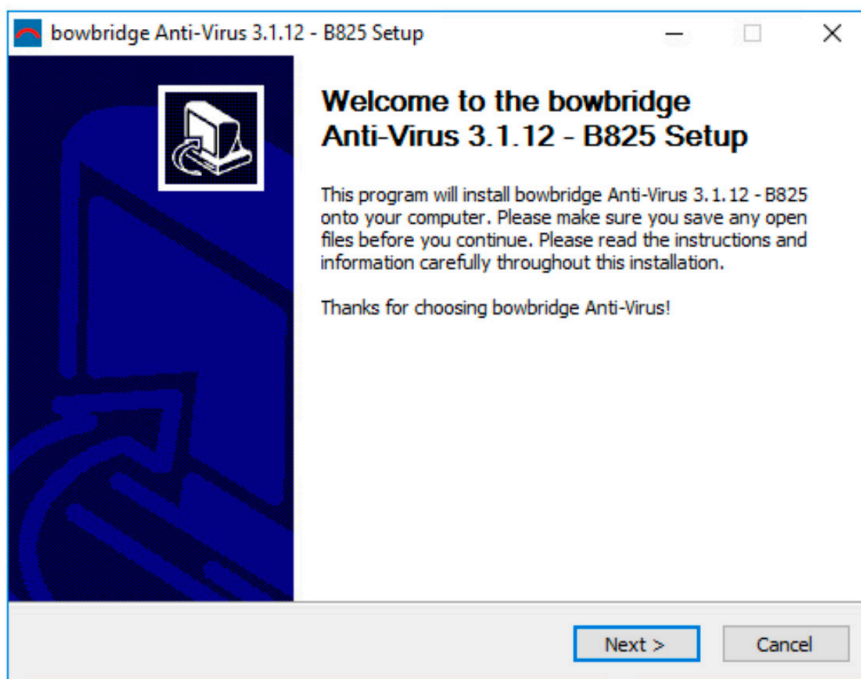
The Windows version of bowbridge Anti-Virus comes as a single file installer.

Local Administrator privileges are required to perform the installation.

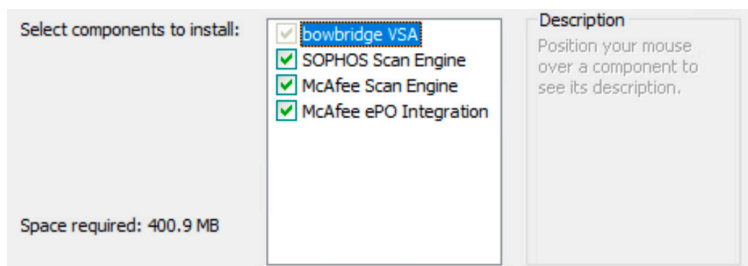
Please download and execute the file

`install_bowbridge[version_[build_]Windows86_64.exe`

and follow the instructions of the installer.

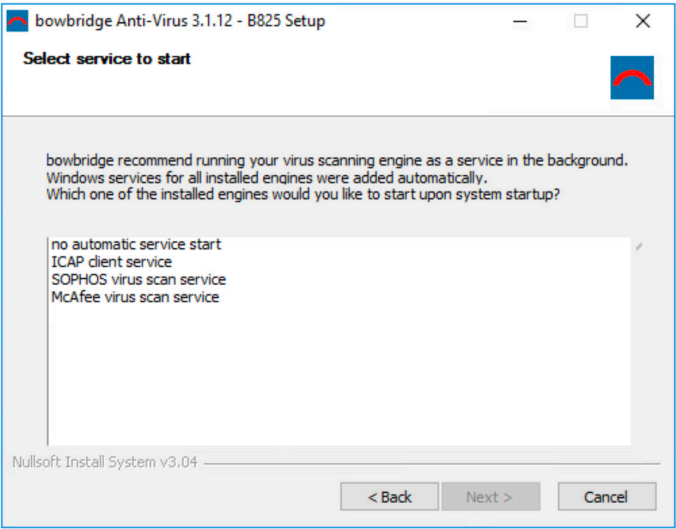


During the installation process, you may deselect components that are not needed in your environment, i.e. one or both of the embedded scan engines, should you not require them.



Providing a license during the installation process is optional, as licenses may be added or replaced at any time after the installation.

After specifying the parameters, the installer copies the product to the installation path provided in the installer.






After the installation of files is complete, please select the virus scan service you would like to start automatically as a Windows service.

When choosing the ICAP Service you will be prompted for the ICAP URL.

When upgrading from earlier versions of the product, selecting "no automatic service start" will replicate the previous experience.

Switching virus scan services or startup modes can be performed at a later time in the Windows Services Management console, where you can change the Startup Type for each of the bowbridge Anti-Virus Services.

Name	Description	Status	Startup Type
 bowbridge Anti-Virus for SAP Solutions - ICAP			Manual
 bowbridge Anti-Virus for SAP Solutions - McAfee			Manual
 bowbridge Anti-Virus for SAP Solutions - SOPHOS		Running	Automatic

Anti-Virus for SAP solutions

Installation and Configuration Guide

Silent/Unattended Installation

For automated or unattended rollout, bowbridge Anti-Virus may be installed without user/administrator interaction.

If an installation already exists in the target directory, an upgrade will be performed. Binaries will be updated but configuration files will not be changed or added.

Note: The VSA must be stopped for the upgrade to succeed. If you are upgrading from a version older than 3.1.12 and want to use the new service-mode, manual configurations must be performed post-install. Please contact bowbridge technical support.

On Windows Server:

```
install_bowbridge[version_[build_]Windows86_64.exe /S /LICENSE=<path  
to license file> /D=<non-standard installation directory>
```

In Silent-Mode the /D parameter MUST be the last parameter of the command line. The installation directory value MUST NOT contain any quotations.

Example:

```
install_bowbridge_3.1.12_B824_Windows86_64.exe /S /LICENSE="C:\Users\  
bbradm\Desktop\bowbridge-license.lic /D=C:\Program Files\bowbridge3x
```

On Linux/UNIX:

Extract the installer-script from the tar.gz file as described on page 5.
run the installer script with the following command-line options:

as SIDadm

```
--silent --targetdir=<installation directory> --licensefile=<path to the license file>  
[ --enable-<servicename>-service --tempdir=<Temp directory> --initservers=<ICAP  
URL> ]
```

as root

```
--silent --targetdir=<installation directory> --licensefile=<path to the license file>  
--user=<SIDadm user> --group=<SAP-System group> [--enable-<servicename>-ser-  
vice --tempdir=<Temp directory> --initservers=<ICAP URL> ]
```

Example:

```
./install-bowbridge-318_435_Linux_x86-64.sh --silent --targetdir=/usr/  
sap/BBR/bowbridge --licensefile=/home/bbradm/Bowbridge-License.lic  
--user=bbradm --group=sapsys
```

Anti-Virus for SAP solutions

Installation and Configuration Guide

SAP-side configuration

For details on how to configure your SAP landscape to enable Virus Protection for your application, bowbridge recommends referring to the latest SAP documentation for your product and version.

Understanding the SAP NetWeaver Virus Scan Service

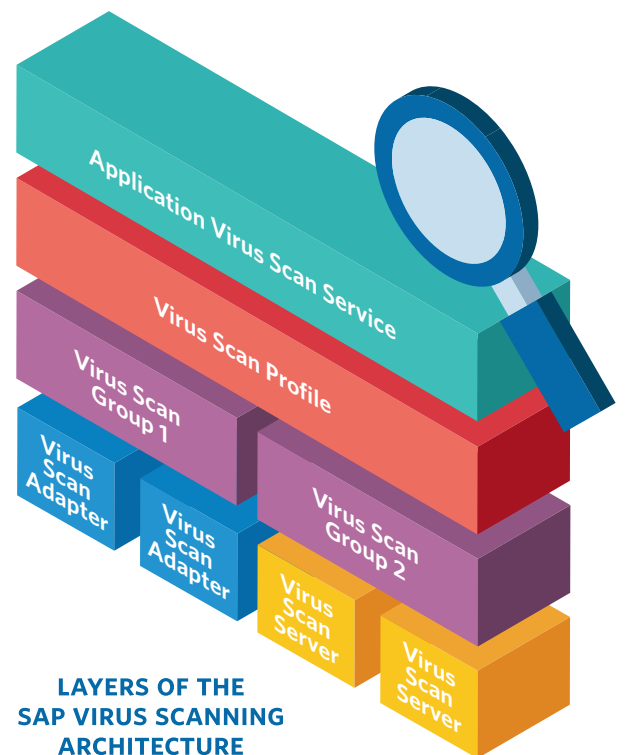
NetWeaver's Virus Scan Service introduces three abstraction layers:

1 Virus Scan Provider: describes the access to a virus scanner

- **Virus Scan Adapter:** allows direct access to a virus scanner. The adapter is loaded as a dynamic library (DLL or lib) and is executed within the address space of the the J2EE or ABAP engine and is therefore the variant offering the highest performance.
- **Virus Scan Server:** defines a (logical or physical) server which gets scan-objects via RPC. This variant has a much lower performance and might fail when scanning large files.

2 Virus Scan Group: A Virus Scan Group may cover several Virus Scan Providers.

3 Virus Scan Profile: allows to consolidate multiple Virus Scan Groups and combine them using logical AND/OR relationships. Thus it is possible to create high-security deployments in which scan objects need to be checked by multiple servers. Also Virus Scan Profiles may be created to allow application-specific scanning configurations.



Configuring Content Scanning in an ABAP Environment

bowbridge Anti-Virus basic configuration is performed entirely from the SAP customization tools. Very few additional options, such as activating debug tracing and alternative update sources or granular deactivation of active-content types can be configured via configuration files, either at the host-level or the application server instance level.

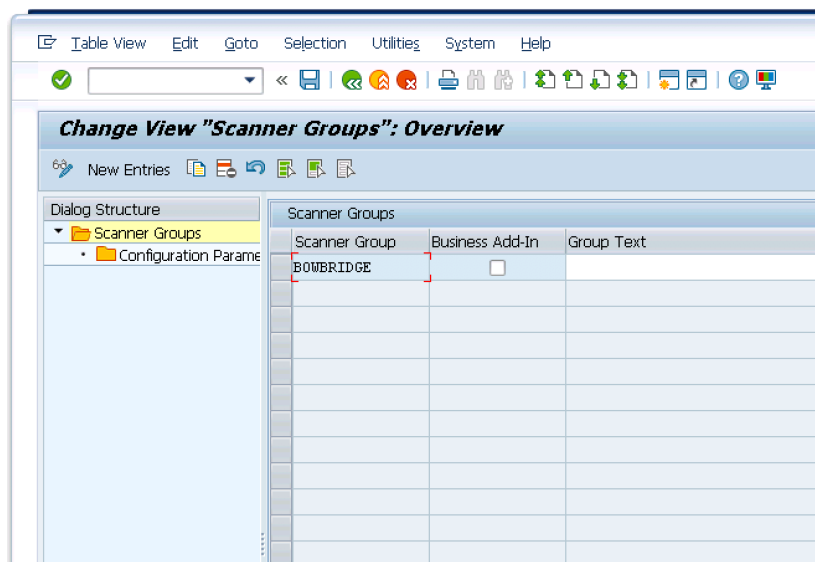
Setting up virus protection for ABAP based SAP applications requires three major steps:

1. Definition of Virus Scan Groups
2. Definition of Virus Scan Providers
3. Definition and activation of virus scan profiles

Defining Scanner Groups

A scanner group combines multiple virus scanners of the same type. Since you select the Virus Scan Provider using the scanner group when maintaining the virus scan profile, you must assign each Virus Scan Provider to a scanner group.

We recommend setting up multiple scanner groups if you want to maintain multiple scan configurations on your system.



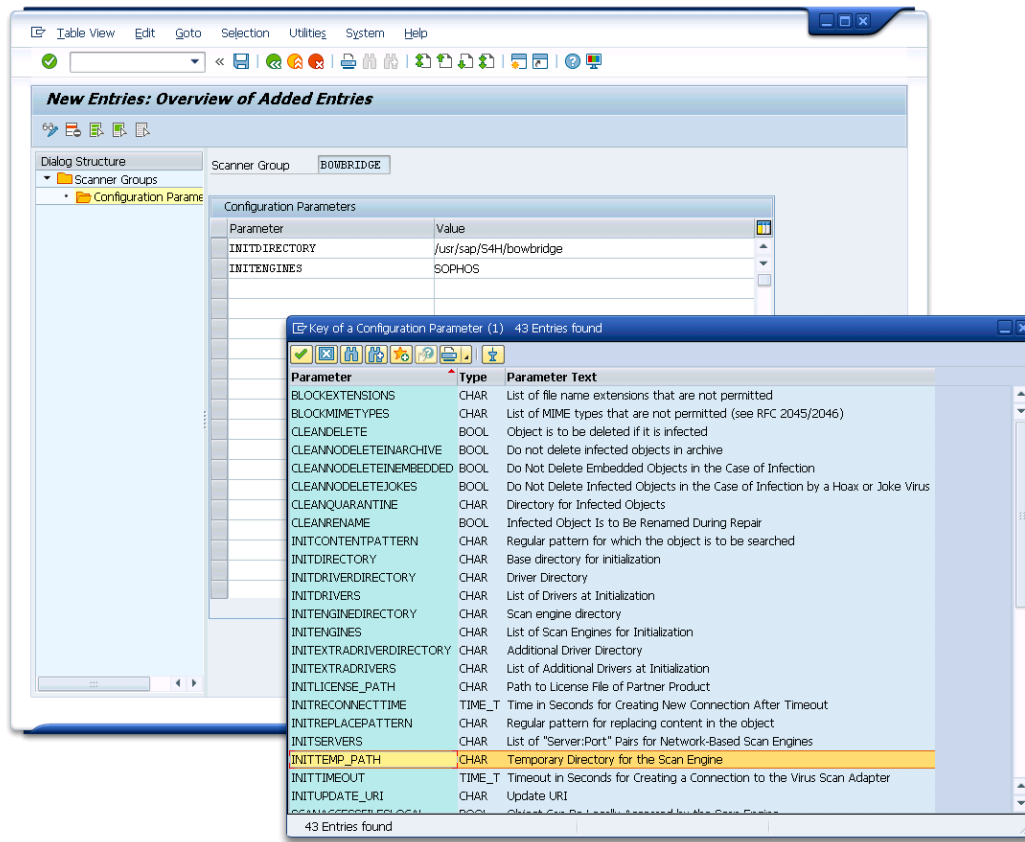


Configuration Steps:

1. Open transaction VSCANGROUP
2. Switch to Change mode and select "New Entries"
3. Specify name and description for the scanner group

FIELD	NOTES
Scanner Group	freely definable name for the group (i.e. BOWBRIDGE)
Group Text	Description of the group

4. Select the group you just created and double-click "Configuration Parameters" in the Dialog structure pane.
Please configure the initialization parameters reflecting your desired configuration.





FIELD	REQUIRED	NOTES
INITDIRECTORY	Yes	Path to the bowbride installation folder
INITENGINES	Yes	Virus scanning engine to start. Choose from: <ul style="list-style-type: none">- SOPHOS (embedded, default)- MCAFEE (embedded)- ICAP (requires INITSERVERS)- CLAMAV (requires INITSERVERS)
INITSERVERS	for ICAP and CLAMAV	Specifies the ICAP service URL(s) or ClamAV Socket or TCP destination Consult section " <i>Configuring ICAP Backends</i> " and " <i>Integrating ClamAV</i> " for details.
INITTEMP_PATH	No	Specifies the temp directory used by Anti-Virus to store synchronization files and repack SAPCAR archives
INITTIMEOUT	No	Specifies the maximum time for the virus scan engines to start

5. Complete the configuration by saving your settings. You will be prompted to create or assign a customization request to transport the changes.



Defining Virus Scan Providers

NetWeaver supports two types of Virus Scan Providers: *Virus Scan Adapters* and *Virus Scan Servers*.

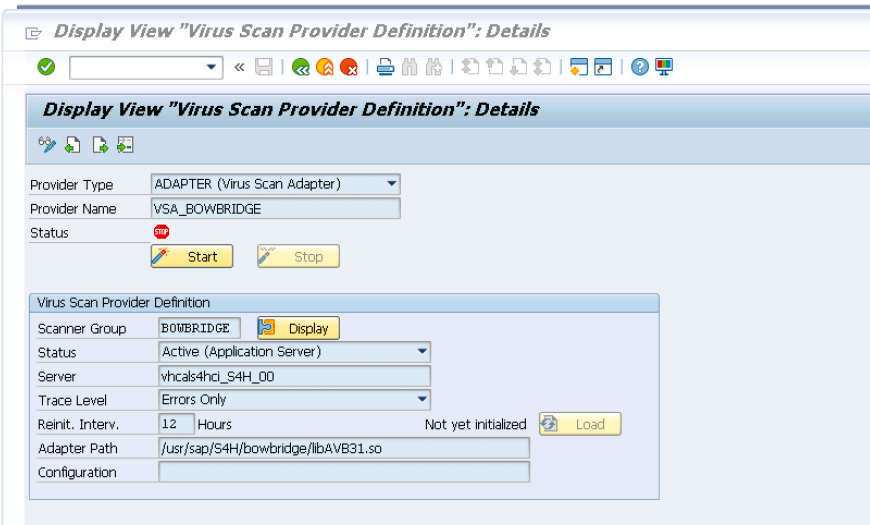
While both options are fully supported with Anti-Virus, bowbridge and SAP both recommend using the Virus Scan Adapter configuration as it is more stable and delivers much better performance and overcomes other limitations of the Virus Scan Server deployment mode.

Those limitations of the Virus Scan Server deployment model are detailed in SAP note 782963.

If you still need to deploy bowbridge Anti-Virus in the Virus Scan Server model, please contact bowbridge technical support for additional documentation on how to implement that configuration.

Configuration Steps:

- 1. Open transaction VSCAN
- 2. Switch to Change mode and add a new entry



Enter the information relevant to your installation based on the table below:



FIELD	VALUE	NOTES
Provider Type	ADAPTER	Deployment as "Virus Scan Adapter" for maximum stability and performance.
Provider Name	VSA_<name> default: VSA_<hostname>	Provide a sensible, unique name for the virus scan provider. The prefix "VSA_" must be retained. The name must be unique per landscape.
Scanner Group	Select the new Virus Scanner Group from the pull-down options.	Ties the initialization parameters defined in the virus scanner group (i.e. which virus scan engine to start) to this virus scan provider
Status	Active	The Virus Scan Provider is started along with the work processes.
Server	<hostname>	If the system has multiple application servers (AS), this setting specifies on which AS this VSA should be started.
Relnit interval	8-12	Interval in hours after which the Virus Scan Adapter is to be re-initialized automatically
Adapter Path	fully qualified path to the VSA shared library on the server specified in the "Server" setting.	Filename of the shared library is: - libAVB31.so on UNIX/Linux - BBVSA3-1.DLL on Windows

3. Save the entries. Specify a customizing request, if prompted to do so.
4. Activate the Virus Scan Provider by clicking the "Start" button
bowbridge Anti-Virus will now be started with the settings specified during the previous configuration steps.
Once started, the "Adapter Details" and "Engine Details" will provide additional information:



Virus Scan Provider Details - meanings

After starting up, details of the Virus Scan Provider are displayed in transaction VSCAN.
They have the meanings layed out below:

Engine Data

Version	<i>Version of the virus scan engine and/or main virus data</i>
Version Text	<i>Version name returned by the scan engine</i>
Date	<i>Date and time of the last update/virus data</i>
Know Viruses	<i>Number of unique viruses detectable by this engine</i>

Adapter Data

Version	Driver Name	Date	Known Viruses
<i>bowbridge Anti-Virus version</i>	<i>"bowbridge VSA", <License ID>, <License expiration date></i>	<i>VSA build date</i>	<i>number of unique viruses detectable by this engine (if reported)</i>

Adapter Data

Manufacturer	<i>bowbridge Software GmbH</i>
Product Name	<i>Anti-Virus for SAP-solutions, <version/build number></i>
Version	<i>Product major release version.</i>



Defining Virus Scan Profiles

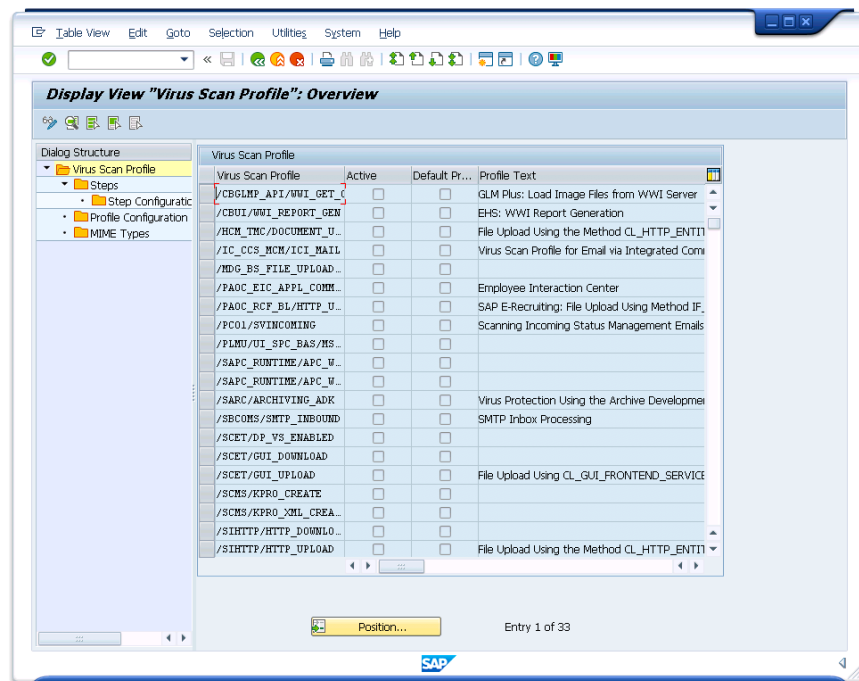
Applications use virus scan profiles to run content checks. Virus scan profiles hold the application specific content security parameters to be passed to bowbridge Anti-Virus in order to perform the proper scan operation.

A virus scan profile specifies steps that are to be run during a content scan. A step is either a virus scanner, which is found using the scanner group, or a step specifies, in turn, a virus scan profile, which is then performed as part of the enclosing virus scan profile.

A virus scan is performed under the name of a virus scan profile. The system administrator can use the profile to activate or deactivate the virus scan for each component.

By default, each SAP application that integrates a virus scan provides a virus scan profile. The names of these virus scan profiles is constructed as follows /<Name of the package of the application>/<Name of the function>. Check the virus scan profiles delivered by SAP, and determine for which components you are activating or deactivating the virus scan.

Create your own virus scan profiles in the Y* and Z* namespaces.





Unlike Virus Scanner Groups and Virus Scan Providers, **the configuration of Virus Scan Profiles is not cross-client**. Virus Scan profiles must therefore be maintained in all active clients separately.

Before maintaining Virus Scan Profiles for your application, log-in to your actual application client.

Configuration Steps:

1. Open transaction VSCANPROFILE, and, if necessary, switch to change mode. The screen View: Change "Virus Scan Profile": Overview appears.
2. Choose New Entries.
3. Specify the data for the virus scan profile according to the table below

The screenshot shows a software interface titled "New Entries: Details of Added Entries". On the left is a "Dialog Structure" tree with nodes: "Virus Scan Profile" (selected), "Steps", "Step Configuration", "Profile Configuration", and "MIME Types". The main area contains a "Scan Profile" text field with the value "Z_BONBRIDGE". Below this is a "Virus Scan Profile" section with a "Profile Text" field containing "Virus Scan Profile to be referenced by all active profiles". There are three checkboxes: "Active" (checked), "Default Profile" (checked), and "Use Reference" (unchecked). There is also a checkbox for "Evaluate Profile Configuration Param." which is checked. At the bottom is a "Link" dropdown menu showing "All steps successful".

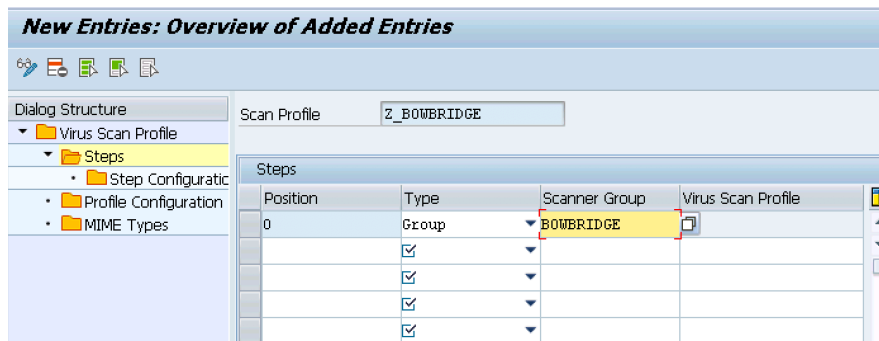
Before saving your profile, select the "Active" and "Default Profile" check-boxes and ensure the "Use Reference" checkbox unchecked. As all pre-defined virus scan profiles reference the default, all applications requesting their active virus scan profile will effectively use this new profile.



FIELD	VALUE	NOTES
Scan Profile	Z_<name>* or Y_<name>	Specifies the name of the virus scan profile
Profile text		Explanatory text for the virus scan profile
Active	on/off	Specifies that this virus scan profile is active. The virus scan profile can only be used if this indicator is set. SAP applications can use fixed profile names that are delivered. By default, these profiles are not active, meaning that the application program works without a virus scan. You can activate the virus scan for each application by setting this indicator.
Default Profile	on/off	Indicator that this virus scan profile is the default profile. You can set this indicator for a maximum of one virus scan profile. This virus scan profile is used in the following cases: - If an application requests a virus scanner without specifying a virus scan profile - If a virus scan profile is requested for which the Use Reference Profile indicator is set, and the Reference Profile is empty
Use Reference	on/off	The Virus Scan Provider is started along with the work processes.
Reference Profile	The input help provides a list of all of the profiles that have already been defined. If you leave the field empty, the system uses the default profile.	Specifies the name of the reference profile. Since a virus scan profile can use another virus scan profile as a reference profile, you can operate multiple applications using the same virus scan profile. If the Use Reference Profile indicator is set in the virus scan profile, this field specifies the name of the reference profile to be used. Instead of the settings of the current virus scan profile, the settings of the reference profile are then used. This means that several virus scan profiles can use the settings of a shared reference profile, such as the scanner groups to be used..
Relationship	- All steps successful: The virus scan must have performed all steps without errors. - At least one step successful: It is sufficient if one step of the virus scan was successfully performed.	Specifies the type of logical linkage for the steps in the virus scan profile. If multiple steps that are to be performed during the virus scan with a virus scan profile are defined for a profile, you can use this field to control how the overall result of the virus scan is to be evaluated. Using multiple steps allows you to scan documents with scan engines from different vendors at the same time. The program interprets a virus scan as error-free only if the scan engine returns the return value Check performed successfully or (in the case of cleanups) Cleanup performed successfully. All other return values are regarded as unsuccessful virus scans. This also includes situations such as: - The program did not check the document because the file name extension is categorized as non-critical. - The program could not check the document, because the document is a password-protected archive. - The scan engine is obsolete.



4. Double-click on "Steps" and add a reference to the new Virus Scanner Group as a new entry at position 0 in the list:



FIELD	VALUE	NOTES
Position	<integer value>	Specifies the position of the scanner group in the virus scan profile. If a virus scan profile uses multiple scanner groups, place these in the desired sequence by assigning a position number.
Type	"Group" or "Profile"	Specifies whether a step in the virus scan profile refers to a scanner group or another virus scan profile. If you choose Group, the system uses a Virus Scan Server from this group (or a BAdI implementation) for the virus scan. If you choose Profile, the program processes the specified virus scan profile instead of this step. You can define any conditions by combining the steps of the virus scan profile with the linkage type of the steps (AND/OR).
Group	The input help provides a list of all existing scanner groups.	Combines multiple Virus Scan Servers. All of the Virus Scan Servers of a scanner group have the same set of configuration parameters and will therefore use the same scan engine.
Profile	The input help provides a list of all existing profiles.	Specifies the name of a virus scan profile that you can include as a step in the profile that you are currently processing.

5. Save the entries

This completes the basic virus scanning configuration in the ABAP stack.

Advanced Content Scanning - ABAP configuration

As a VSI 2.0-certified solution, bowbridge Anti-Virus offers further content scanning capabilities beyond the scanning for malware. Content can be filtered based on its MIME-type, the file extension, the combination of content and extension and based on active content included in the files. While none of those criteria qualify as malware by definition, they still pose a relevant threat to your SAP application and users.

Advanced content filters are configured via Virus Scan Profiles as follows:

File Extension Blacklist:

The file extension blacklist may be used to block files with certain extensions prior to the virus scan.

Configuration Steps:

1. Open the virus scan profile for your application (or the one it references) and open the "Step Configuration Parameters" of the Step linked to your virus scan group.
2. Add "BLOCKEXTENSIONS" as a new entry.
3. Specify the extensions you want to block as a semicolon-separated list:

Example: ".exe; .com; .dll"

New Entries: Overview of Added Entries

Dialog Structure

- Virus Scan Profile
 - Steps
 - Step Configuration Parameters
 - Profile Configuration
 - MIME Types

Scan Profile: Z_BOWBRIDGE

Position: 0

Parameter	Value
BLOCKEXTENSIONS	.exe; .com; .dll

4. Save the entries

File Extension Whitelist:

The file extension whitelist may be used to allow only files with certain extensions to continue to be processed and scanned. All other files will be blocked.

Configuration Steps:

1. Open the virus scan profile for your application (or the one it references) and open the "Step Configuration Parameters" of the Step linked to your virus scan group.
2. Add "SCANEXTENSIONS" as a new entry.
3. Specify the extensions you want to allow as a semicolon-separated list:
Example: ".doc; .pdf; .odt"

New Entries: Overview of Added Entries

Scan Profile: Z_BOWBRIDGE
Position: 0

Parameter	Value
SCANEXTENSIONS	.doc; .pdf; .odt

4. Save the entries

MIME-Type Filtering

bowbridge Anti-Virus allows for filtering of content based on their MIME-type. The MIME-type of any given file is determined by analysing the content of the file and therefore offers a more thorough protection than filtering based on the filename extension.

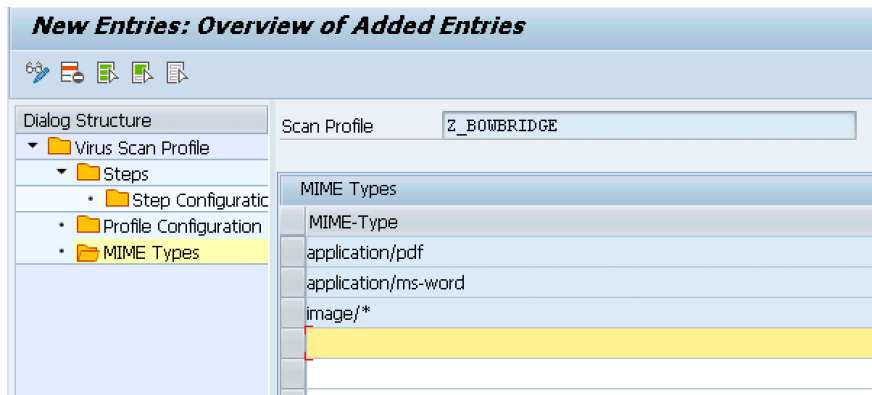
MIME filters may be implemented as Whitelist or Blacklist.

Setting up a MIME-type Whitelist

This is the default behaviour of the MIME filter.

Configuration Steps:

1. Open the MIME-Types- section of the Dialogue Structure:
2. Add entries for each MIME-type you wish to allow. Any file with a MIME-type not on the list of types provided will be rejected with the message "*MIME-Type not allowed*". Simple wildcards, such as "image/*" are supported.



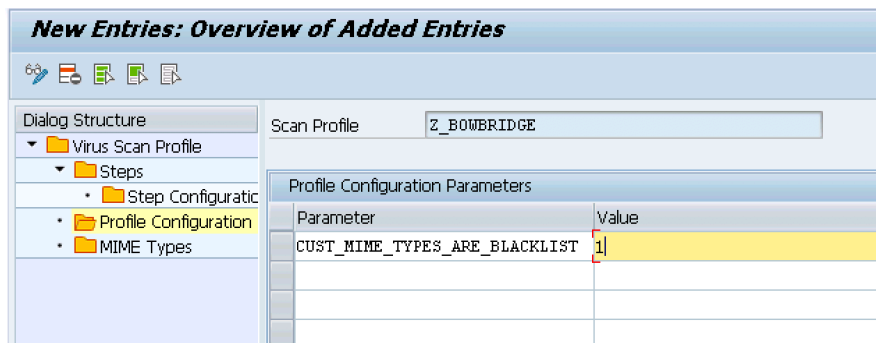
3. Save the entries

Setting up a MIME-type Blacklist

Inverting the MIME-type list

Configuration Steps:

1. Create a list of entries of MIME-types you want to block, analogous to creating a MIME-type Whitelist.
2. Open the "Profile Configuration Parameters" from the Dialogue Structure Pane
3. Add the Parameter CUST_MIME_TYPES_ARE_BLACKLIST and set the value to 1.
Files with MIME-types defined on the list of MIME-types will be blocked with the message "MIME-type forbidden".



4. Save the entries

Content Validation

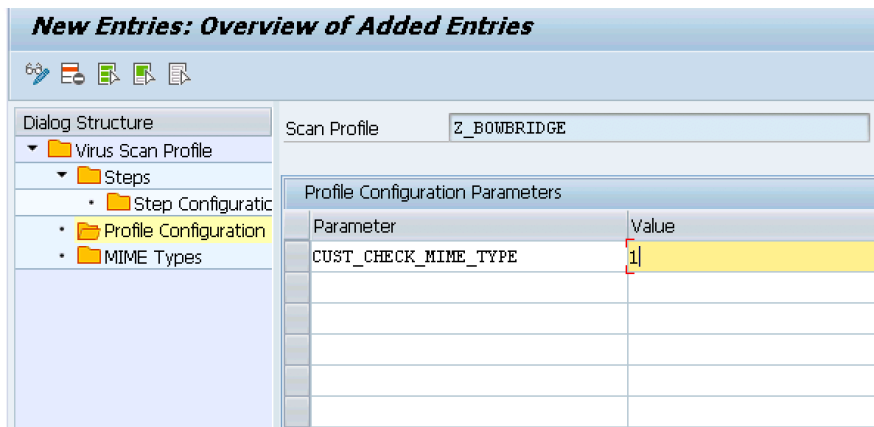
Attackers may try to circumvent security by assigning files a file extension that does not match its actual content. bowbridge Anti-Virus can analyze the content of any file and compare the file extension to legitimate extensions for that content type. Deviations are blocked.

Configuration Steps:

1. Open the "Profile Configuration Parameters" from the Dialogue Structure Pane
2. Add the Parameter CUST_CHECK_MIME and set the value to 1.

Files with extensions not matching the well-known extensions for the actual content of the file are blocked with the message *"MIME validation failed"*.

The mappings of extensions to MIME-types can be adjusted in the file mime_ext_map, located in your bowbridge installation directory. Re-initializing the Virus Scan Provider is required for the changes to the mime_ext_map file to go into effect.



3. Save the entries



Blocking Active Content

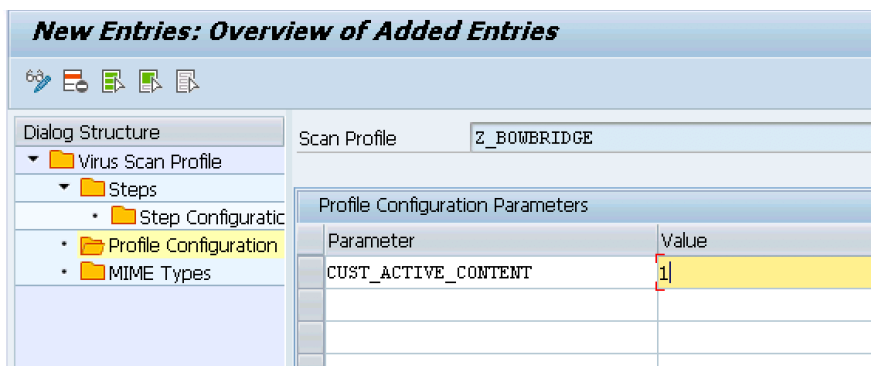
Attackers may try upload files with active elements into your application in order to compromise clients accessing these documents or in order to stage a Cross-Site Scripting (XSS) attack.

bowbridge Anti-Virus can detect and block files containing active content. It is equipped with filters detecting:

- JavaScript in HTML, XML and SVG
- Scripts and Macros in Office documents
- JavaScript, OpenAction and ActiveAction in PDF
- Silverlight
- Flash
- Java archives embedded in image files and Office documents.
- XSLT

Configuration Steps:

1. Open the virus scan profile for your application (or the one it references) and open the "Profile Configuration Parameters" of the Step linked to your virus scan group.
2. Add "CUST_ACTIVE_CONTENT" as a new entry.
3. Set the value to 1



Logging Scan Activity

bowbridge Anti-Virus supports a simple logging of all scan activities in a plain-text, human readable log file.

Logging of scans may be activated via a specific virus scan profile, or in the one referenced as the default profile.

Configuration Steps:

1. Open the Step Configuration Parameters for the relevant Step in the Virus Scan Profile dialogue
2. Add the parameter SCANLOGPATH and provide a fully qualified filename as the parameter value. Please ensure the scan log file must be in a location writeable for the <SID>adm user on UNIX or SAPService<SID>-user on Windows
3. Save the changes

Step Configuration Parameters	
Parameter	Value
SCANLOGPATH	/home/S4Hadm/logs/SAP-scans.log



Configuring Content Scanning in a Java Environment

The Virus Scan Provider is the service of the J2EE Engine that makes the tc/sec/vsi/ interface interface available to the SAP applications of the Engine.

The implementation involves three steps:

1. Defining a Scanner Group
2. Defining a Virus Scan Provider
3. Defining and activating a Virus Scan Profile.

Depending on the release of your NetWeaver Application Server, the configuration steps below need to be performed in NetWeaver Administrator. In older releases, analogous configurations need to be performed in the Visual Administrator.

Defining a Virus Scanner Group

Virus Scan Providers with identical configuration are grouped together in a Virus Scanner Group. However, even with only one Virus Scan Provider, a Scanner Group containing just this one element must be created.

Configuration Steps:

1. Log-in to NetWeaver Administrator, access the Configuration tab and select "Virus Scan Provider"

The screenshot displays the SAP NetWeaver Administrator web interface. At the top, the title bar shows 'SAP NetWeaver Administrator' with navigation links like 'Personalize', 'Back Forward', 'History', 'Site Map', 'Help', and 'Log Off'. Below this, a status bar indicates the user is 'Administrator', the active profile is 'Complete List', the system is 'J2E On vhaa[2ed], v7.50', and the system time is '10/17/2016 09:23 AM UTC'. A search bar is also present. The main navigation pane on the left includes 'My Workspace', 'Availability and Performance', 'Operations', 'Configuration' (which is selected), 'Troubleshooting', and 'SOA'. Under the 'Configuration' tab, there are sub-tabs for 'Security', 'Infrastructure', 'Scenarios', and 'Connectivity'. The 'Security' sub-tab is active, showing a list of security-related services. The 'Virus Scan Provider' service is highlighted, with a description: 'You can use the virus scan interface to include external virus scanners in the SAP system to increase the security of your system. This means that you can use a high-performance integration solution to scan files or documents that are processed by applications for viruses. This applies both for applications delivered by SAP and for customer developments, for example, during data transfers across networks or when documents are exchanged using interfaces.' Below this description, there is a link to 'ClickJacking Whitelist Configuration'.

2. From the Virus Scan Provider Overview, select the "Groups" tab and switch to Edit-Mode to add a new Group.

The screenshot shows the 'Virus Scan Provider: Virus Scan Provider' interface. At the top, there are tabs for 'Overview', 'Groups' (selected), 'Adapters', 'Servers', and 'Profiles'. Below the tabs, there is a 'Virus Scan Groups' section with buttons for 'Add', 'Remove', and 'Remove All'. A form for adding a new group is visible, with the 'Group Name' field containing 'BOWBRIDGE' and buttons for 'Continue' and 'Cancel'. Below the form is a table with columns 'Name' and 'Description'.

3. Mark the newly created Group as the "Default Scan Group" and save the changes

Note: unlike on an ABAP stack, no INIT parameters are set at the Virus Scanner Group level

Defining a Virus Scan Adapter

Although configuration as Virus Scan Server and Virus Scan Adapter are both supported, bowbridge and SAP strongly recommend using the Adapter mode.

In Adapter mode, the VSA loads directly into the SAP kernel, providing increased stability and significantly better performance.

Configuration Steps:

1. Open NWA's Virus Scan Provider -> Configuration dialogue
2. Select the "Adapter" tab
3. Switch to Edit Mode and add a new Virus Scan Adapter
4. Define a name for the virus scan adapter. Note the name must start with VSA_

The screenshot shows the 'Virus Scan Adapters' configuration window. At the top, there are tabs: Overview, Groups, **Adapters**, Servers, and Profiles. Below the tabs, there is a section titled 'Virus Scan Adapters' with buttons: Add, Remove, Remove All, Activate, and Deactivate. Below these buttons, there is a text field for 'Adapter Name' containing 'VSA_BOWBRIDGE' and buttons 'Continue' and 'Cancel'. Below this, there is a table with columns: Status, Name, and Description. The table is currently empty, and a message at the bottom states: 'No available virus scan adapters to display'.

5. In the next step, provide the path to the VSA shared library/DLL (libAVB31.so on UNIX, BBVSA3-1.DLL on Windows), set the Scan Group and re-init interval (optional)

The screenshot shows the 'Virus Scan Adapter Details' configuration window. At the top, there are tabs: **Settings**, Trace, and Parameters. Below the tabs, there is a section titled 'Virus Scan Adapter Settings'. It contains the following fields:

- ☒ Default Scan Provider
- Adapter Name: VSA_BOWBRIDGE
- Adapter Description: bowbridge Virus Scan Adapter
- Scan Group: * BOW (dropdown menu)
- Init Interval (Hours): 8
- Maximum Instances: 20
- VSA Library Path: :ap/J2E/bowbridge/libAVB31.so



6. select the "Default Scan Provider" checkbox

7. Open the Parameters tab and add entries for the parameters per the table below:

FIELD	REQUIRED	NOTES
INITDIRECTORY	Yes	Path to the bowbride installation folder
INITENGINES	Yes	Virus scanning engine to start. Choose from: <ul style="list-style-type: none">- SOPHOS (embedded, default)- MCAFEE (embedded)- ICAP (requires INITSERVERS)- CLAMAV (requires INITSERVERS)
INITSERVERS	for ICAP and CLAMAV	Specifies the ICAP service URL(s) or ClamAV Socket or TCP destination Consult section " <i>Configuring ICAP Backends</i> " and " <i>Integrating ClamAV</i> " for details.
INITTEMP_PATH	No	Specifies the temp directory used by Anti-Virus to store synchronization files and repack SAPCAR archives
INITTIMEOUT	No	Specifies the maximum time for the virus scan engines to start

8. Save your settings and activate the Virus Scan Provider



Defining Virus Scan Profiles

Application programs use virus scan profiles to check data for viruses. A virus scan profile contains a list of scanner groups that check a document. You can also use a virus scan profile to assign configuration parameters for the virus scanner. If you check for viruses with this virus scan profile, the virus scanner receives the parameters.

A virus scan profile specifies steps that are to be run during a scan. A step is either a virus scanner, which is found using the scanner group, or a step specifies, in turn, a virus scan profile, which is then performed as part of the enclosing virus scan profile.

A virus scan is performed under the name of a virus scan profile. The system administrator can use the profile to activate or deactivate the virus scan for each component. By default, a virus scan profile is provided for each SAP application that integrates virus scan functionality.

Configuration Steps:

1. On the Profiles tab page, create a virus scan profile in change mode by choosing the Add button.
2. In the Profile Name field, enter the rest of the name after the predefined prefix, and choose Continue. This adds a new row in the Virus Scan Profiles group box.
3. In the Virus Scan Profile Details group box, you have the following options on the Settings tab page:
 - Select the profile to be edited as a reference profile by setting the Default Scan Profile indicator.
 - Use the default profile.
 - In the Reference Profile field, select the <Default Profile>.
 - Use a reference profile

Since a virus scan profile can use another virus scan profile as a reference profile, it is possible to operate multiple applications using the same virus scan profile.

This creates a link to an existing reference profile. To do this, use the input help for the Reference Profile field to select a reference profile.
 - Define a new profile
 - Choose Add and enter information according to the following table:

FIELD	NOTES
Profile Name	The name of the new profile is displayed.
Profile Description	Description of the new profile
Reference Profile	This indicator must not be set, since the other input fields would otherwise be hidden.
Step Linkage	<p>Linkage of the steps of this profile:</p> <p><u>All steps successful:</u> AND linkage, with which every step must be successful for the overall result to be successful.</p> <p><u>At least one Step successful:</u> OR linkage, with which only one step needs to be successful for the overall result to be successful.</p>
Profile Steps	Use the input help to select profile steps.

- Specify the profile steps in the Profile Steps group box.
 - + Choose Add.
 - + Use the input help to specify in the Type field whether a group or another profile is to be used.
 - + Use input help to specify the value of the group or profile.
 - + Configure the list with the buttons Move up, Move down, and Remove.

SettingsParameters

Virus Scan Profile Settings

☒ Default Scan Profile

Profile Name:

Profile Description:

Reference Profile:

Profile Steps

AddRemoveMove UpMove Down

Step Linkage: * All steps successful

Step Type	Value
Group	▼ BOWBRIDGE

- + Complete the installation by saving the entries and activating the profile

Advanced Content Scanning - Java configuration

As a VSI 2.0-certified solution, bowbridge Anti-Virus offers further content scanning capabilities beyond the scanning for malware. Content can be filtered based on its MIME-type, the file extension, the combination of content and extension and based on active content included in the files. While none of those criteria qualify as malware by definition, they still pose a relevant threat to your SAP application and users.

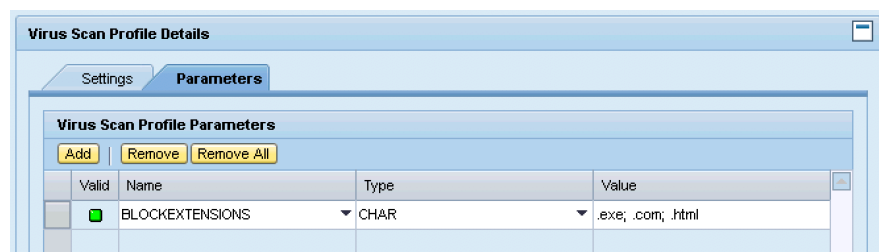
Advanced content filters are configured via Virus Scan Profiles as follows:

File Extension Blacklist:

The file extension blacklist may be used to block files with certain extensions prior to the virus scan.

Configuration Steps:

1. Open the Parameters tab of the relevant Profile in Edit mode
2. Choose Add to create a new entry
3. Select BLOCKEXTENSIONS from the input help
4. Set the type to CHAR
5. Provide the semicolon-separated list of extensions to block:



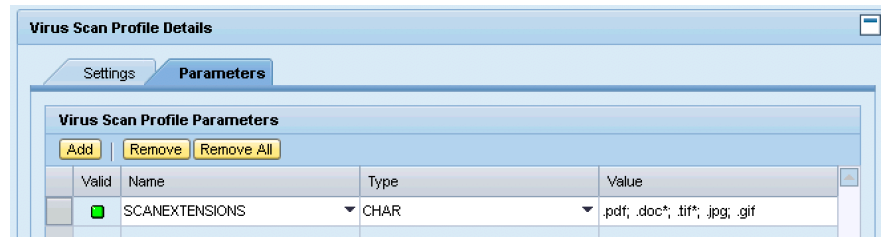
6. Upon saving the settings, NWA will validate the entries and show green if they passed validation

File Extension Whitelist:

The file extension whitelist may be used to allow only files with certain extensions to continue to be processed and scanned. All other files will be blocked.

Configuration Steps:

1. Open the Parameters tab of the relevant Profile in Edit mode
2. Choose Add to create a new entry
3. Select SCANEXTENSIONS from the input help
4. Set the type to CHAR
5. Provide the semicolon-separated list of extensions to process:



6. Upon saving the settings, NWA will validate the entries and show green if they passed validation

MIME-Type Filtering

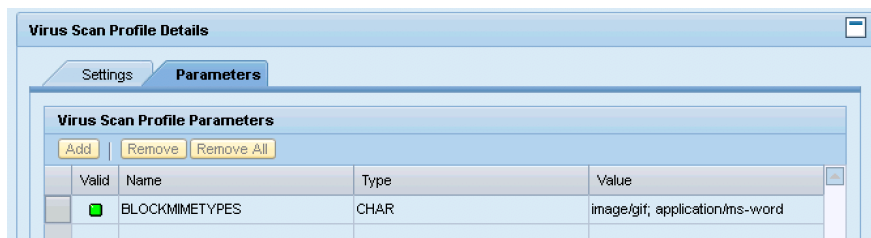
bowbridge Anti-Virus allows for filtering of content based on their MIME-type. The MIME-type of any given file is determined by analysing the content of the file and therefore offers a more thorough protection than filtering based on the filename extension.

MIME filters may be implemented as Whitelist or Blacklist.

Setting up a MIME-type Blacklist

Configuration Steps:

1. Open the Parameters tab of the relevant Profile in Edit mode
2. Choose Add to create a new entry
3. Select BLOCKMIMETYPES from the input help
4. Set the type to CHAR
5. Provide the semicolon-separated list of MIME-types to block:

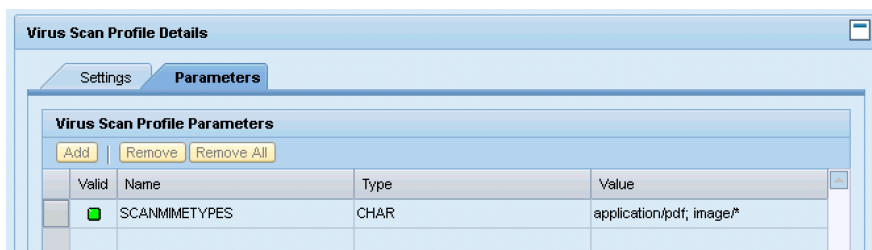


6. Upon saving the settings, NWA will validate the entries and show green if they passed validation

Setting up a MIME-type Whitelist

Configuration Steps:

1. Open the Parameters tab of the relevant Profile in Edit mode
2. Choose Add to create a new entry
3. Select SCANMIMETYPES from the input help
4. Set the type to CHAR
5. Provide the semicolon-separated list of MIME-types to process:



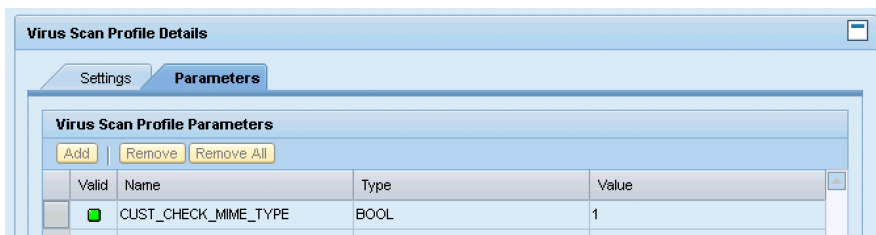
6. Upon saving the settings, NWA will validate the entries and show green if they passed validation

Content Validation

Attackers may try to circumvent security by assigning files a file extension that does not match its actual content. bowbridge Anti-Virus can analyze the content of any file and compare the file extension to legitimate extensions for that content type. Deviations are blocked.

Configuration Steps:

1. Open the Parameters tab of the relevant Profile in Edit mode
2. Choose Add to create a new entry
3. Select CUST_CHECK_MIME from the input help
4. Set the type to BOOL and value to 1
5. Save the entries





Blocking Active Content

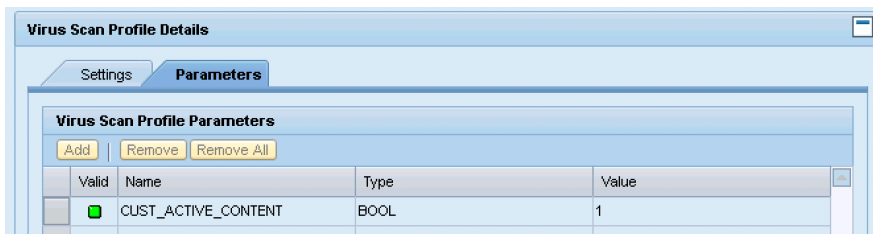
Attackers may try upload files with active elements into your application in order to compromise clients accessing these documents or in order to stage a Cross-Site Scripting (XSS) attack.

bowbridge Anti-Virus can detect and block files containing active content. It is equipped with filters detecting:

- JavaScript in HTML, XML and SVG
- Scripts and Macros in Office documents
- JavaScript, OpenAction and ActiveAction in PDF
- Silverlight
- Flash
- Java archives embedded in image files and Office documents.
- XSLT

Configuration Steps:

1. Open the Parameters tab of the relevant Profile in Edit mode
2. Choose Add to create a new entry
3. Select CUST_ACTIVE_CONTENT from the input help
4. Set the type to BOOL and value to 1
5. Save the entries



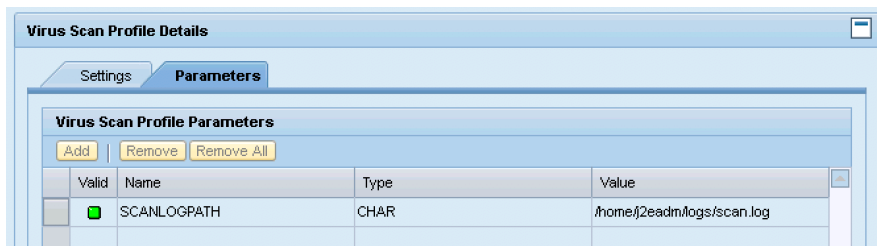
Logging Scan Activity

bowbridge Anti-Virus supports a simple logging of all scan activities in a plain-text, human readable log file.

Logging of scans may be activated via a specific virus scan profile, or in the one referenced as the default profile.

Configuration Steps:

1. Open the Parameters tab of the relevant Profile in Edit mode
2. Choose Add to create a new entry
3. Select SCANLOGPATH from the input help
4. Set the type to CHAR and
5. Provide a filename in a location writable by <SID>adm on UNIX and SAPService<-SID> on Windows
6. Save the entries



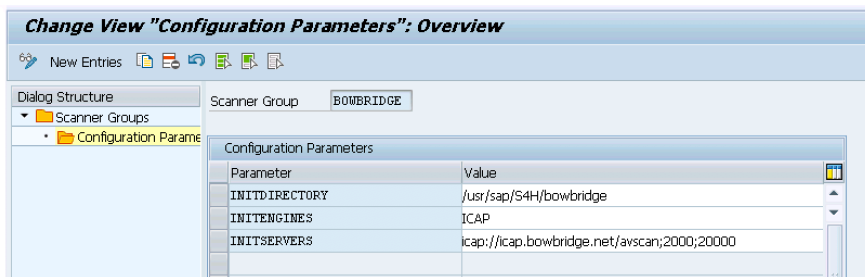
Configuring ICAP-based virus scanning

bowbridge Anti-Virus can leverage existing ICAP-capable virus scan engines. Despite offering less scan performance than the embedded engines, the use of ICAP can be an interesting option if:

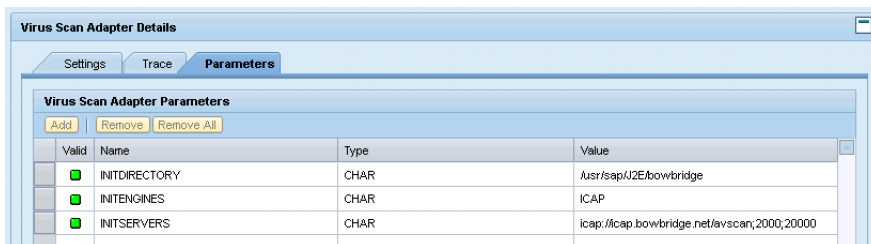
- scanning with an engine from a specific vendor, other than McAfee or SOPHOS is desired
- separation of SAP-management and security management is desired.
- ICAP-based virus scanning is provided as a service by your security department
- you do not wish to run a virus scan engine on your NetWeaver application server

To use ICAP for virus scanning, you need to specify "ICAP" as the INITENGINES parameter:

- on ABAP: in the Virus Scan Group configuration



- on J2EE: in the Virus Scan Provider parameters tab





bowbridge Anti-Virus supports up to two ICAP servers. When two ICAP servers are provided, concurrent connections are automatically shared among the two ICAP servers. Also, if one of the ICAP servers fails, the remaining one will be used for scanning. To setup ICAP servers, you need to configure the INITSERVERS parameter to contain the ICAP URL(s) and timeout values in the following format:

Scanning with one ICAP server:

```
icap://[hostname or IP]:[port - optional]/ICAP-service-path ; connect-timeout ; operation timeout
```

Example:

```
icap://192.168.10.123:11344/avscan;2000;20000
```

Note: the port option i.e. “:11344” is only required if your ICAP service runs on a port other than the default port TCP/1344)

Scanning with two ICAP servers:

```
icap://[server 1 hostname or IP]:[port - optional]/ICAP-service-path ; connect-timeout ; operation timeout ;
```

```
icap://[server 2 hostname or IP]:[port - optional]/ICAP-service-path ; connect-timeout ; operation timeout
```

Example:

```
icap://192.168.10.123/avscan;2000;20000;icap://192.16.10.124/avscan;3000;25000
```

ICAP over SSL ("ICAPS")

ICAP over SSL is supported.

To activate this functionality, specify the ICAP URL starting with "icaps://".

The default port for ICAP over SSL is TCP/1345

Example:

```
icaps://192.168.10.123/avscan;2000;20000
```

Note: When using service-mode with ICAP or CLAMAV engines, the INITSERVERS parameter must be set in the bbvsa31.cfg configuration file.

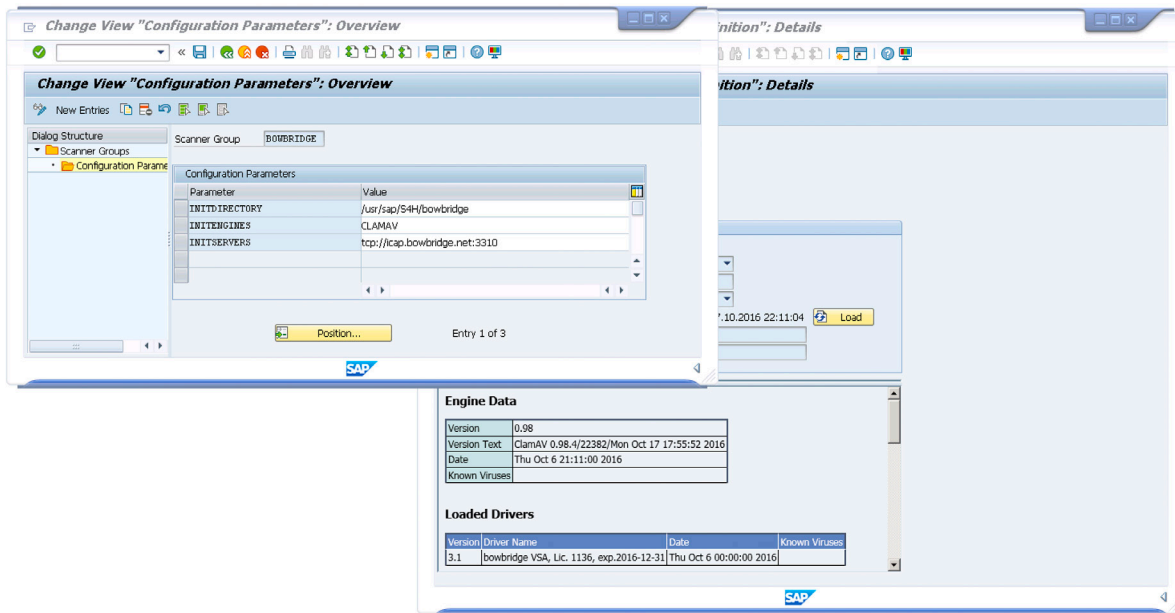
Configuring ClamAV-based virus scanning

bowbridge Anti-Virus can leverage the open-source virus scanning solution "ClamAV". While the use of ClamAV is not recommended for production environments, it represents an interesting alternative to commercial virus scanning engines for development instances or as a "second opinion scanner".

Connection to ClamAV's Clam-Daemon (clamd) can be via setup a local socket (UNIX/Linux only) or via TCP/3310.

To use ClamAV for virus scanning, you need to specify "CLAMAV" as the INITENGINES parameter.

- on ABAP: in the Virus Scan Group configuration



- on J2EE: in the Virus Scan Provider parameters tab

SettingsTraceParameters				
Virus Scan Adapter Parameters				
AddRemoveRemove All				
Valid	Name	Type	Value	
<input checked="" type="checkbox"/>	INITDIRECTORY	CHAR	/usr/sap/J2E/bowbridge	
<input checked="" type="checkbox"/>	INITENGINES	CHAR	CLAMAV	
<input checked="" type="checkbox"/>	INITSERVERS	CHAR	/var/lib/clamav/clamd-socket	



Preloading configuration parameters from configuration files

In some deployments, configuration settings need to be provided to bowbridge Anti-Virus without them being configured at the SAP customization level. For this purpose, Anti-Virus will check for the presence of a host-global configuration file and a SID-specific configuration file.

Further, some functionality, such as trace-file output, alternate update sources and the definition of what is detected as active content can be set via configuration files only.

Host-global configuration file

The host-global configuration file (UNIX only) is to be created and stored as:

`/etc/bowbridge/bbvsa31.cfg`

SID-specific configuration file

The SID-specific configuration file is to be created and stored as: `/usr/sap/[SID]/bowbridge/bbvsa31.cfg`

Anti-Virus evaluates parameters in the following order:

- host-global configuration file
- SID-specific configuration file
- parameters passed from the SAP application server

Configuration file parameter format

The host-global and SID-specific configuration file follow the same simple format. It is structured in sections:

- INIT
- SCAN
- ACTIVE_CONTENT
- TRACE
- UPDATE
- SCRIPTS
- EPO
- MISC

where section names need to be in brackets (i.e. `[INIT]`).

Values for the supported parameters are provide without quotation marks after an equal sign (i-e: `INITENGINES=SOPHOS;2`)

Name-Value-pairs or entire sections may be commented out with a preceeding `"#"`



Controlling Automatic Updates

bowbridge Anti-Virus, when used with either of the integrated virus scanning engines, performs automatic downloads of virus scanning engine updates and virus definition updates from the bowbridge CDN.

These updates are installed automatically. Manual intervention or scheduled re-initialization of the Virus Scan Adapter is not required.

Update Sources

By default, bowbridge Anti-Virus attempts to download updates directly from the bowbridge CDN via HTTP/HTTPS.

The URLs accessed are

`http(s)://update.update.bowbridge.net`

and

`http(s)://cdn.update.bowbridge.net`

It is in the nature of a CDN that IP-addresses for the CDN edge node can (and will) change over time and based on your location.

bowbridge Anti-Virus can be configured to download updates via a Web-Proxy or from an internal update source, such as the bowbridge Local Update Service.

Please refer to the Configuration Parameter Overview at the end of this document for details or contact bowbridge technical support for assistance on how to configure alternate update sources.

Integration with McAfee ePO

bowbridge Anti-Virus provides an integration with McAfee e-Policy Orchestrator (ePO). Once enabled, McAfee customers are able to monitor security relevant events and product properties in ePO. To benefit from the integration, it is required to install and configure the McAfee Agent on the SAP systems and establish communication between the McAfee agent and the ePO server.

SAP-server-side configuration (Linux/UNIX only)

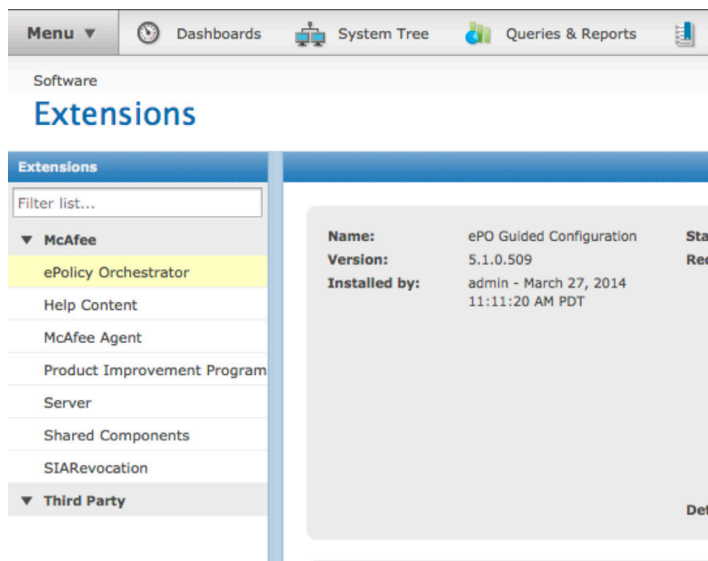
In order to activate the integration on UNIX platforms an additional installation step is required:

- Please open a terminal into your bowbridge installation directory
- In the `bbvsa31.cfg` file, locate the `[EPO]` section and set `EPOLOG=1`
- restart the Virus Scan Adapter in order to activate the changes

ePO-side configuration

In order for ePO to interpret the events generated by Anti-Virus, it is necessary to install the bowbridge ePO extension.

To do so, navigate to the Extensions settings from the ePO management interface:



Click the "Install Extension"-Button at the bottom of the page and select the bowbridge ePO Extension file:

Software

Extensions

Install Extension

Name:	S_BBRSAP3000
Version:	1.0.0.0
Product:	BowBridge
Details:	Extension for S_BBRSAP3000
Signed by:	Not signed by McAfee
Requires:	<ul style="list-style-type: none"> • core • EPOCore

Choose OK to activate the extension.

Software

Extensions

Extensions

Filter list...

▼ McAfee

- ePolicy Orchestrator
- Help Content
- McAfee Agent
- Product Improvement Program
- Server
- Shared Components

Name:	S_BBRSAP3000	Status:	Installed	Modules:
Version:	1.0.0.0	Requires:	<ul style="list-style-type: none"> • Core Modules 2.5 • ePO Core 4.5 	
Installed by:	admin - April 6, 2014 3:19:42 PM PDT	Details:	Extension for S_BBRSAP3000	

bowbridge Anti-Virus properties will be displayed and updated in your ePO console:

System Properties	Products	Threat Events	McAfee Agent
Product	Version	Dat Version	
Agent	4.8.0.887		
BowBridge AntiVirus Bridge for SAP solutions	3.0.11	7400.0	
Product properties for BowBridge AntiVirus Bridge for SAP solutions			
BowBridge AntiVirus Bridge for SAP solutions	S_BBRSAP		
Product Version	3.0.11		
Language	English (United States)		
Hotfix/ Patch Version	1471		
Engine Version	5600.1067		
DAT Version	7400.0		
Details			
DAT File 1	/usr/sap/NPL/bowbridge/mcafee/1396819810/dat/avvnames.dat		
DAT File 1 Date	6.4.2014		
DAT File 2	/usr/sap/NPL/bowbridge/mcafee/1396819810/dat/avvscan.dat		
DAT File 2 Date	6.4.2014		
DAT File 3	/usr/sap/NPL/bowbridge/mcafee/1396819810/dat/avvclean.dat		
DAT File 3 Date	6.4.2014		
Last update	Sun Apr 6 23:30:10 2014		
General			
DatVer	7400.0		
EngineVer	5600.1067		



Security events will be displayed in your ePO console:

Event Generated Time ▼	Event ID	Event Category	Threat Name	Action Taken
4/6/14 2:08:45 AM	202958	Update failed	Engine update failed	Automatic engine update
4/6/14 2:08:45 AM	202960	Update failed	Automatic DAT update failed	DAT update not deployed
4/6/14 2:08:19 AM	202950	Service started	VSA started	None
4/6/14 2:07:36 AM	202952	Service ended	VSA shut down	None
4/6/14 2:05:09 AM	202960	Update failed	Automatic DAT update failed	DAT update not deployed
4/6/14 2:03:05 AM	202960	Update failed	Automatic DAT update failed	DAT update not deployed
4/6/14 2:03:05 AM	202950	Service started	VSA started	None
4/6/14 2:03:05 AM	202957	Update ended	Engine update deployed	Engine 5600.1067 deploye
4/6/14 2:03:05 AM	202954	Malware detected	EICAR test file	Blocked
4/6/14 2:03:05 AM	202959	Update ended	DAT update deployed	DAT 7400.0 deployed
4/6/14 2:03:05 AM	202952	Service ended	VSA shut down	None
4/6/14 2:03:05 AM	202950	Service started	VSA started	None
4/6/14 2:03:05 AM	202954	Policy (policy.detect)	MIME type blocked	Blocked
4/6/14 2:03:05 AM	202952	Service ended	VSA shut down	None
4/6/14 2:03:05 AM	202950	Service started	VSA started	None
4/6/14 2:03:05 AM	202956	Scan failed	BowBridge license invalid or expl	Blocked

Deactivating the ePO integration

In order to deactivate the forwarding of properties and events to ePO, edit your relevant bbvsa30.cfg configuration file and delete or comment-out (by adding “#” in front of the parameter) the EPOLOG=1 parameter in the [EPO]-section of the configuration file.



Integration with OS-level anti-virus updates

bowbridge Anti-Virus can leverage centrally distributed updates to McAfee Virus Scan Enterprise for Windows and McAfee Endpoint Security for Linux.

Configuration on Windows Servers:

Locate and open the configuration file bbvsa31.cfg in a text editor

locate the [UPDATE] section and adjust the following parameters:

VSE_DATDIR= <Fully qualified path to the directory where AVVSCAN.DAT is located>

VSE_ENGINEDIR= <Fully qualified path to the directory where MSCAN64A.DLL is located>

VSE_EXTRADATDIR=<optional, fully qualified path to where EXTRA.DAT is located>

In default Virus Scan Enterprise installations, the values will be:

VSE_DATDIR=C:\Program Files (x86)\Common Files\McAfee\Engine

VSE_ENGINEDIR=C:\Program Files (x86)\Common Files\McAfee\Engine\x64

EXTRADATDIR=C:\Program Files (x86)\Common Files\McAfee\Engine

Anti-Virus will monitor these files for modification and trigger copying and applying the updates as soon as a change is detected.

For the changes to become active, please stop/start the VSA, or terminate the UPD-MCAF.EXE process in Task Manager. The process will be restarted automatically and leverage the new configuration.

Configuration on Linux Servers

Locate and open the configuration file bbvsa31.cfg in a text editor

locate the [UPDATE] section and adjust the following parameters:

ENS_LIBDIR=<Fully qualified path to the directory where the engine version subdirectories are located>

ENS_DATDIR=<Fully qualified path to the directory where the DAT subdirectories are located>

ENS_EXTRADATDIR=<optional, fully qualified path to where the extra dat is located>

ENS_SIDADM=<name of the SIDadm user of the instance>



In default Endpoint Security for Linux installations, the values will be:

```
ENS_LIBDIR=/opt/isec/ens/threatprevention/var/engine/lib
ENS_DATDIR=/opt/isec/ens/threatprevention/var/engine/dat
ENS_EXTRADATDIR=/opt/isec/ens/threatprevention/var/engine/dat/extra
```

Granting UPDMCAF extended privileges

With Endpoint Security for Linux, McAfee updates are readable for the root-user only. Therefore the UPDMCAF process must have access to root permissions via a SetUID configuration.

When running with SUID root, the process will immediately drop privileges to the SIDadm user configured in the ENS_SIDADM parameter (or SIDadm user name derived from the SAPSYSTEMNAME environment variable).

In order to give the required permissions to the UPDMCAF process, login or su to the root user and perform the following steps inside the bowbridge installation directory:

```
su root
chown root UPDMCAF
chmod 755 UPDMCAF
chmod +s UPDMCAF
exit
```

For the changes to go into effect, please stop/start the VSA (waiting for the UPDMCAF process to terminate) or simply kill the UPDMCAF process; it will be restarted automatically.



Configuration Parameter Reference

Initialization Parameters

Section Name: INIT
Parameter Name: INITDIRECTORY
Parameter Type: String (pszChar)
Description: Specifies the path to where AVB is installed. All paths for loading of libraries, components and engines are built based on INITDIRECTORY
Default: n/a
Set via: SAP Customizing/Configuration files

Section Name: INIT
Parameter Name: INITENGINES
Parameter Type: String (pszChar)
Values: ICAP, CLAMAV, SOPHOS, MCAFEE, DUMMY
Description: Specifies the virus scan engine to use. CLAMAV and ICAP also require INITSERVERS to be defined.
The DUMMY engine allows an adapter to be configured on the system but does not provide any actual scanning capabilities.
Default: SOPHOS
Set via: SAP Customizing/Configuration files

Section Name: INIT
Parameter Name: INITSERVERS
Parameter Type: String (pszChar)
Description: For ICAP: ICAP URL(s) to the scan servers. URL format:
icap://<IP-address>[:port]/<service path>; <connect timeout>;<scan timeout>
For HA and Load-Balancing (Round Robin scheme) 2 ICAP URLs can be specified, separated by semicolon:
icap://<first P-address>[:port]/<service path>; <connect timeout>;<scan timeout>;icap://<second IP-address>[:port]/<service path>; <connect timeout>;<scan timeout>;

Load-balancing can be switched off by adding „;HA-ONLY“ after the second: CAP URL. i.e.:
icap://<first P-address>[:port]/<service path>; <connect timeout>;<scan timeout>; icap://<second IP-address>[:port]/<service path>; <connect timeout>;<scan timeout>;HA-ONLY

For ClamAV: Filesystem-Path to the ClamAV socket file. For example:
/var/run/clamav/clamd.sock
For remote connections:



Default: tcp://<ip-address>:<port>
n/a
Set via: SAP Customizing/Configuration files

Section Name: INIT
Parameter Name: INITTEMP_PATH
Parameter Type: String (pszChar)
Description: Overrides the OS/Environment-provided temp-path.
Locking and synchronization files will be created and maintained in this directory. Further the repackaging of SAPCAR archives is performed in this directory
Default: n/a
Set via: SAP Customizing/Configuration files

Section Name: INIT
Parameter Name: INITTIMEOUT
Parameter Type: Integer
Description: Specifies the number in seconds after which the adapter initialization must be completed
Default: 90
Set via: SAP Customizing/Configuration files

Section Name: INIT
Parameter Name: SAPCARPATH
Parameter Type: String (pszChar)
Description: Specifies the fully qualified path to the SAPCAR executable. This parameter is needed only if handling of SAPCAR files should be performed by the SAPCAR executable rather than the built-in SAPCAR decompression.
Default: n/a (commented out)
Set via: Configuration files

Section Name: INIT
Parameter Name: SERVICE_MODE
Parameter Type: Integer
Description: When set to "1", the VSAs do not control the virus scan engine and associated services. These must be controlled via the Operating system's services management console. Service mode provides faster startup and increased stability on Windows
Default: n/a (User-selected upon installation/upgrade)
Set via: Configuration files



Scan Parameters

Section Name: SCAN
Parameter Name: SCANBESTEFFORT
Parameter Type: Bool
Description: Toggles whether the scan engine should use ALL available technologies to scan the file (signature, heuristics, none) is left to the scan engine.
Default: 1
Set via: SAP Customizing Virus Scan Profile/Configuration files

Section Name: SCAN
Parameter Name: SCANALLFILES
Parameter Type: Bool
Description: Toggles whether the scan engine should scan ALL files or may choose to not scan certain files, that may be considered benign (i.e. text/plain)
Default: 1
Set via: SAP Customizing Virus Scan Profile/Configuration files

Section Name: SCAN
Parameter Name: SCANEXTRACT
Parameter Type: Bool
Description: Toggles whether the scan engine should unpack and scan inside archives
Default: TRUE
Set via: SAP Customizing Virus Scan Profile/Configuration files
Note: SCANEXTRACT = 0 cannot be used with ICAP

Section Name: SCAN
Parameter Name: SCANEXTRACT_DEPTH
Parameter Type: Integer
Description: Specifies the maximum number of nested archives that will be unpacked for scanning. Exceeding the value will result in SCAN_FAILED
Default: 20
Set via: SAP Customizing Virus Scan Profile/Configuration files



Section Name: SCAN
Parameter Name: BLOCKACTIVECONTENT (= CUST_ACTIVE_CONTENT)
Parameter Type: Bool
Description: Toggles the detection and blocking of active content. Granular configuration of what is considered active content is to be performed in the [ACTIVECONTENT] section of the bbvsa30.cfg configuration file. SAP Customizing does not provide sufficient configuration options.
Default: 0
Set via: SAP Customizing Virus Scan Profile/Configuration files

Section Name: SCAN
Parameter Name: CHECKCONTENT
Parameter Type: String (pszChar)
Description: RegEx Filter, Largely irrelevant for file-based scanning
Default: n/a

Section Name: SCAN
Parameter Name: CHECKMIMETYPE (= CUST_CHECK_MIME_TYPE)
Parameter Type: Bool
Description: Toggles the MIME-to-Extension check. When TRUE, the detected MIME type and file extensions will be checked against the mime_ext_map file. Mappings not detected in the map file will result in the file being blocked.
Default: 0
Set via: SAP Customizing Virus Scan Profile/Configuration files

Section Name: n/a
Parameter Name: CUST_CLEAN
Parameter Type: Bool
Description: Toggles the signal sent to the virus scan engine to attempt to clean infected files. For this parameter to have an effect with ICAP-connected scan engines, the ICAP-sever must be configured on server-side to attempt cleaning of infected files.
Note: From a forensics perspective, bowbridge does not recommend using cleaning of infected files, as the originally uploaded files will be modified in this process.
Set via: SAP Customizing Virus Scan Profile (Profile Parameter)



Section Name: n/a
Parameter Name: CUST_NO_SCANINFO
Parameter Type: Bool
Description: Requests the VSA to return the respective return-code only and not attach a Scan-Information structure. Hence, the MIME-type, File-extension and blocking reasons are not provided back to the calling function.
Note: From a forensics perspective, bowbridge does not recommend using this parameter as it keeps important forensic information from being written to the SAP Security Audit Log.
Set via: SAP Customizing Virus Scan Profile (Profile Parameter)

Section Name: SCAN
Parameter Name: SCANMIMETYPES
Parameter Type: String (pszChar)
Description: MIME types Whitelist. Semicolon-delimited list of MIME-Types. Wildcards („*” and „?”) are permitted. Only files with MIME-types found on this list will be accepted for further processing. All other files will be blocked with BLOCKED_BY_POLICY („MIME-Type not allowed”)
Default: n/a
Set via: SAP Customizing Virus Scan Profile/Configuration files

Section Name: SCAN
Parameter Name: BLOCKMIMETYPES
Parameter Type: String (pszChar)
Description: MIME types Blacklist. Semicolon-delimited list of MIME-Types. Wildcards („*” and „?”) are permitted. Files with MIME-types found on this list will not be accepted for further processing. They will be blocked with BLOCKED_BY_POLICY („MIME-Type forbidden”)
Default: n/a
Set via: SAP Customizing Virus Scan Profile/Configuration files

Section Name: SCAN
Parameter Name: SCANEXTENSIONS
Parameter Type: String (pszChar)
Description: File extension Whitelist. Semicolon-delimited list of MIME-Types. Wildcards („*” and „?”) are permitted. Only files with extensions found on this list will be accepted for further processing. All other files will be blocked with BLOCKED_BY_POLICY („Extension not allowed”)
Default: n/a
Set via: SAP Customizing Virus Scan Profile/Configuration files



Section Name: SCAN
Parameter Name: BLOCKEXTENSIONS
Parameter Type: String (pszChar)
Description: File Extension Blacklist. Semicolon-delimited list of MIME-Types. Wildcards („*” and „?“) are permitted. Files with extensions found on this list will not be accepted for further processing. They will be blocked with BLOCKED_BY_POLICY („Extension forbidden“)
Default: n/a
Set via: SAP Customizing Virus Scan Profile/Configuration files

Section Name: SCAN
Parameter Name: SCANLOGPATH
Parameter Type: String (pszChar)
Description: Fully qualified path to a log file to which all scanning activity will be logged in a human readable format. The containing directory must exist.
Default: n/a
Set via: SAP Customizing Virus Scan Profile/Configuration files

Section Name: SCAN
Parameter Name: BLOCKHTMLINPDF
Parameter Type: Bool
Description: When set, HTML tags in PDF documents are flagged as „Chameleon File“, resulting in blocking of the file. Note: As there is an overlap between valid HTML and PDF tags (i.e.), Support recommends to disable it by default, based on a high number of false positives.
Default: 1
Set via: Configuration files

Section Name: SCAN
Parameter Name: MAX_SCANLOGSIZE_MB
Parameter Type: Int
Description: Maximum size of the Scan log file (parameter SCANLOGPATH). If the size is exceeded, a new scan log file is created and the old one is compressed (ZIPped).
Default: n/a
Set via: Configuration files



Active Content Definitions

These parameters define what potentially dangerous content-types are flagged as active content:

Section Name: ACTIVECONTENT
Parameter Name: PDF_JAVASCRIPT
Parameter Type: Integer [0-2]
Description: Toggles the blocking of Javascript in PDF.
0: Off
1: identify „/JS“ and „/JavaScript“ active content
2: identify „/JavaScript“ active content
Default: 1
Set via: Configuration files

Section Name: ACTIVECONTENT
Parameter Name: PDF_ACTIVE_ACTION
Parameter Type: Bool
Description: Identify „/AA“ as active content
Default: 1
Set via: Configuration files

Section Name: ACTIVECONTENT
Parameter Name: PDF_OPEN_ACTION
Parameter Type: Bool
Description: Identify „/OpenAction“ as active content
Default: 1
Set via: Configuration files

Section Name: ACTIVECONTENT
Parameter Name: PDF_LAUNCH
Parameter Type: Bool
Description: Identify „/Launch“ as active content
Default: 1
Set via: Configuration files



Section Name: ACTIVECONTENT
Parameter Name: PDF_ACROFORM
Parameter Type: Bool
Description: identify „/AcroForm“ as active content
Default: 1
Set via: Configuration files

Section Name: ACTIVECONTENT
Parameter Name: PDF_RICHMEDIA
Parameter Type: Bool
Description: identify „/RichMedia“ as active content
Default: 1
Set via: Configuration files

Section Name: ACTIVECONTENT
Parameter Name: MSOFFICE_MACRO
Parameter Type: Bool
Description: identify macros in MS Office files (POLE and OOXML) as active content
Default: 1
Set via: Configuration files

Section Name: ACTIVECONTENT
Parameter Name: MSOFFICE_JAVA
Parameter Type: Bool
Description: identify JavaClasses in MS Office OOXML files
Default: 1
Set via: Configuration files

Section Name: ACTIVECONTENT
Parameter Name: MSOFFICE_OLE
Parameter Type: Bool
Description: identify OLE embedded objects as active content (no recursive scan)
Default: 1
Set via: Configuration files



Section Name: ACTIVECONTENT
Parameter Name: ZIP_JAVAARCHIVE
Parameter Type: Bool
Description: identify ZIP Archives containing Java Archive artefacts (JAR) as active content
Default: 1
Set via: Configuration files

Section Name: ACTIVECONTENT
Parameter Name: HTML_SCRIPT
Parameter Type: Bool
Description: identify HTML as active content when containing:
- <SCRIPT ...>
- <EMBED ...>
- <OBJECT ...>
- <XSL ...>
- JavaScript
Default: 1
Set via: Configuration files

Section Name: ACTIVECONTENT
Parameter Name: HTML_EVENTHANDLER
Parameter Type: Bool
Description: identify HTML containing event handler registrations as active content
Default: 1
Set via: Configuration files

Section Name: ACTIVECONTENT
Parameter Name: GIFAR
Parameter Type: Bool
Description: identify chameleon files (i.e. GIFAR) as active content
Default: 1
Set via: Configuration files



Section Name: ACTIVECONTENT
Parameter Name: FLASH
Parameter Type: Bool
Description: identify Macromedia Flash as active content
Default: 1
Set via: Configuration files

Section Name: ACTIVECONTENT
Parameter Name: SILVERLIGHT
Parameter Type: Bool
Description: identify Microsoft Silverlight as active content
Default: 1
Set via: Configuration files

Section Name: ACTIVECONTENT
Parameter Name: EXECUTABLE
Parameter Type: Bool
Description: identify all executable file types as active content
Default: 1
Set via: Configuration files.

Section Name: ACTIVECONTENT
Parameter Name: XML_JAVASCRIPT
Parameter Type: Bool
Description: identify JavaScript in XML as active content
Default: 1
Set via: Configuration files.



Quarantine Parameters

Section Name: QUARANTINE
Parameter Name: ON_BLOCK
Parameter Type: Bool
Description: Copy files blocked to an encrypted quarantine file
Default: 0
Set via: Configuration files.

Section Name: QUARANTINE
Parameter Name: ON_ERROR
Parameter Type: Bool
Description: Copy to an encrypted quarantine file if a scan error occurred
Default: 0
Set via: Configuration files.

Section Name: QUARANTINE
Parameter Name: QUARANTINEPATH
Parameter Type: Char
Description: Directory where encrypted quarantine files should be stored
Default: n/a
Set via: Configuration files.

Section Name: QUARANTINE
Parameter Name: QUARANTINEPASSWORD
Parameter Type: Char
Description: Password/Key for the encryption of the quarantined files
Default: n/a
Set via: Configuration files.



Update Parameter

Section Name: UPDATE
Parameter Name: SERVER
Parameter Type: Char
Description: IP-Address or host name of an alternative update source (LUS)
Default: n/a
Set via: Configuration files

Section Name: UPDATE
Parameter Name: PROXY
Parameter Type: Char
Description: configuration of an HTTP proxy to be used for downloading the updates.
Syntax:
 <proxynome/IP>:<proxyport>
 or
 <username>:<password>@<proxynome/IP>:<proxyport>
Default: n/a
Set via: Configuration files

Section Name: UPDATE
Parameter Name: POLL_INTERVAL
Parameter Type: Integer
Description: Number of seconds before querying the update source for a new signature file
Default: 300 (5min)
Set via: Configuration file

Section Name: UPDATE
Parameter Name: POLL_TURNAROUND
Parameter Type: Integer
Description: Specifies after how many pattern update queries an engine update query is to be performed
Default: 288 (24 hrs for the default POLL_INTERVAL of 300s)
Set via: Configuration files



Section Name: UPDATE
Parameter Name: AUTHENTICATE
Parameter Type: Bool
Description: Specifies whether the update requests should be authenticated with the license signature
Default: 1
Set via: Configuration files

Section Name: UPDATE
Parameter Name: PATTERN_WARN_AGE
Parameter Type: Integer
Description: Specifies the age (in days) of the virus signature file after which the ON_PATTERN_TOOOLD event will be generated to notify the admin of potentially outdated signatures
Default: 5
Set via: Configuration files

Section Name: UPDATE
Parameter Name: PATTERN_BLOCK_AGE
Parameter Type: Integer
Description: Specifies the age (in days) of the virus signature files after which all scans will be blocked with „Virus signature too old“
Default: 30
Set via: Configuration files

Section Name: UPDATE
Parameter Name: GET_SCANENGINE
Parameter Type: Bool
Description: Toggles whether automatic download and installation of the scan engine component should be performed.
Default: 1
Set via: Configuration files

Section Name: UPDATE
Parameter Name: GET_VIRUSDATA
Parameter Type: Bool
Description: Toggles whether automatic download and installation of the virus definitions should be performed.
Default: 1
Set via: Configuration files



Section Name: UPDATE
Parameter Name: VSE_ENGINEDIR
Parameter Type: Char
Description: Directory of the McAfee virus scan engine to monitor for changes. If set, no updates will be downloaded from the bowbridge CDN
Default: n/a
Set via: Configuration files

Section Name: UPDATE
Parameter Name: VSE_DATDIR
Parameter Type: Char
Description: Directory of the McAfee virus definition files to monitor for changes
Default: n/a
Set via: Configuration files

Section Name: UPDATE
Parameter Name: EXTRADATDIR
Parameter Type: Char
Description: Directory of the McAfee extra virus definition files to monitor for changes
Default: n/a
Set via: Configuration files



Custom notification parameters

These parameters map internal notification events to OS-level scripts in the custom_alerts subfolder. The scripts are executed upon each of these events.

Section Name: SCRIPTS
Parameter Name: ON_STARTUP
Script input: Engine name and version

Section Name: SCRIPTS
Parameter Name: ON_SHUTDOWN
Script input: n/a


Section Name: SCRIPTS
Parameter Name: ON_FILE_BLOCKED
Script input: filename, blocking reason

Section Name: SCRIPTS
Parameter Name: ON_STARTUP_ERROR
Script input: failure reason

Section Name: SCRIPTS
Parameter Name: ON_SCAN_ERROR
Script input: filename, error description

Section Name: SCRIPTS
Parameter Name: ON_UPDATE
Script input: component updated (engine/signature)

Section Name: SCRIPTS
Parameter Name: ON_UPDATE_ERROR
Script input: component failed to update (engine/signature)



Section Name: SCRIPTS
Parameter Name: ON_PATTERN_TOOOLD
Script input: descriptive message



Miscellaneous parameters:

Section Name: EPO
Parameter Name: EPOLOG
Parameter Type: Bool
Description: Toggles the generation of log and event information for the McAfee ePO integration
Default: 0
Set via: Configuration files

Section Name: MISC
Parameter Name: LEGACY_MODE
Parameter Type: Bool
Description: Switches the adapter to legacy mode. In this mode, the VSA only advertises VSI 1.0 functionality to the SAP processes for backward compatibility. In legacy mode several features for which there are not SAP SAP Customizing switches can be set through the configuration file only.
Default: 0
Set via: Configuration files





bowbridge Software GmbH

Altrottstraße 31  69190 Walldorf  Germany

t +49-6227-69899-50
e sales@bowbridge.net
w www.bowbridge.net

bowbridge Software USA

530 Lytton Ave, 2nd Floor  Palo Alto, CA 94301  United States

t +1-650-617-3408
e us-sales@bowbridge.net
w www.bowbridge.net