Install and Configure the WMI Agent

For supported software information, click here.

The Windows Management Instrumentation (WMI) agent receives notifications from Microsoft Active Directory (AD) and passes them on the Versa Messaging Service (VMS) so that the VMS can keep its entries updated and can learn about new events. The WMI agent also publishes incremental updates to a real-time messaging server.

VMS is a message streaming server that handles high volumes of streamed data and disseminates this data to the Versa Operating System™ (VOS™) devices that are deployed in a network. Passive authentication based on VMS checks and confirms user identity without requiring any specific action to authenticate users. For more information, see Configure Passive Authentication for VMS. The VMS server receives user events from WMI agents and shares this data with VOS for policy enforcement.

This article describes how to install the WMI agent and how to perform the initial configuration of the WMI agent.

Install the WMI Agent

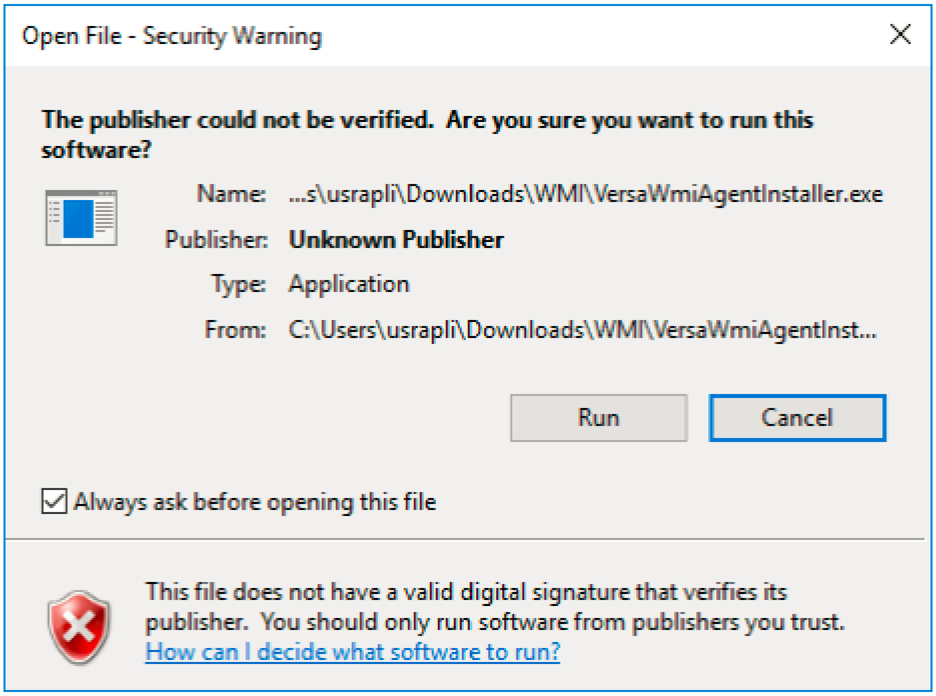
You can install the Versa WMI agent as a standalone component or as a software package installed on a Windows server. The standalone installation is supported on the Windows 10 Client or Windows Server 2016. For hardware requirements, see the Windows 10 Client or Windows Server 2016 documentation.

Before you install the WMI agent, ensure the following:

- Download the Winscp or Wireshark application to the Windows device, to use for debugging.
- After you install Windows, copy the VersaWmiAgentInstaller.exe file to the Windows device from the following link: https://versanetworks.app.box.com/s/d7jh1z6y3kaijd3yfwil0uxchr1w9ton

To install the WMI agent:

1. Double-click the VersaWmiAgentInstaller.exe file.
2. In the Security Warning popup window, click Run.



Open File - Security Warning

The publisher could not be verified. Are you sure you want to run this software?

Name: ...s\usrapli\Downloads\WMI\VersaWmiAgentInstaller.exe

Publisher: **Unknown Publisher**

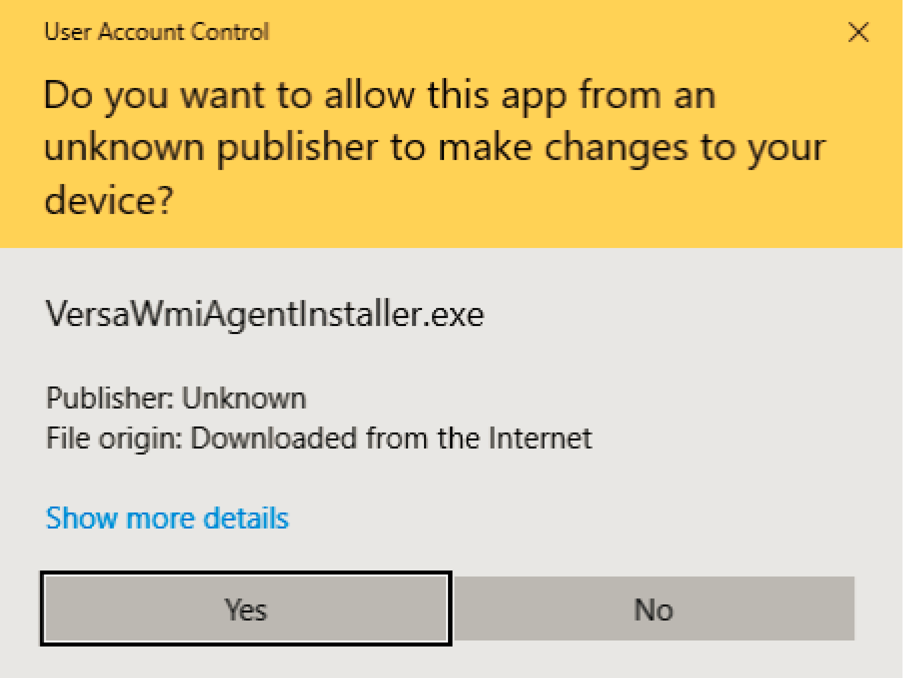
Type: Application

From: C:\Users\usrapli\Downloads\WMI\VersaWmiAgentInst...

☑ Always ask before opening this file

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust.
How can I decide what software to run?

3. In the User Account Control popup window, click Yes.



User Account Control

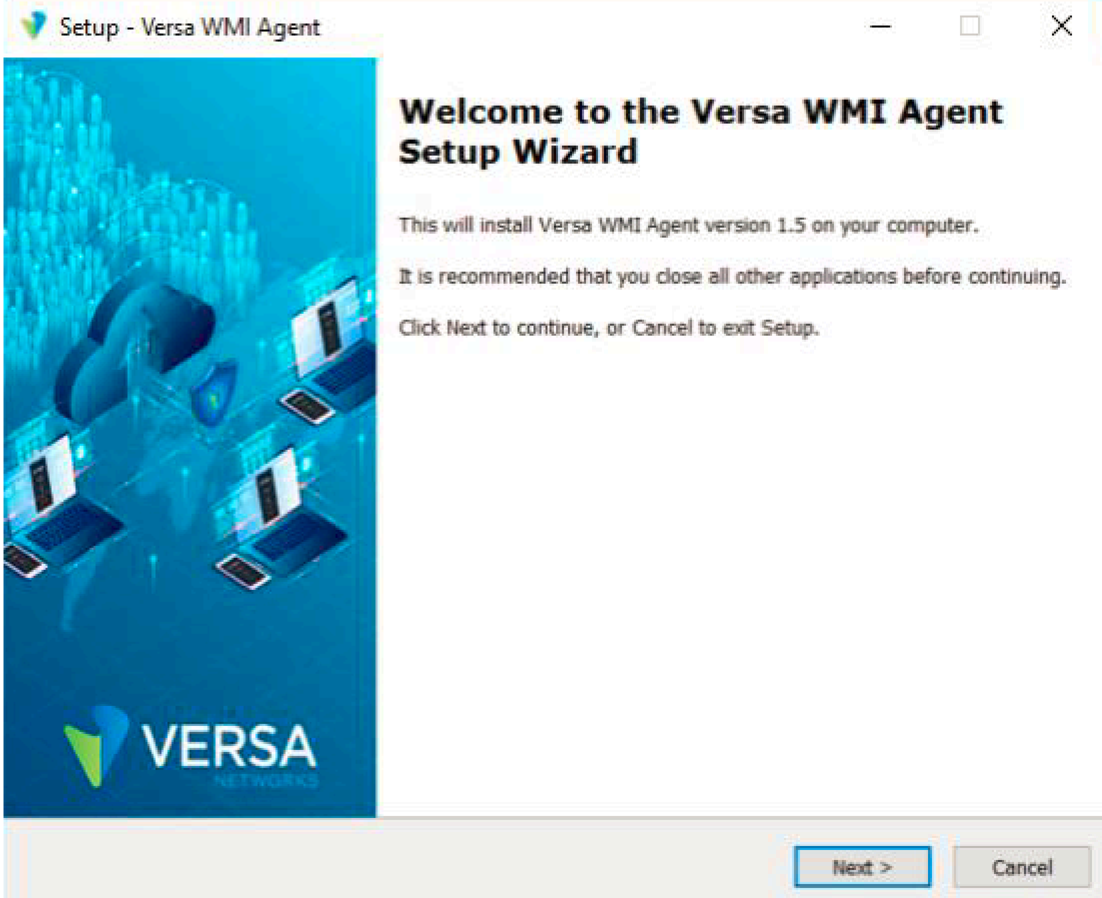
Do you want to allow this app from an unknown publisher to make changes to your device?

VersaWmiAgentInstaller.exe

Publisher: Unknown
File origin: Downloaded from the Internet

Show more details

4. Click Next in all the windows of the WMI agent installation wizard until you finish the installation. The first window of the installation wizard is shown below.



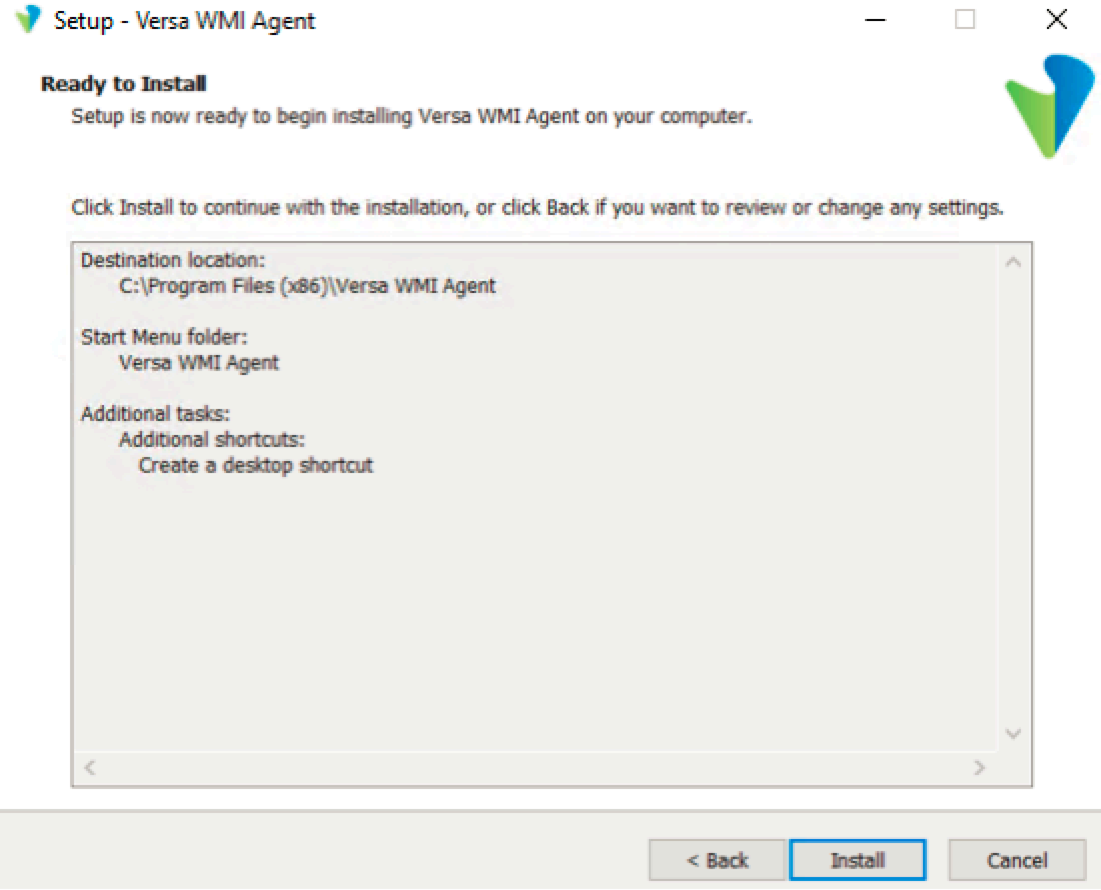
Welcome to the Versa WMI Agent Setup Wizard

This will install Versa WMI Agent version 1.5 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

5. In the Ready to Install window, click Install, and In the last wizard window, click Finish to complete the installation.



Ready to Install

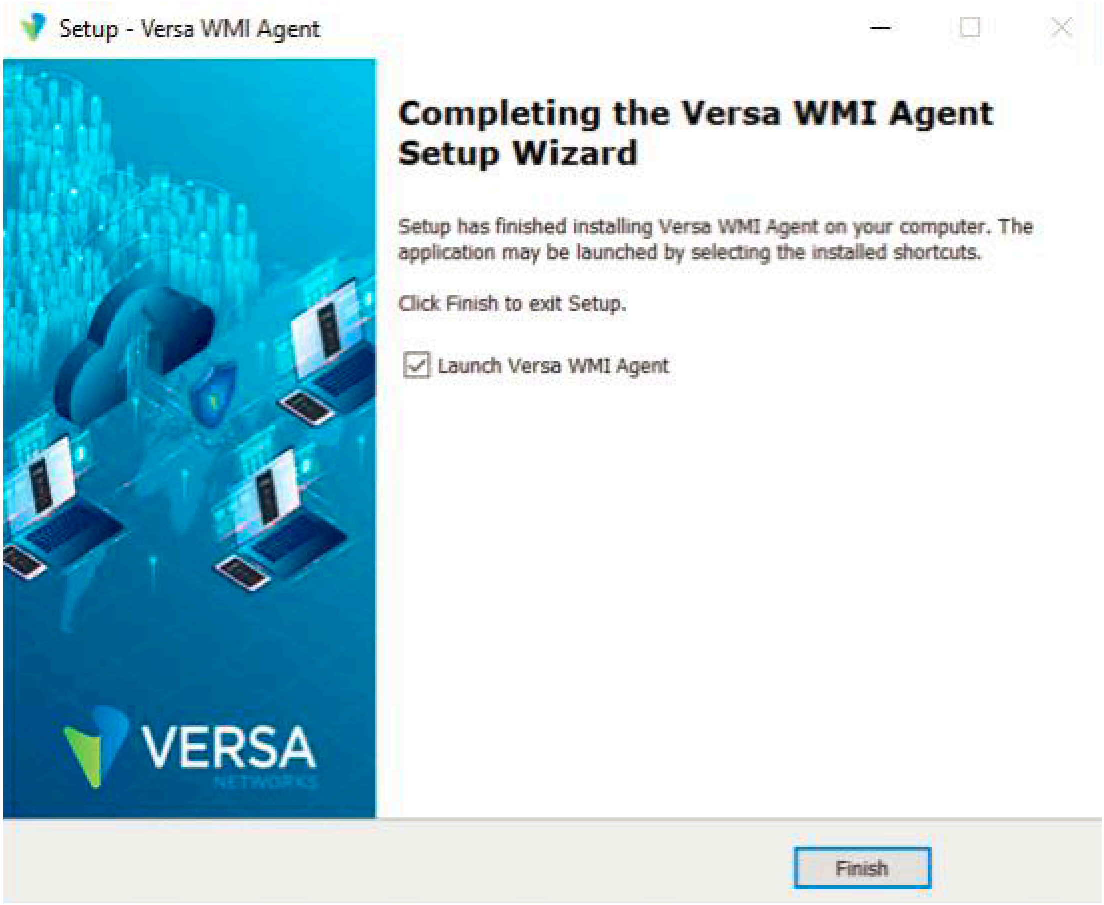
Setup is now ready to begin installing Versa WMI Agent on your computer.

Click Install to continue with the installation, or click Back if you want to review or change any settings.

```
Destination location:
    C:\Program Files (x86)\Versa WMI Agent

Start Menu folder:
    Versa WMI Agent

Additional tasks:
    Additional shortcuts:
      Create a desktop shortcut
```



Completing the Versa WMI Agent Setup Wizard

Setup has finished installing Versa WMI Agent on your computer. The application may be launched by selecting the installed shortcuts.

Click Finish to exit Setup.

☑ Launch Versa WMI Agent

After you click Finish, the WMI agent launches.

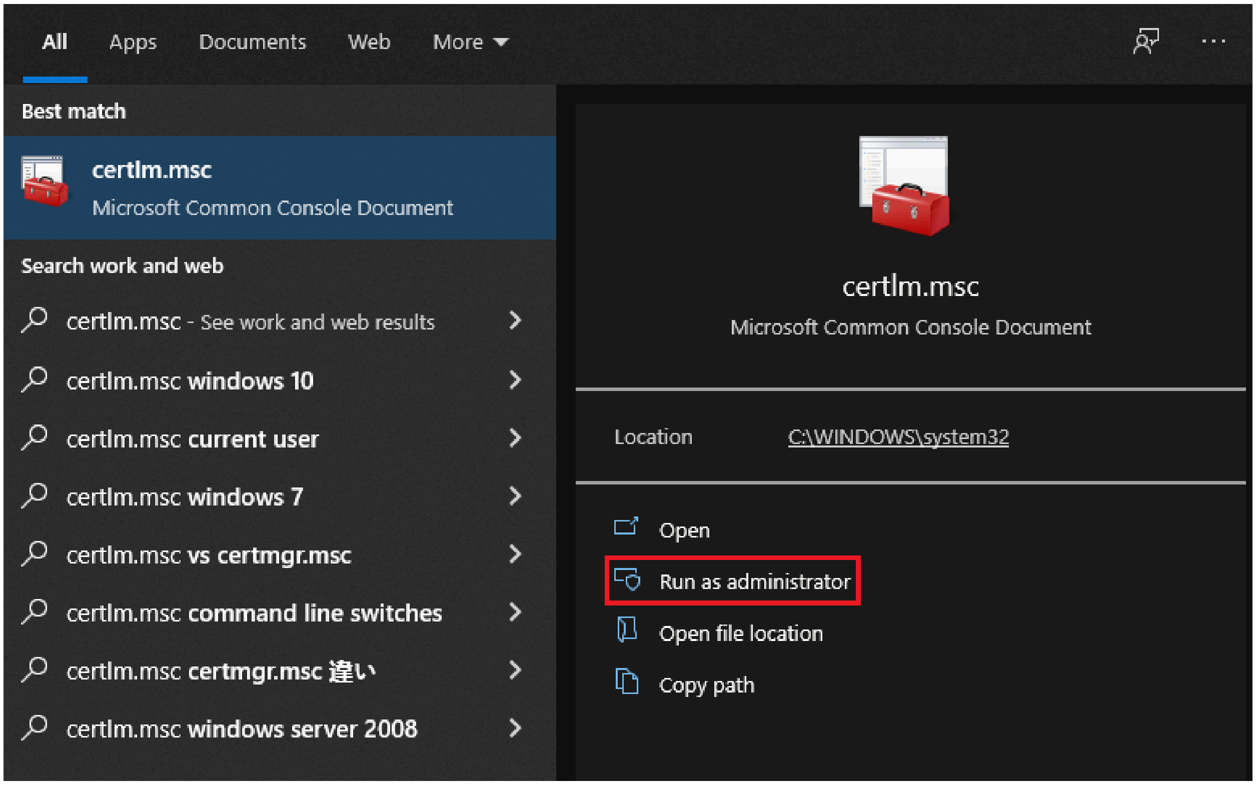
Install the WMI Certificate Files

You must install two certificate files on the device running the WMI agent:

- root-ca-cert.pem—Root certificate file. This file is created on the VMS message-streaming server and is placed in the /opt/versa/vms/certs/ directory. You must install this certificate file on the device running the WMI agent before you install the WMI agent.
- client-cert.pfx—Client certificate file. This file is located in the /opt/versa/vms/certs/ directory on the VMS message-streaming server. You install this certificate file on the device running the WMI agent after you install the WMI agent.

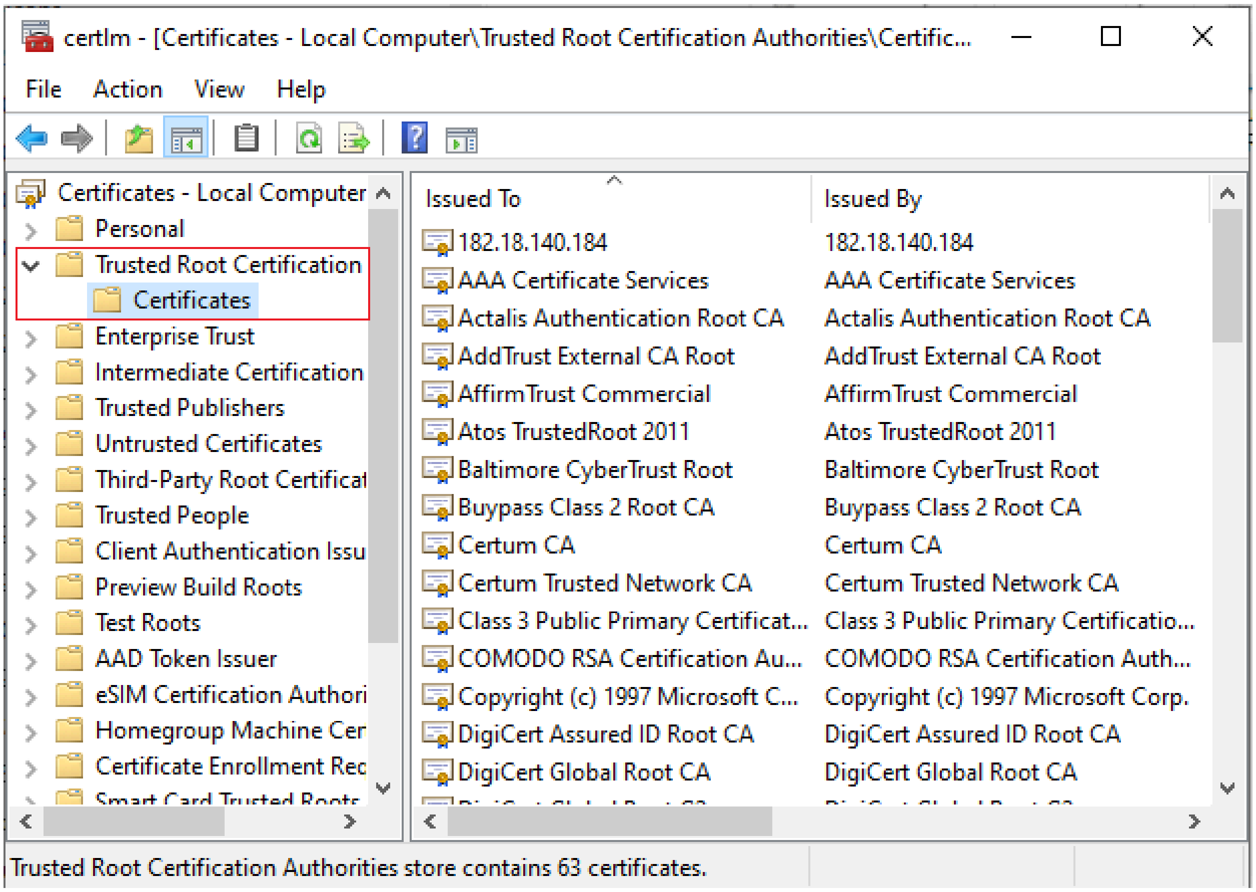
To install the root-ca-cert.pem certificate file on the device running the WMI agent:

1. Copy the root-ca-cert.pem certificate file from the /opt/versa/vms/certs/ folder on the VMS message-streaming server. For more information, see Install the Versa Messaging Service.
2. On your Windows device, open certlm.msc and select Run as Administrator.



All
Apps
Documents
Web
More
Best match
certlm.msc
Microsoft Common Console Document
Search work and web
certlm.msc - See work and web results
certlm.msc windows 10
certlm.msc current user
certlm.msc windows 7
certlm.msc vs certmgr.msc
certlm.msc command line switches
certlm.msc certmgr.msc 違い
certlm.msc windows server 2008
certlm.msc
Microsoft Common Console Document
Location
C:\WINDOWS\system32
Open
Run as administrator
Open file location
Copy path

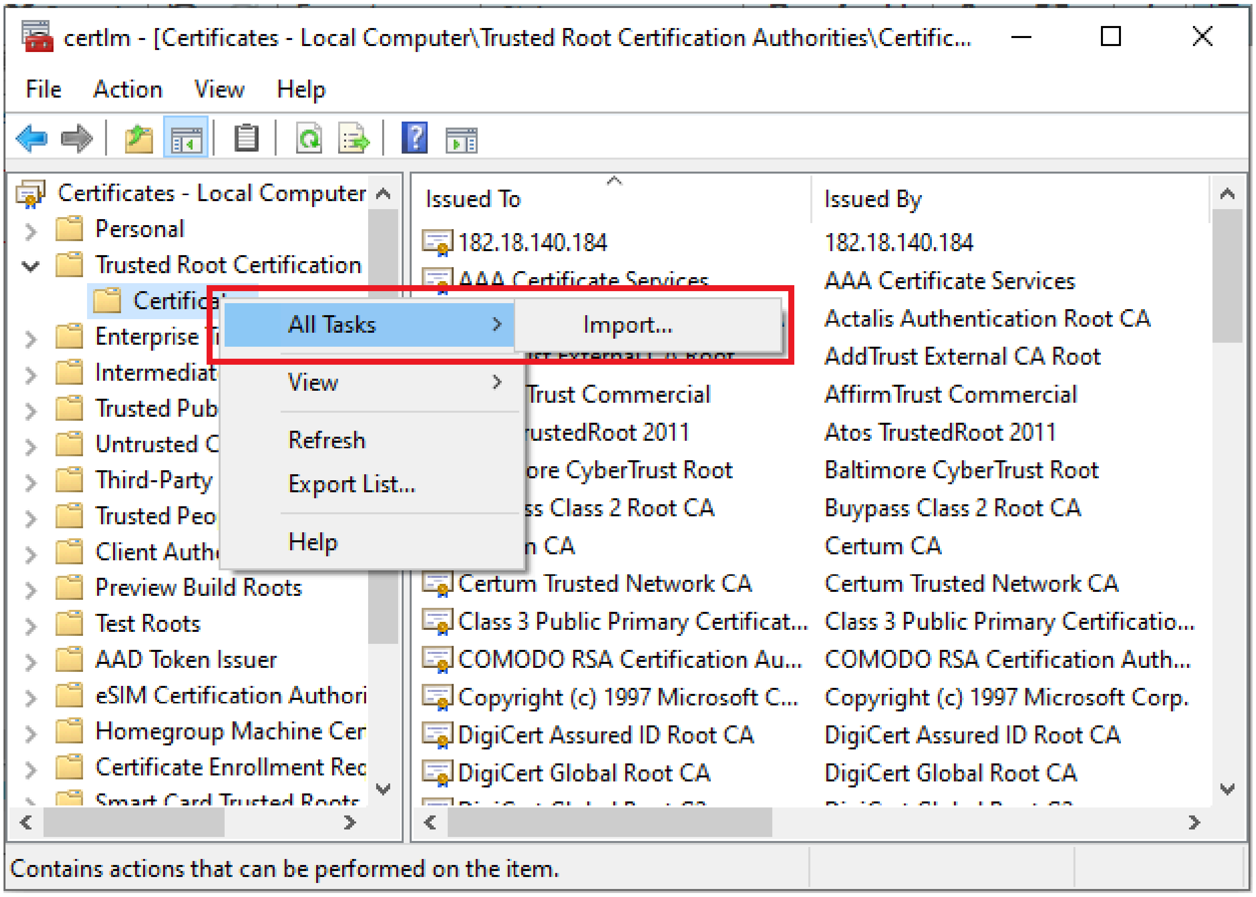
3. In the certlm popup window, select Trusted Root Certification Authorities > Certificates.


certlm - [Certificates - Local Computer\Trusted Root Certification Authorities\Certific...
File
Action
View
Help
Certificates - Local Computer
Personal
Trusted Root Certification
Certificates
Enterprise Trust
Intermediate Certification
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificat
Trusted People
Client Authentication Issu
Preview Build Roots
Test Roots
AAD Token Issuer
eSIM Certification Authori
Homegroup Machine Cer
Certificate Enrollment Rec
Smart Card Trusted Roots

Issued To	Issued By
182.18.140.184	182.18.140.184
AAA Certificate Services	AAA Certificate Services
Actalis Authentication Root CA	Actalis Authentication Root CA
AddTrust External CA Root	AddTrust External CA Root
AffirmTrust Commercial	AffirmTrust Commercial
Atos TrustedRoot 2011	Atos TrustedRoot 2011
Baltimore CyberTrust Root	Baltimore CyberTrust Root
Buypass Class 2 Root CA	Buypass Class 2 Root CA
Certum CA	Certum CA
Certum Trusted Network CA	Certum Trusted Network CA
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...
COMODO RSA Certification Au...	COMODO RSA Certification Auth...
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA
DigiCert Global Root CA	DigiCert Global Root CA

Trusted Root Certification Authorities store contains 63 certificates.

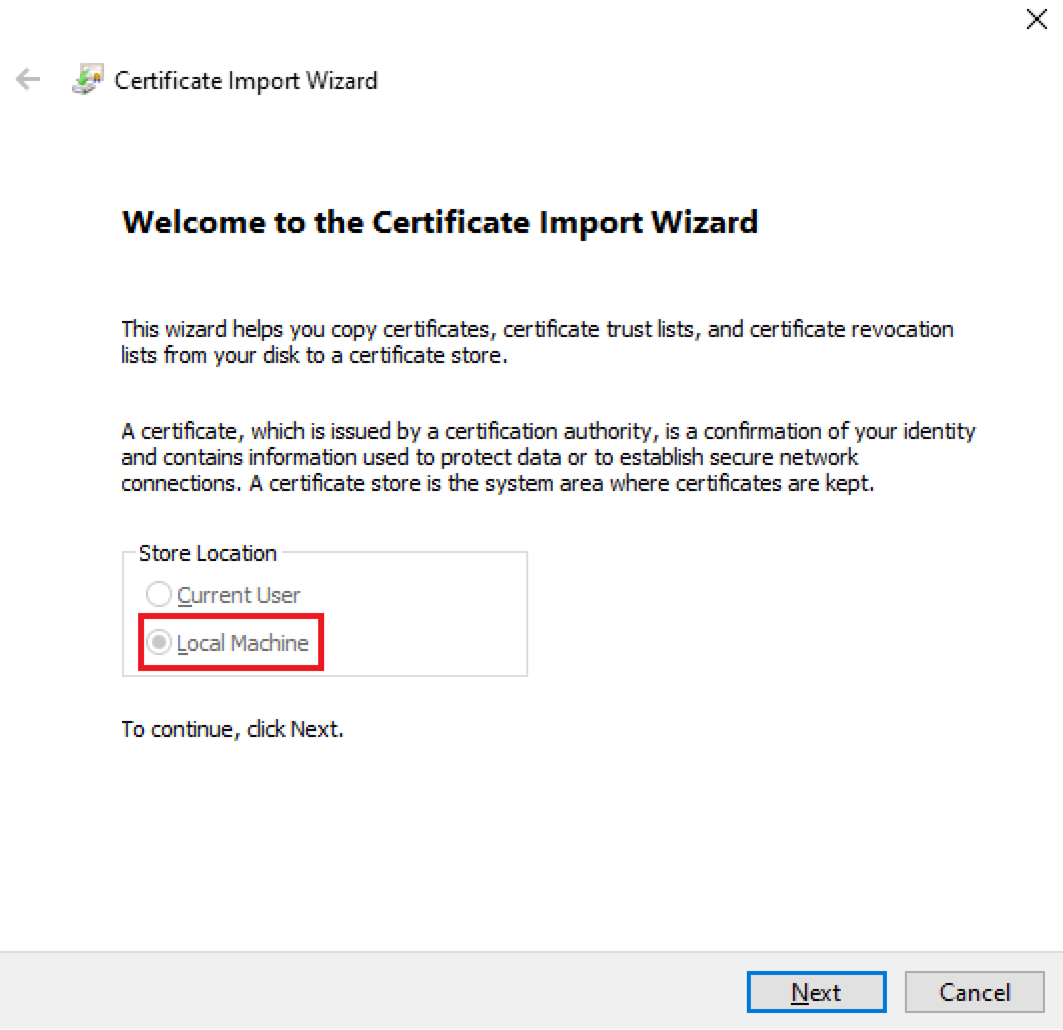
4. Right-click Certificates, select All Tasks, and click Import.



Issued To	Issued By
182.18.140.184	182.18.140.184
AAA Certificate Services	AAA Certificate Services
	Actalis Authentication Root CA
ust External CA Root	AddTrust External CA Root
Trust Commercial	AffirmTrust Commercial
ustedRoot 2011	Atos TrustedRoot 2011
ore CyberTrust Root	Baltimore CyberTrust Root
ss Class 2 Root CA	Buypass Class 2 Root CA
n CA	Certum CA
Certum Trusted Network CA	Certum Trusted Network CA
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...
COMODO RSA Certification Au...	COMODO RSA Certification Auth...
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA
DigiCert Global Root CA	DigiCert Global Root CA

Contains actions that can be performed on the item.

5. In the Certificate Import Wizard popup window, click Local Machine (default) under Store Location and click Next.



Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

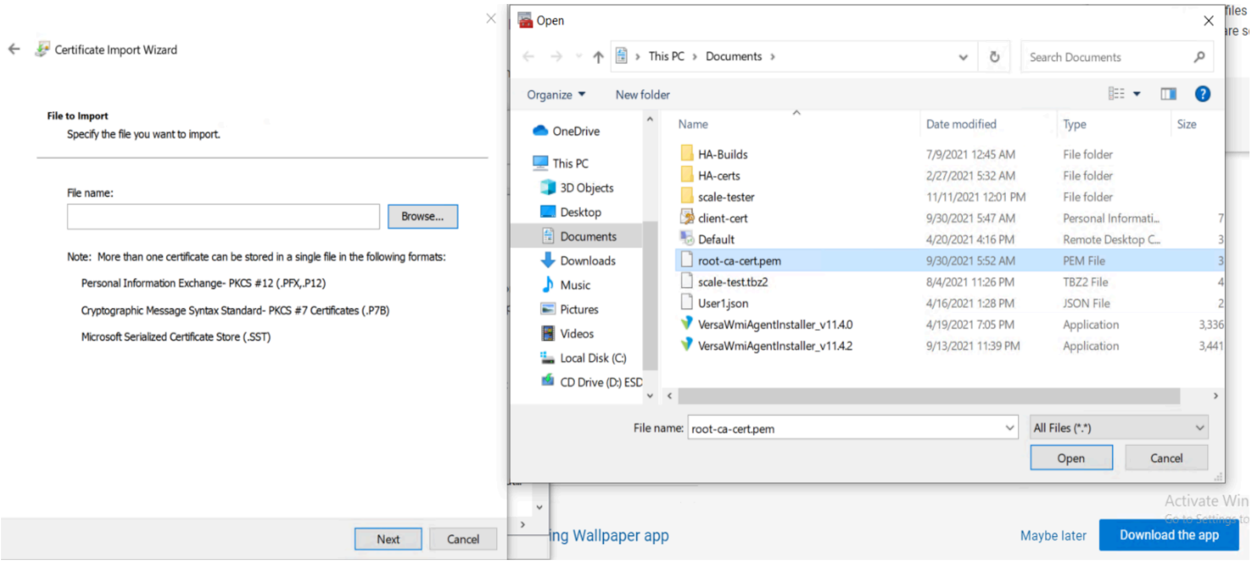
Store Location

○ Current User

● Local Machine

To continue, click Next.

6. In the File to Import window, click Browse and select the root-ca-cert.pem certificate from the location where you saved the file.



File to Import

Specify the file you want to import.

File name:

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

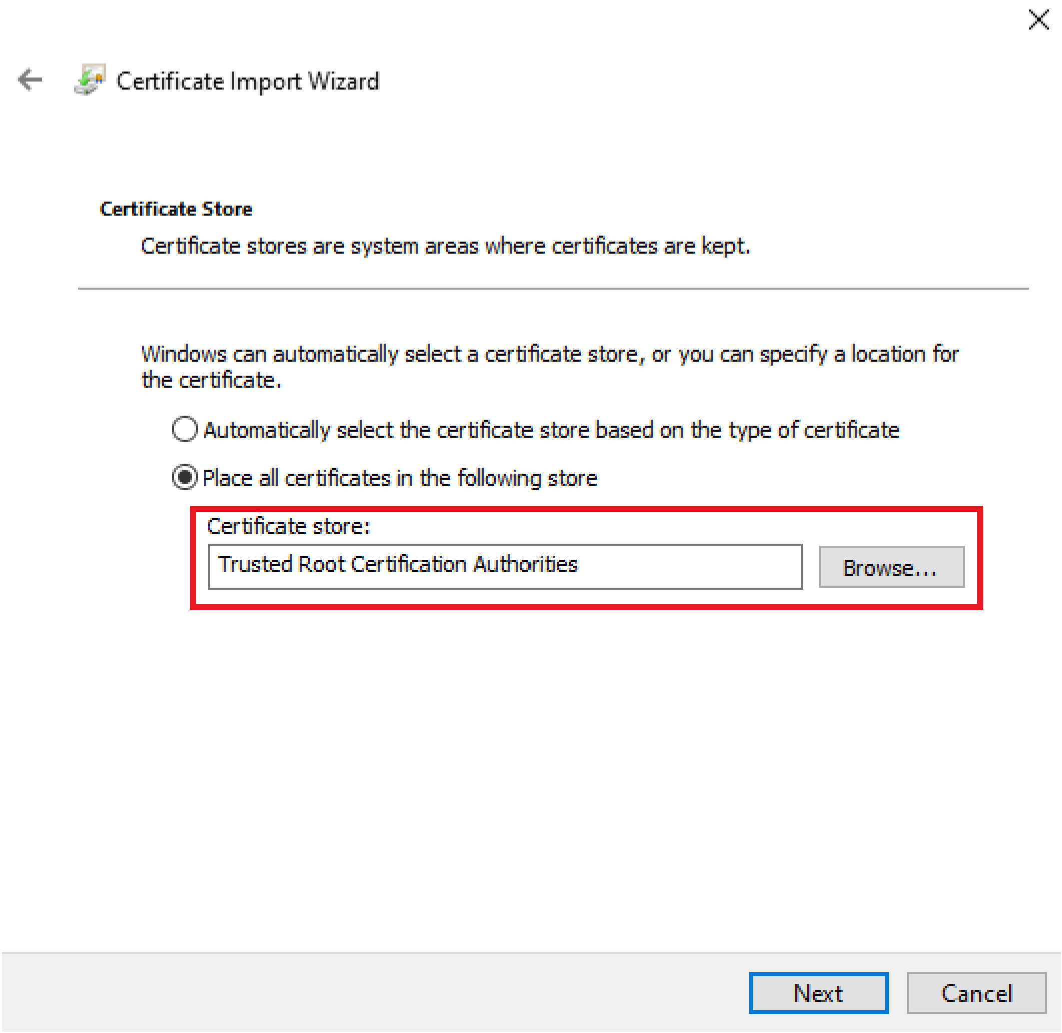
Microsoft Serialized Certificate Store (.SST)

Name	Date modified	Type	Size
HA-Builds	7/9/2021 12:45 AM	File folder	
HA-certs	2/27/2021 5:32 AM	File folder	
scale-tester	11/11/2021 12:01 PM	File folder	
client-cert	9/30/2021 5:47 AM	Personal Informati...	7
Default	4/20/2021 4:16 PM	Remote Desktop C...	3
root-ca-cert.pem	9/30/2021 5:52 AM	PEM File	3
scale-test.tbz2	8/4/2021 11:26 PM	TBZ2 File	4
User1.json	4/16/2021 1:28 PM	JSON File	2
VersaWmiAgentInstaller_v11.4.0	4/19/2021 7:05 PM	Application	3,336
VersaWmiAgentInstaller_v11.4.2	9/13/2021 11:39 PM	Application	3,441

File name: root-ca-cert.pem

All Files (*.*)

7. Click Next.
8. In the Certificate Store window, click Place All Certificates in the Following Store (Default) and select Trusted Root Certification Authorities (Default).



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

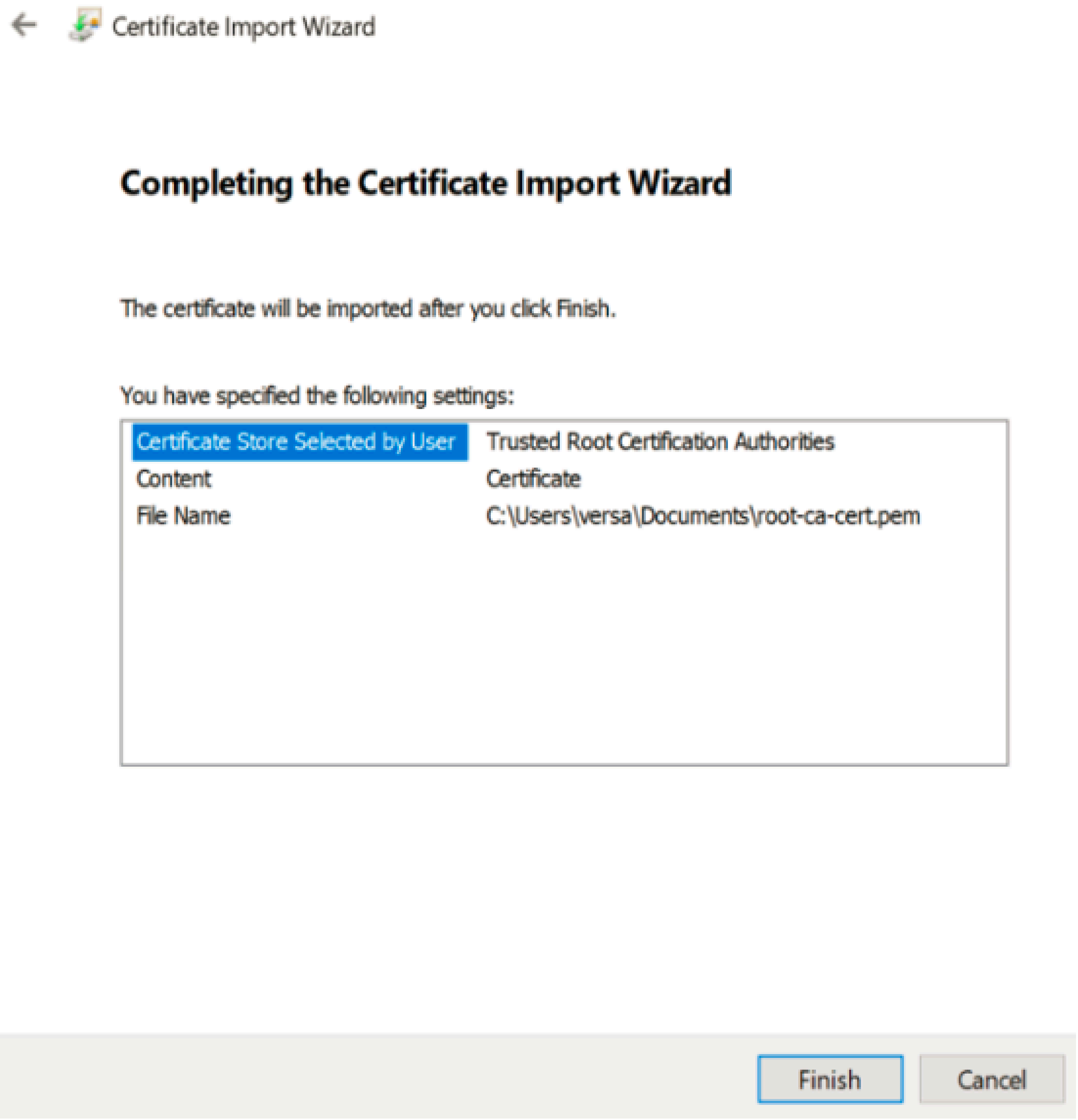
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

9. Click Next and then click Finish in the final window of the wizard.



Certificate Import Wizard

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate
File Name	C:\Users\versa\Documents\root-ca-cert.pem

To install the client-cert.pfx certificate file on the device running the WMI agent:

1. Copy the WMI certificates from the /opt/versa/vms/certs/ folder on the VMS message-stream server. For more information, see Install the Versa Messaging Service.
2. After you install the WMI agent, click the VMS tab.
3. Click Import Client Certificate and select the client-cert.pfx certificate file that you copied from the VMS message-streaming server. For more information, see Step 4 in Configure a VMS Server, below.

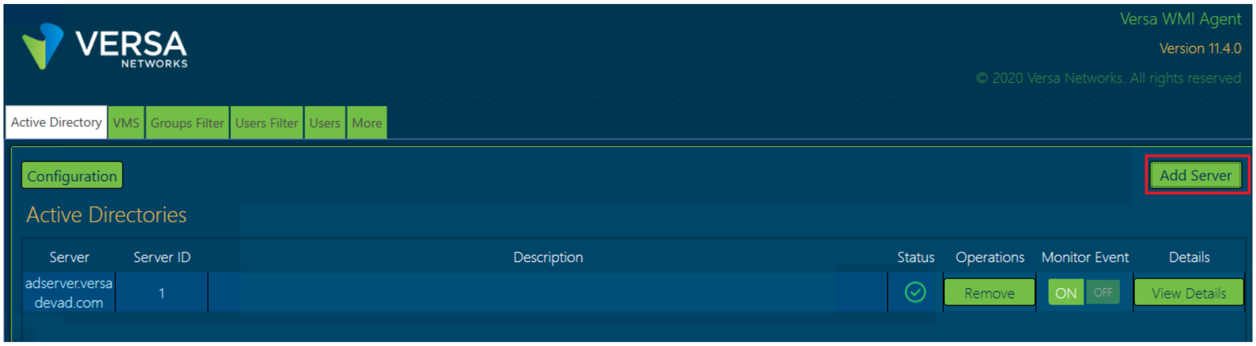
Configure the WMI Agent

After you install the WMI agent, you configure the Active Directory and VMS server details for the WMI agent so that it can receive information from Active Directory and pass it to the VMS server. You can create user groups and user filters to enable or disable monitoring, and you can perform basic troubleshooting from the WMI agent.

Configure the Active Directory Server

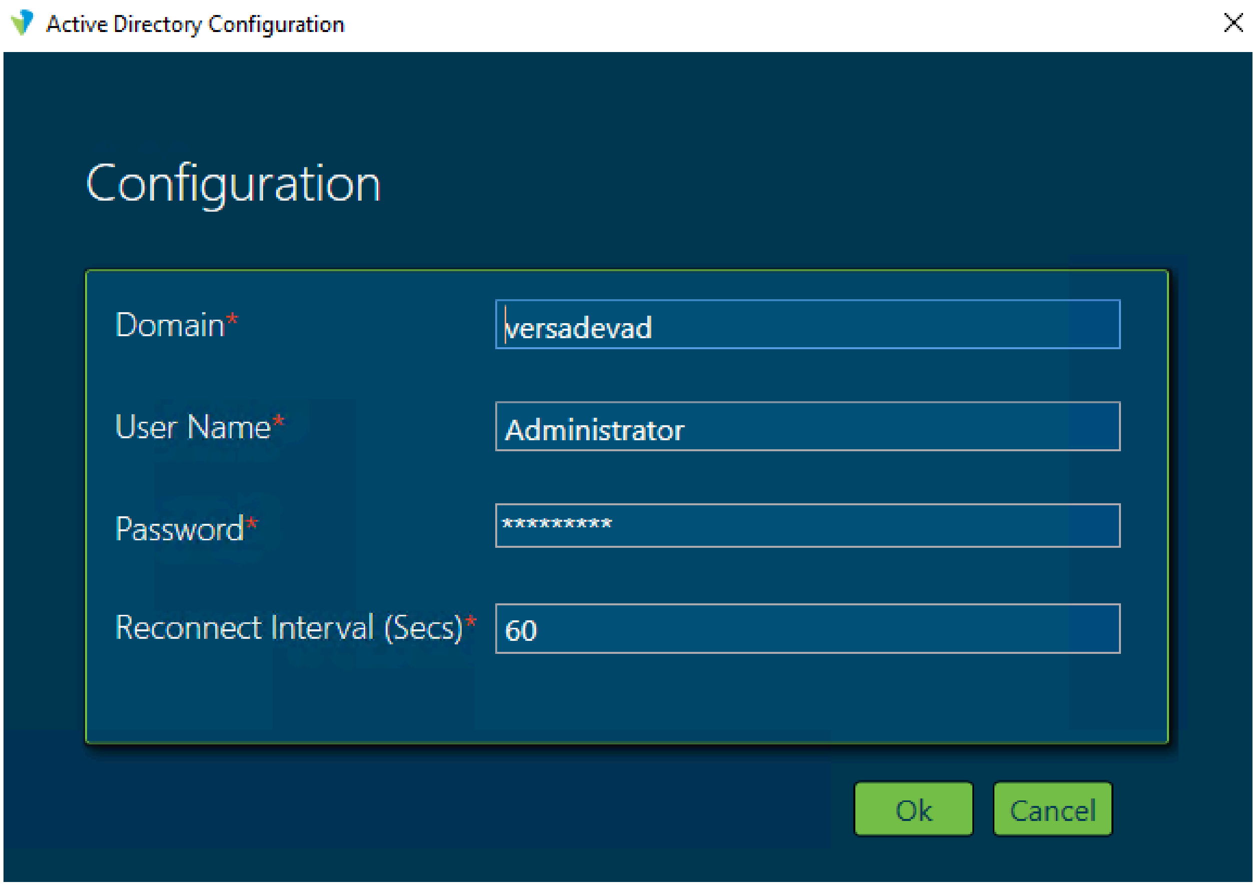
To configure an Active Directory server on the WMI agent:

1. To start the WMI agent, double-click the WMI agent shortcut on the desktop. The Active Directory tab displays.



Server	Server ID	Description	Status	Operations	Monitor Event	Details
adserver.versadevad.com	1		✓	Remove	ON OFF	View Details

2. To configure authentication details for Active Directory, in the Active Directory tab, click Configuration to update the WMI agent Active Directory configuration. Enter information for the following fields.



Active Directory Configuration

Configuration

Domain* versadevad

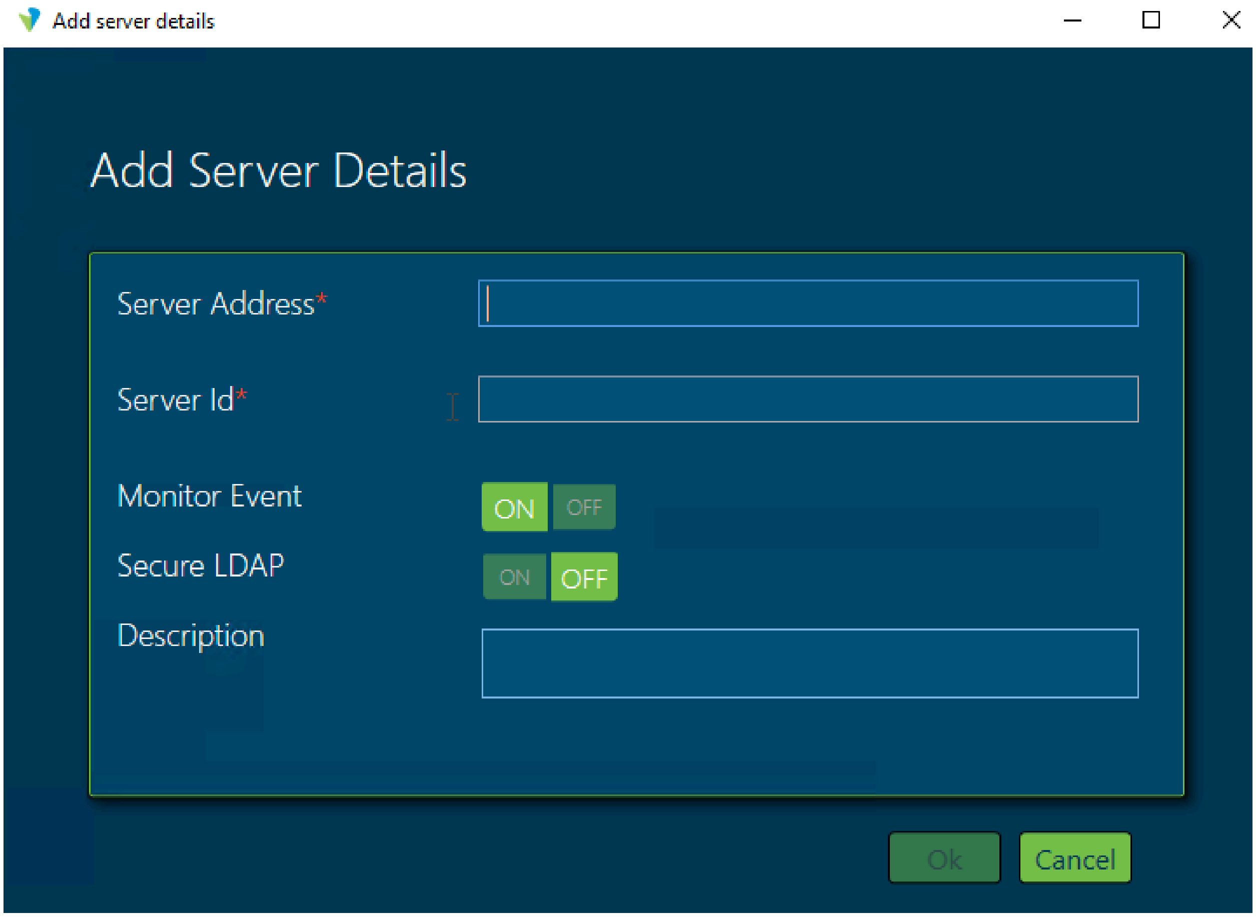
User Name* Administrator

Password* **********

Reconnect Interval (Secs)* 60

Field	Description
Domain (Required)	Enter the name of the organization domain configured on the Active Directory server.
Username (Required)	Enter the username to log in to the Active Directory server. If the user has Administrator privileges on the Active Directory server, they can perform all operations. If the user does not have Administrator privileges on the Active Directory server, they can access event logs. For more information, see Create a Non-Administrator User To Access Event Logs, below.
Password	Enter the password to log in to the Active Directory server.
Reconnect Interval (Required)	Enter the time, in seconds, after which the WMI agent tries to reconnect to the Active Directory server after reconnection failures. The WMI agent attempts reconnections until the connection is re-established. *Value*: 1 through 1800 seconds *Default*: 10 seconds

3. Click OK.
4. Click Add Server to enter the active directory server details. In the Active Directory Configuration popup window, enter information for the following fields.



Add server details

Add Server Details

Server Address*

Server Id*

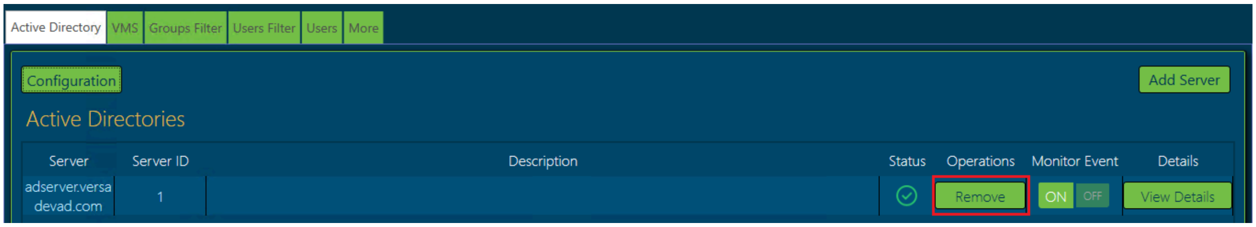
Monitor Event: ON

Secure LDAP: OFF

Description

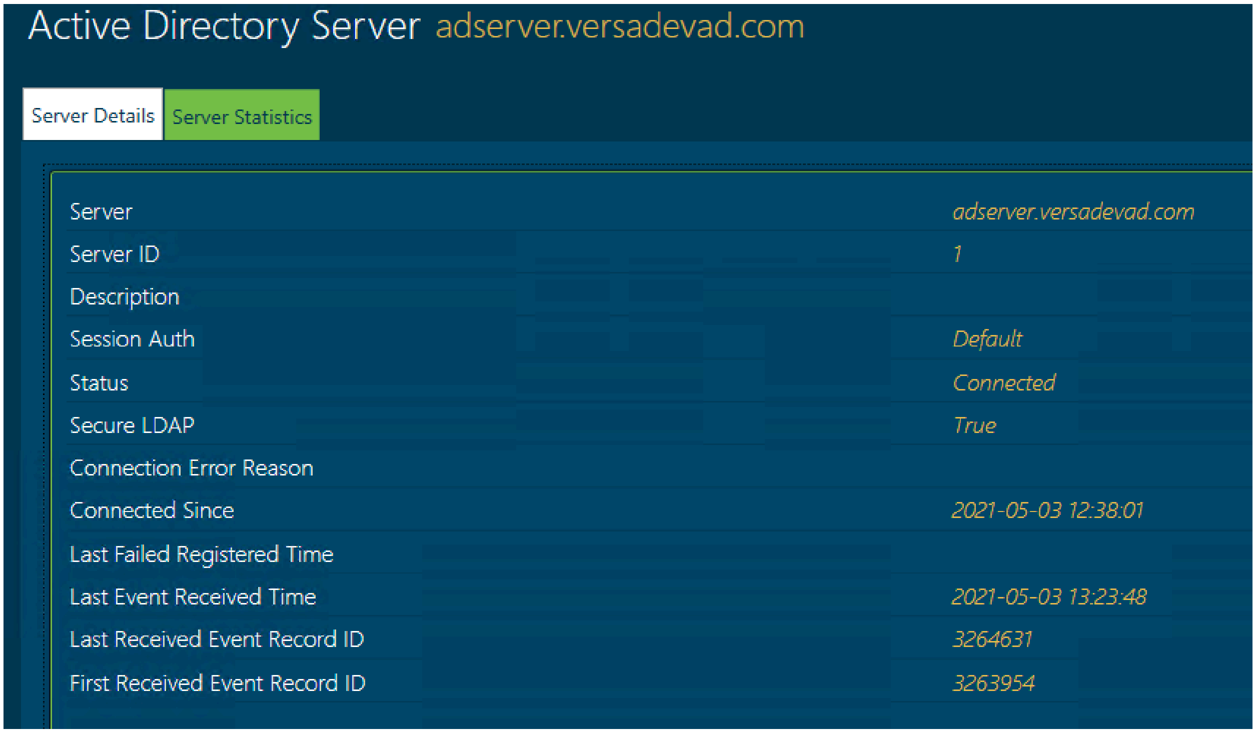
Field	Description
Server Address (Required)	Enter the IP address of the Active Directory server to which the WMI agent connects.
Server ID (Required)	Enter the identifier of the Active Directory server.
Monitor Event	Click On to enable event monitoring of the Active Directory server on the WMI agent. This provides monitoring of connection errors and other debugging. It is recommended that you enable event monitoring.
Secure LDAP	Click On to enable secure LDAP query. The WMI agent fetches the principal user name using LDAP query. For more information, see Configure a VMS Server below. *Default*: Off
Description	Enter a description for the Active Directory server.

5. Click OK.
6. To delete an Active Directory server record, click Remove in the Active Directory tab:



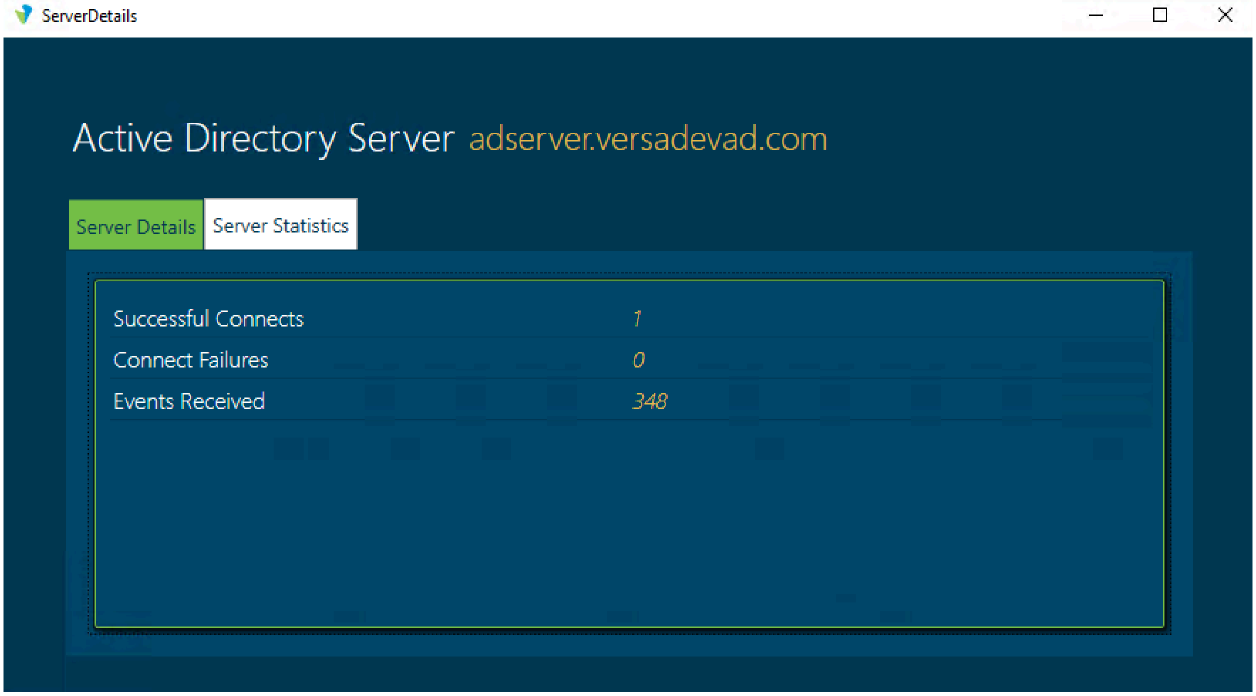
Server	Server ID	Description	Status	Operations	Monitor Event	Details
adserver.versadevad.com	1		✓	Remove	ON OFF	View Details

To display information about the Active Directory server, click View Details for the Active Directory server and then select the Server Details tab. For example:



Server	adserver.versadevad.com
Server ID	1
Description	
Session Auth	Default
Status	Connected
Secure LDAP	True
Connection Error Reason	
Connected Since	2021-05-03 12:38:01
Last Failed Registered Time	
Last Event Received Time	2021-05-03 13:23:48
Last Received Event Record ID	3264631
First Received Event Record ID	3263954

To display statistics about the Active Directory server, click View Details for the Active Directory server and then select the Server Statistics tab. For example:



Successful Connects	1
Connect Failures	0
Events Received	348

Create a Non-Administrator User To Access Event Logs

By default, an Administrator user can perform all operations on the Active Directory server. If you want to allow a non-Administrator user to access the event logs on the Active Directory server, you create a user who has access to the built-in Active Director groups and configure security settings to allow the groups to access Active Director server and all name spaces.

To create a new user and add the user to predefined Active Director built-in groups:

1. On the Active Director Server, add a new user (For example, event-auditor)
2. In the Active Director domain, click Builtin.
3. In the right panel, right-click Event Log Readers and then select Add To a Group.
4. In the Enter the object names to select field, enter the username you created in Step 1.
5. Click Check Names, and then click OK.
6. In the Active Director domain, click Builtin.
7. In the right panel, right click Distributed COM Users and then select Add To a Group.
8. In the Enter the object names to select field, enter the username you created in Step 1.
9. Click Check Names, and then click OK.

To configure the Distributed COM security settings to allow the groups to access the system remotely:

1. Click Start > Run.
2. Enter dcomcnfg, and then click OK.
3. Drill down in the Component Services tree until you get to My Computer.
4. Right-click My Computer, and in the menu, click Properties.
5. Select the COM Security tab.
6. In the Launch and Activation Permissions section, click Edit Limits.
7. Click Add.
8. In the Enter the object names to select field, enter the string Distributed COM Users.
9. Click Check Names, and then click OK.
10. Click Add.
11. Repeat Steps 5 through 10 for the Performance Monitor Users group.
12. For each of the permissions (Local Launch, Remote Launch, Local Activation, Remote Activation) for each group, check Allow
13. Click OK.

Finally, to enable OpManager to fetch the data using WMI, you provide access for all classes under all namespaces for both the user groups. To set the WMI control security settings so that they apply to all namespaces:

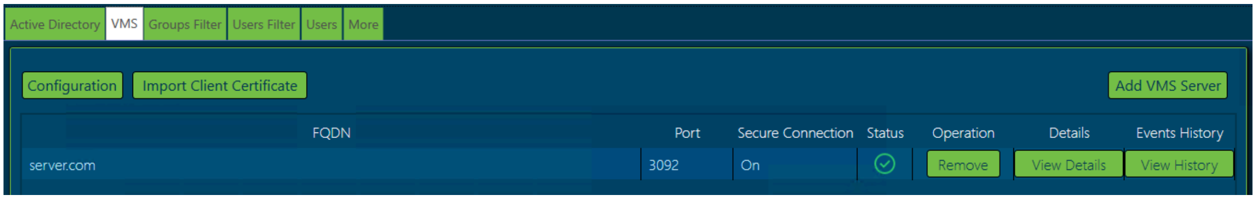
1. Click Start > Run.
2. Enter wmimgmt.msc, and then click OK.
3. Right-click WMI Control (Local), and in the menu, click Properties.

4. Click over to the Security tab, click Root, and then click Security.
5. Click Add.
6. In the Enter the object names to select field, enter the string Distributed COM Users.
7. Click Check Names, and then click OK.
8. Ensure that the Distributed COM Users group is selected, and then click Advanced.
9. Highlight the row with Distributed COM Users in it and click Edit.
10. In the Applies to field, select This namespace and subnamespaces.
11. In the Allow column, check Execute Methods, Enable Account and Remote Enable.
12. Click OK.
13. Repeat Steps 4 through 12 for the Performance Monitor Users group.

Configure a VMS Server

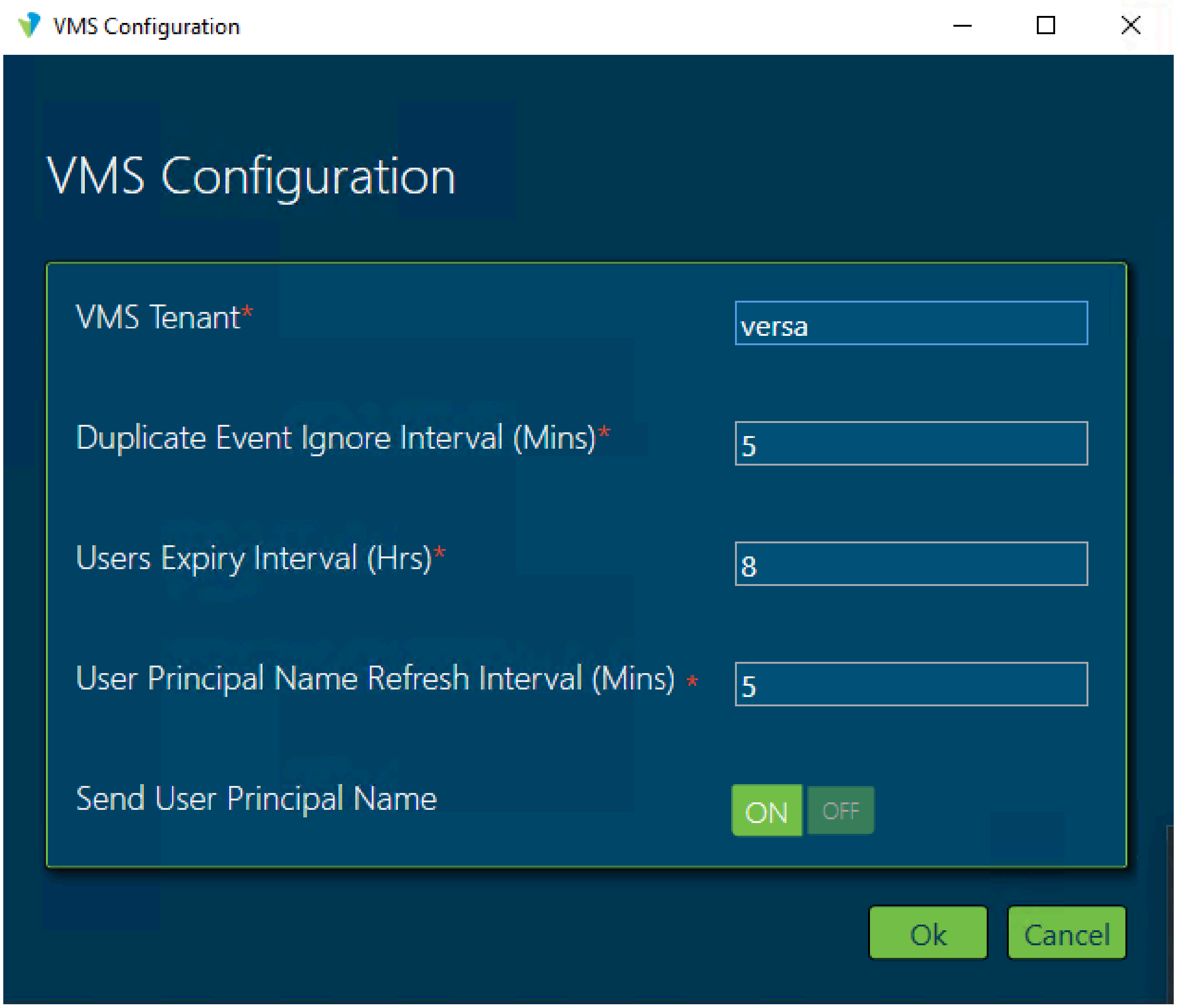
To configure a VMS server for the WMI agent:

1. In the WMI agent main window, select the VMS tab.



FQDN	Port	Secure Connection	Status	Operation	Details	Events History
server.com	3092	On	✓	Remove	View Details	View History

2. In the VMS tab, click Configuration to configure VMS server details to send data to VMS. In the VMS Configuration popup window, enter information for the following fields.



VMS Configuration

VMS Tenant*: versa

Duplicate Event Ignore Interval (Mins)*: 5

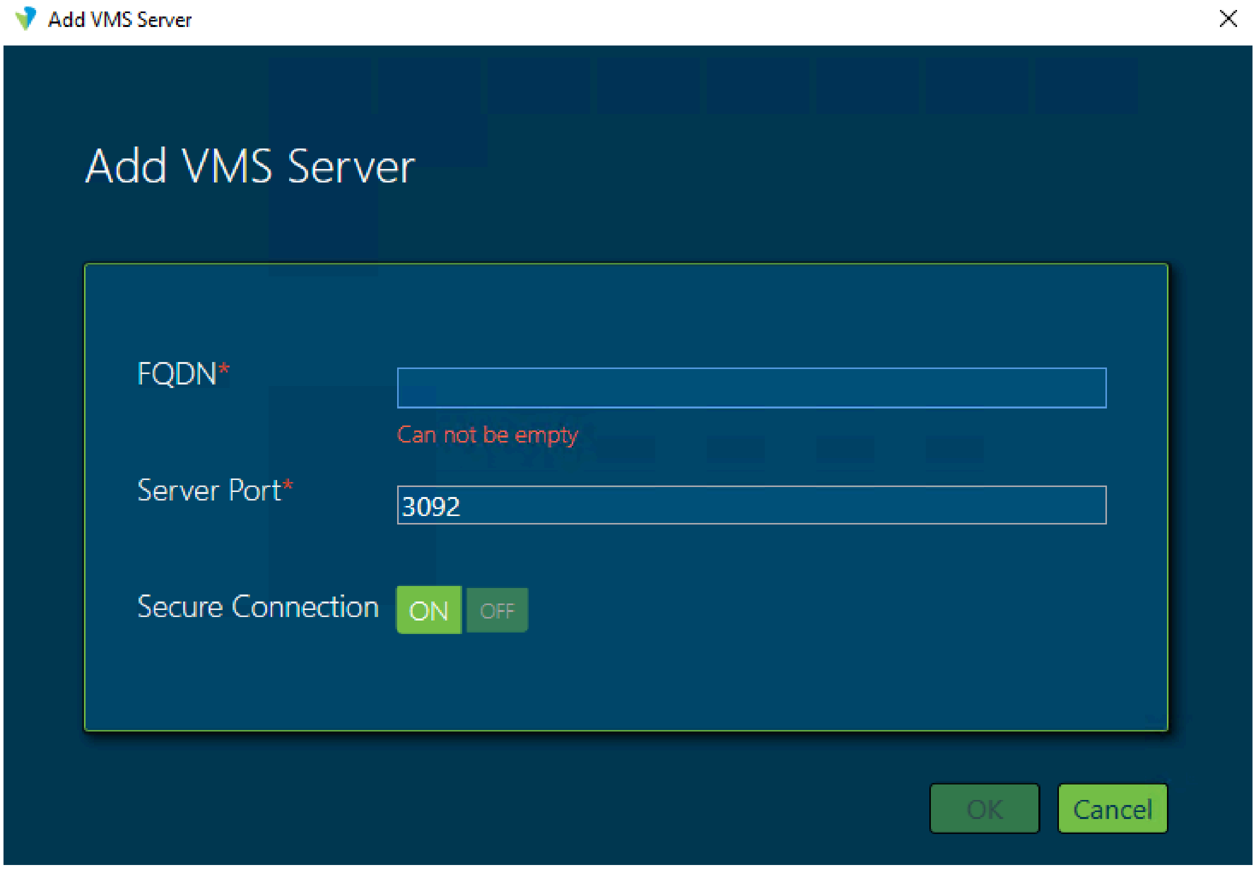
Users Expiry Interval (Hrs)*: 8

User Principal Name Refresh Interval (Mins) *: 5

Send User Principal Name: ON

Field	Description
VMS Tenant (Required)	Enter the VMS tenant or organization name. This name must match the tenant or organization name on the VOS devices.
Duplicate Event Ignore Interval (Required)	Enter the time, in minutes, after which duplicate user login–related events received from Active Directory servers are ignored. *Value*: 1 through 60 minutes *Default*: 5 minutes
Users Expiry Interval (Required)	Enter the time, in hours, after which user records expire. A user–IP address record is valid on a VOS device until either the device receives a new user–IP address record or the expiration time interval occurs, whichever happens first. *Value*: 1 through 168 hours *Default*: 8 hours
User Principal Name Refresh Interval	Enter the refresh interval, in minutes, to fetch user principal names in order to update with new users or to modify existing user principal names. The user principal name is the fully qualified username for a domain. For example, if domain is xyz-networks.com and username is "testuser," the user principal name is testuser@xyz-networks.com. *Value*: 5 through 60 minutes *Default*: 5 minutes
Send User Principal Name	Click On to send the principal name of the user to the VMS server. *Default*: On

3. Click OK.
4. Click Add VMS Server. In the Add VMS Server popup window, enter information for the following fields.



Add VMS Server

FQDN*

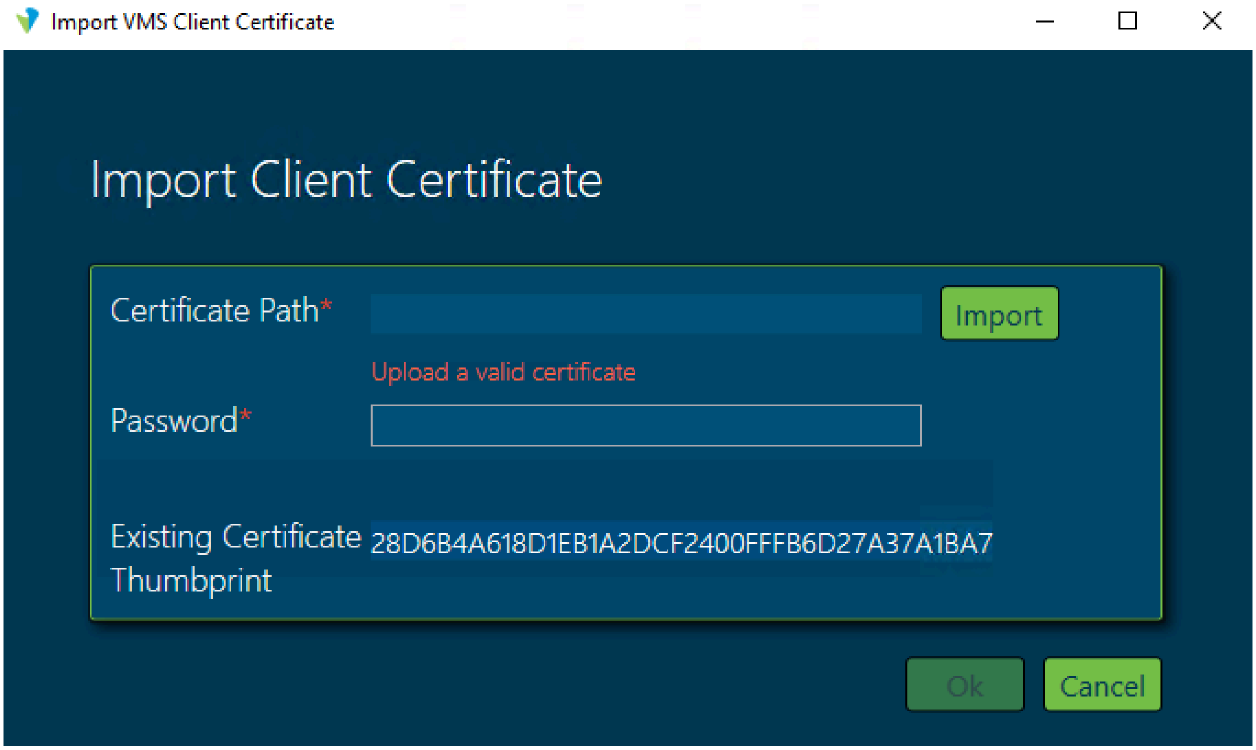
Can not be empty

Server Port* 3092

Secure Connection ON OFF

Field	Description
FQDN (Required)	Enter the fully qualified domain name (FQDN) of the VMS server to which to connect the WMI agent.
Server Port (Required)	Enter the port number of the VMS server. *Value*: 1 through 65535 *Default*: 3092
Secure Connection	Click On to enable secure connection between WMI Agent and VMS server. A secure connection uses HTTPS and a non-secure connection uses HTTP. Secure connection is usually used if the server is configured for two-way authentication, that is, when server and client use authentication. A client certificate is used for client authentication. *Default*: On
Description	Enter a description for the VMS server.

5. Click Ok.
6. To import a client certificate for client authentication, click Import Client Certificate in the VMS tab. The Import VMS Client Certificate popup window displays.
   a. Click Import to select the client certificate from the Windows device to import, or enter the path in the Certificate Path field.
   b. Enter the certificate key-store password.
   c. Click OK.
   d. Copy the client certificate that you set in Step 6a to the Windows machine on which the WMI agent is running. On the VMS server, the client server certificate is located in the directory /opt/versa/vms/certs/, in the file client-cert.pfx. Note that you can only import PFX certificates (.pfx).



Import Client Certificate

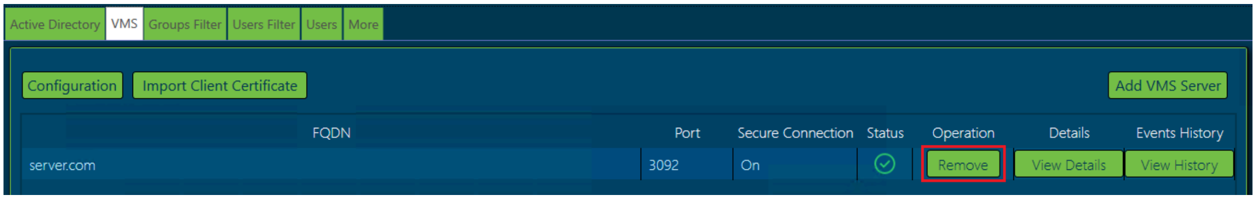
Certificate Path*

Upload a valid certificate

Password*

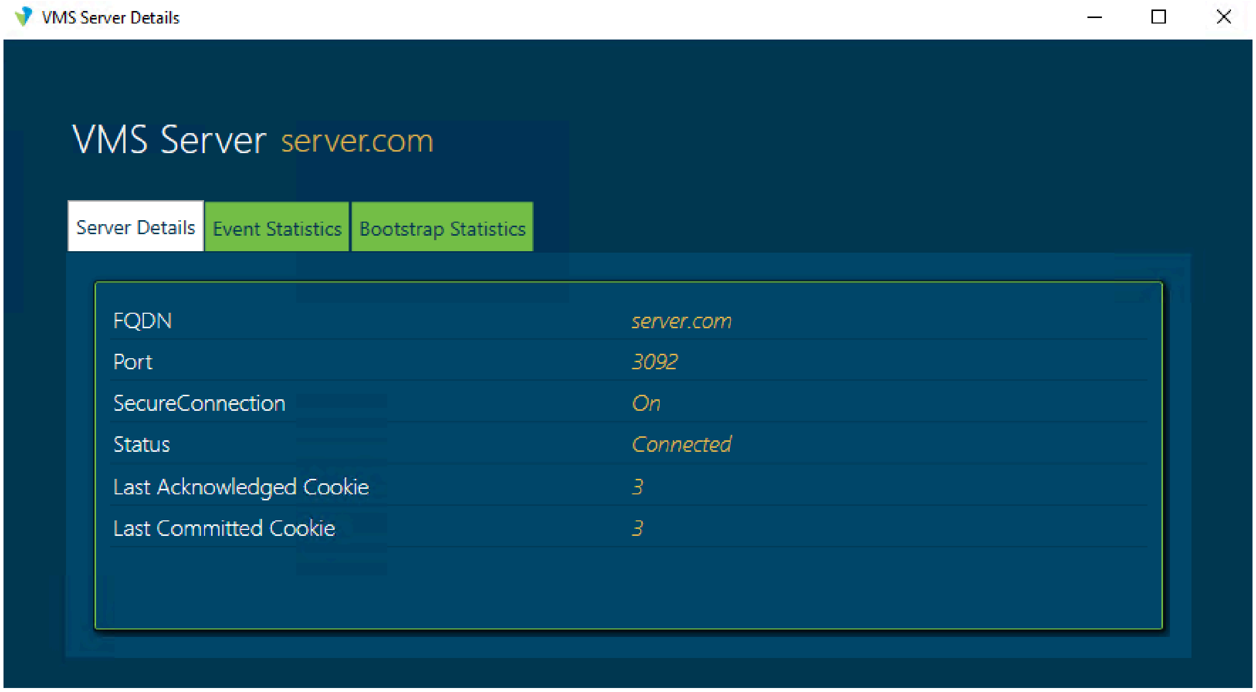
Existing Certificate Thumbprint 28D6B4A618D1EB1A2DCF2400FFFB6D27A37A1BA7

To delete a VMS server record, click Remove in the VMS tab:



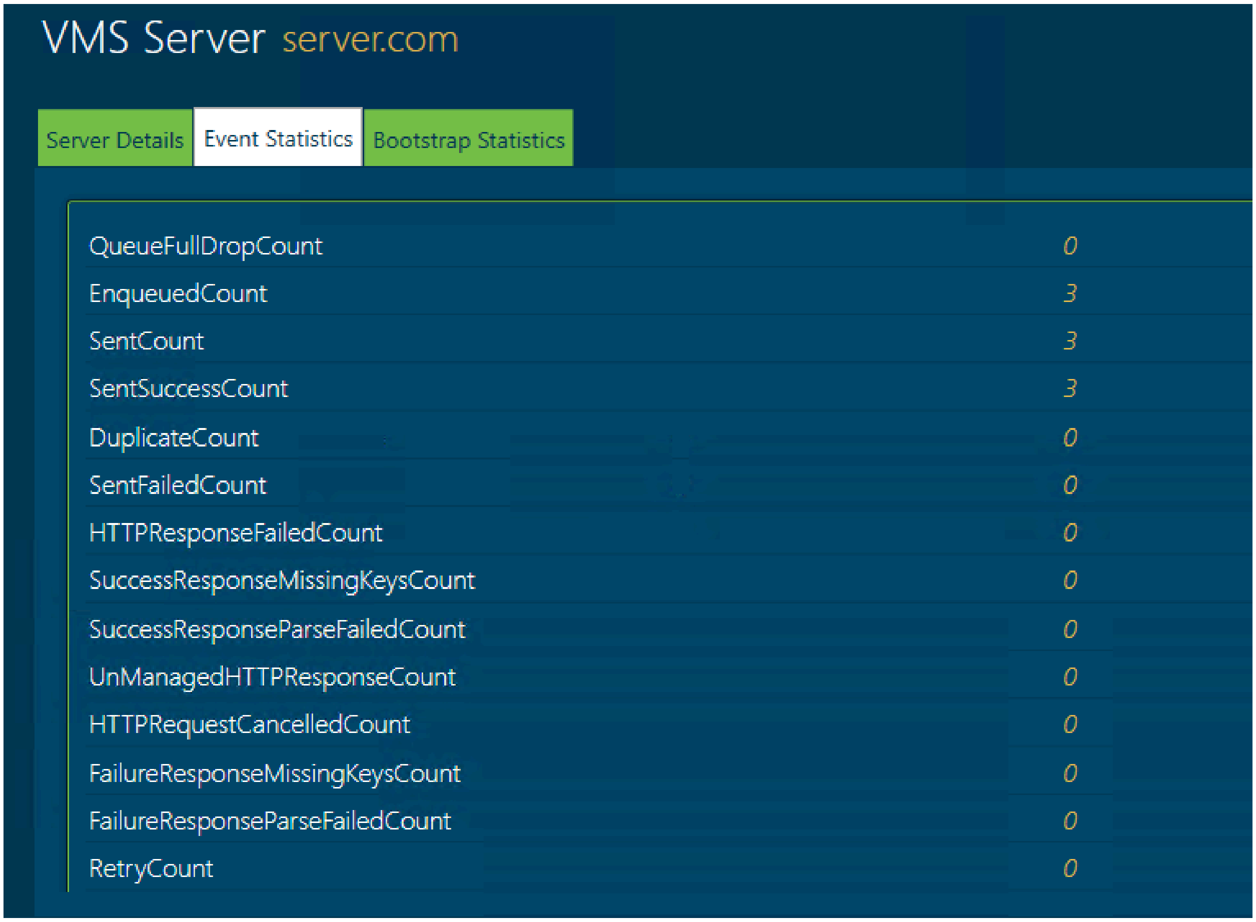
FQDN	Port	Secure Connection	Status	Operation	Details	Events History
server.com	3092	On	✓	Remove	View Details	View History

To display information about the VMS server, click View Details for the VMS server and then select the Server Details tab. For example:



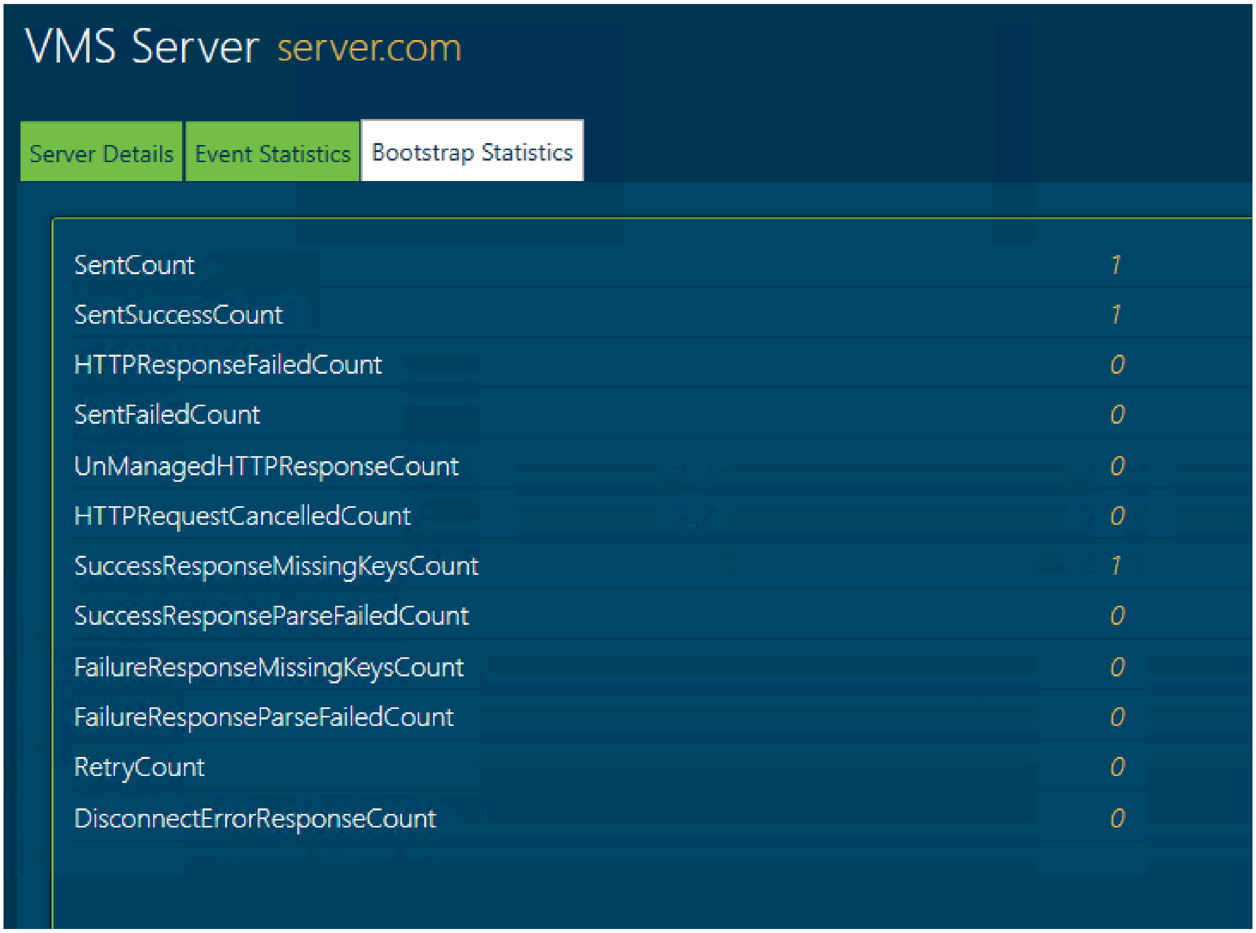
FQDN	server.com
Port	3092
SecureConnection	On
Status	Connected
Last Acknowledged Cookie	3
Last Committed Cookie	3

To display event statistics for the VMS server, click View Details for the VMS server and then select the Event Statistics tab. For example:


VMS Server server.com

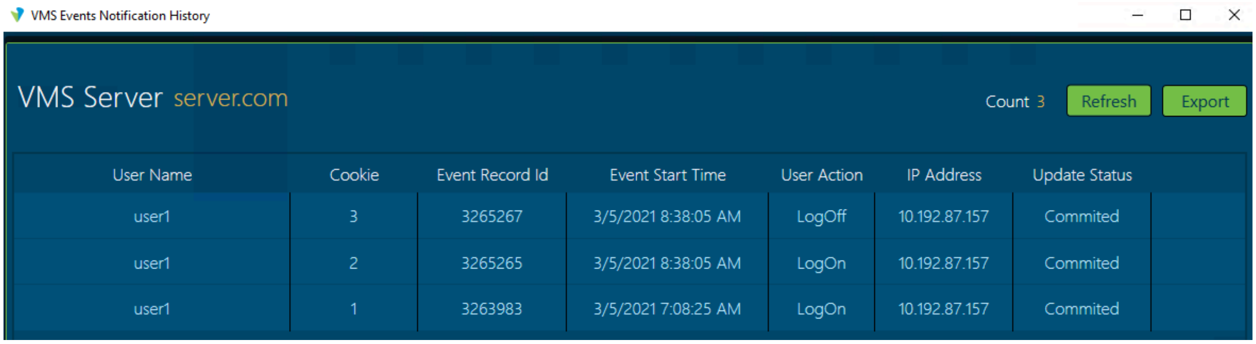
QueueFullDropCount	0
EnqueuedCount	3
SentCount	3
SentSuccessCount	3
DuplicateCount	0
SentFailedCount	0
HTTPResponseFailedCount	0
SuccessResponseMissingKeysCount	0
SuccessResponseParseFailedCount	0
UnManagedHTTPResponseCount	0
HTTPRequestCancelledCount	0
FailureResponseMissingKeysCount	0
FailureResponseParseFailedCount	0
RetryCount	0

To display bootstrap statistics for the VMS server after connection initiates with the server, click View Details for the VMS server and then select the Bootstrap Statistics tab. For example:



SentCount	1
SentSuccessCount	1
HTTPResponseFailedCount	0
SentFailedCount	0
UnManagedHTTPResponseCount	0
HTTPRequestCancelledCount	0
SuccessResponseMissingKeysCount	1
SuccessResponseParseFailedCount	0
FailureResponseMissingKeysCount	0
FailureResponseParseFailedCount	0
RetryCount	0
DisconnectErrorResponseCount	0

To view event history for the VMS server, click View History. For example:



User Name	Cookie	Event Record Id	Event Start Time	User Action	IP Address	Update Status
user1	3	3265267	3/5/2021 8:38:05 AM	LogOff	10.192.87.157	Commited
user1	2	3265265	3/5/2021 8:38:05 AM	LogOn	10.192.87.157	Commited
user1	1	3263983	3/5/2021 7:08:25 AM	LogOn	10.192.87.157	Commited

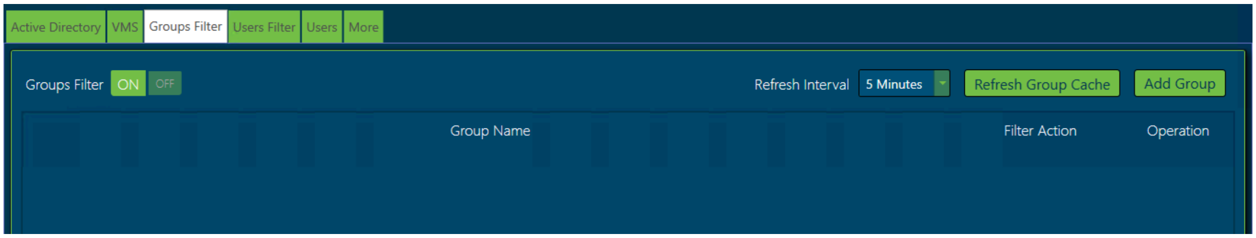
To export the event history records to an Excel (.xls) file, click Export.

Add Group Filters

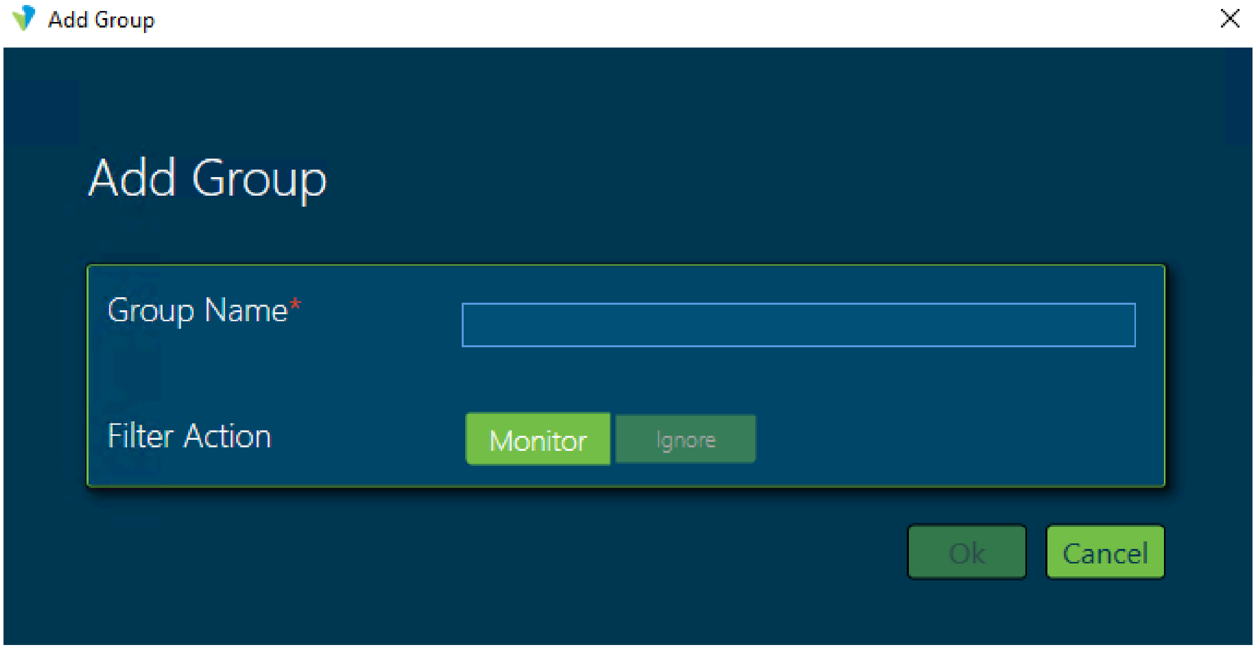
You can create groups that the WMI agent can monitor or not monitor. For example, you can create group filters for sales staff or system administrators.

To create a group and enable group filtering:

1. In the WMI agent main window, select the Groups Filter tab.



2. In the Groups Filter field, click On to enable filtering for the groups that you are when you click the Add Group field on this tab. When you enable group filtering, only groups that you add on this tab are monitored. If you disable group filtering, all groups are monitored. If you enable group filtering and do not add any groups, no user groups are filtered. So, enable group filtering only if you want to monitor or not monitor specific groups.
3. Click Add Group.The Add Group popup window displays.



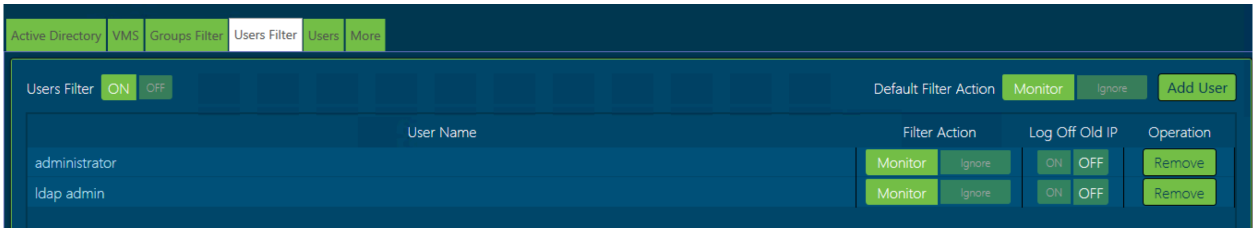
4. In the Group Name field, enter a name for the group. This is a required field. Note that the group name you enter must be same as the group name in Active Directory.
5. In the Filter Action field, select Monitor, to allow monitoring of the group, or Ignore, to disable monitoring for the group.
6. Click OK.

Add User Filters

You can add users (for example, admin), and you can enable or disable filtering for users. You can add specific uses who you want to monitor or do not want to monitor.

To add user filters:

1. In the WMI agent main window, select the Users Filter tab.

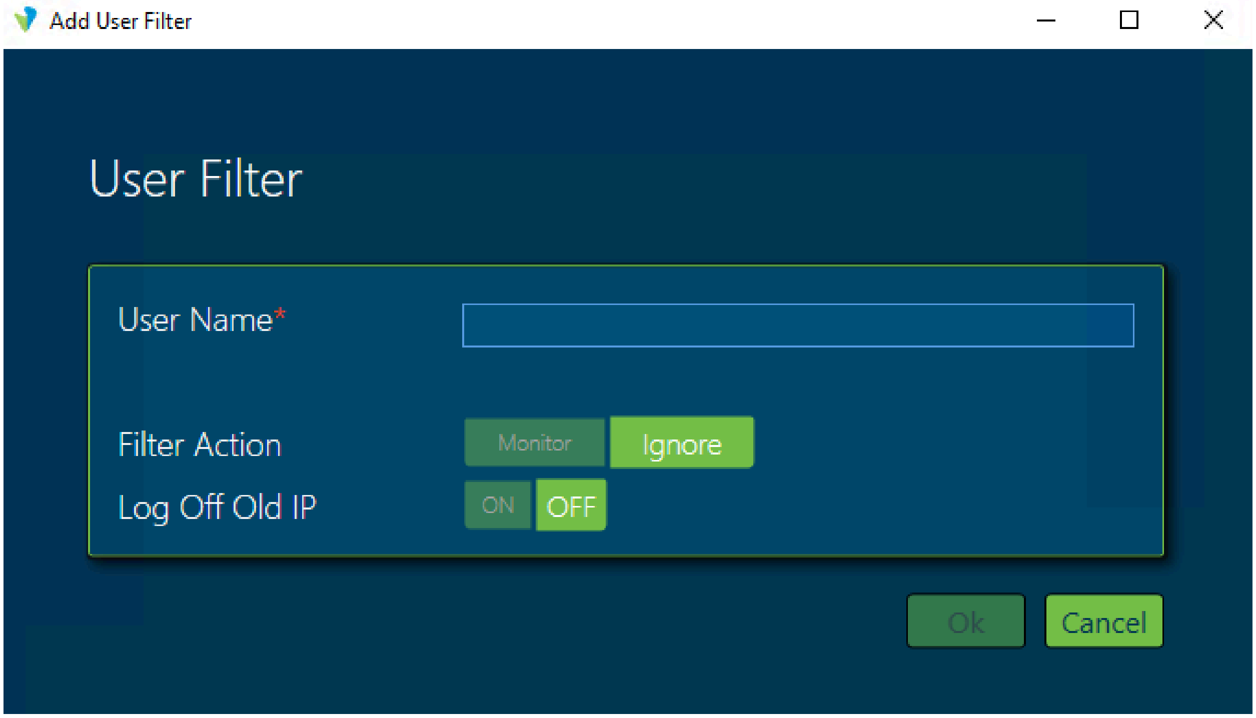


Users Filter: ON OFF

Default Filter Action: Monitor Ignore

User Name	Filter Action	Log Off Old IP	Operation
administrator	Monitor Ignore	ON OFF	Remove
ldap admin	Monitor Ignore	ON OFF	Remove

2. In the Users Filter field, click On to enable filtering for all users, or click Off to disable filtering for all users. If you set User Filter to On and you set Default Filter Action to Monitor, the filter action that you set for each user is used.
3. In the Default Filter Action field, click Monitor to monitor all users, or click Ignore to not monitor all users. The Default Filter Action also applies to the users that are not added here. For example, if you set Default Filter Action to Ignore, and when a user who is not added here logs in, that user's record is ignored as is not monitored.
4. If you set the Filter Action for a user to, in the Log Off Old IP field, configure whether to log the user in or out if they use an old IP address. For example, if you set the Filter Action for the user "administrator" to Ignore, the Log Off Old IP field is enabled (On) by default.
5. Click Add User to add a user filter. The Add User Filter popup window displays.



User Name*

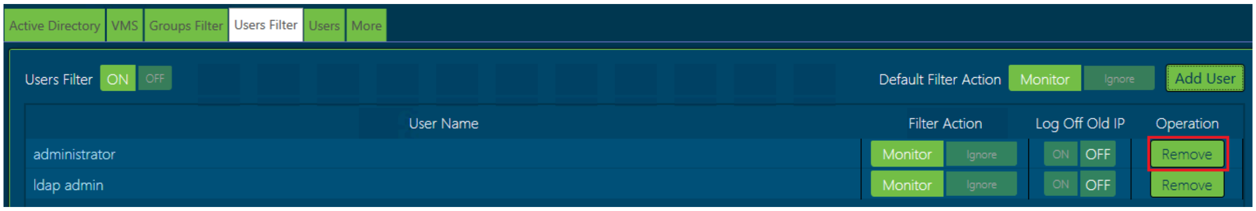
Filter Action: Monitor Ignore

Log Off Old IP: ON OFF

   a. In the Username file, enter the name of the user. A name is required.
   b. In the Filter Action field, click Monitor to monitor the user and click Ignore to not monitor the user. If you click Ignore, Log Off Old IP is enabled.
   c. If Filter Action is Ignore, in the Log Off Old IP field, select On to log off the user from an old IP address if the user logs in with a new IP address.

    d. Click OK.

To delete a user record, click Remove in the Users Filter tab:



Users Filter ON OFF

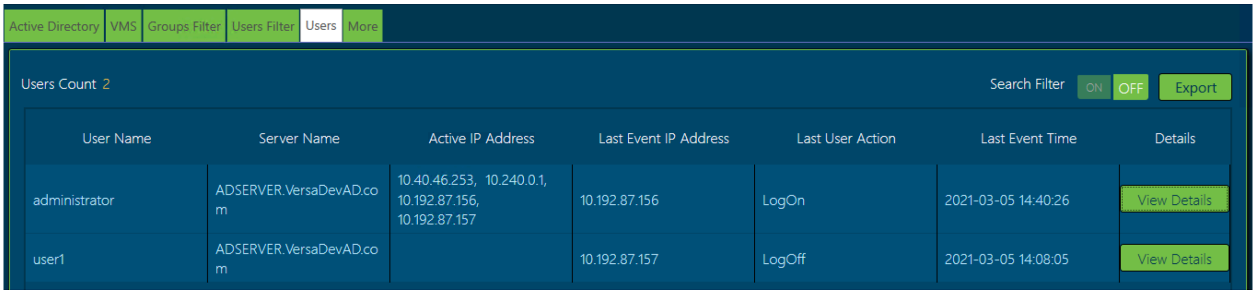
Default Filter Action Monitor Ignore

User Name	Filter Action	Log Off Old IP	Operation
administrator	Monitor Ignore	ON OFF	Remove
ldap admin	Monitor Ignore	ON OFF	Remove

View User Details

To view information about the users that you have added to the WMI agent:

1. In the WMI agent main window, select the Users tab to display the username, the server to which a user is connected, the active and last event IP addresses, the last user action, and the time of the last event.

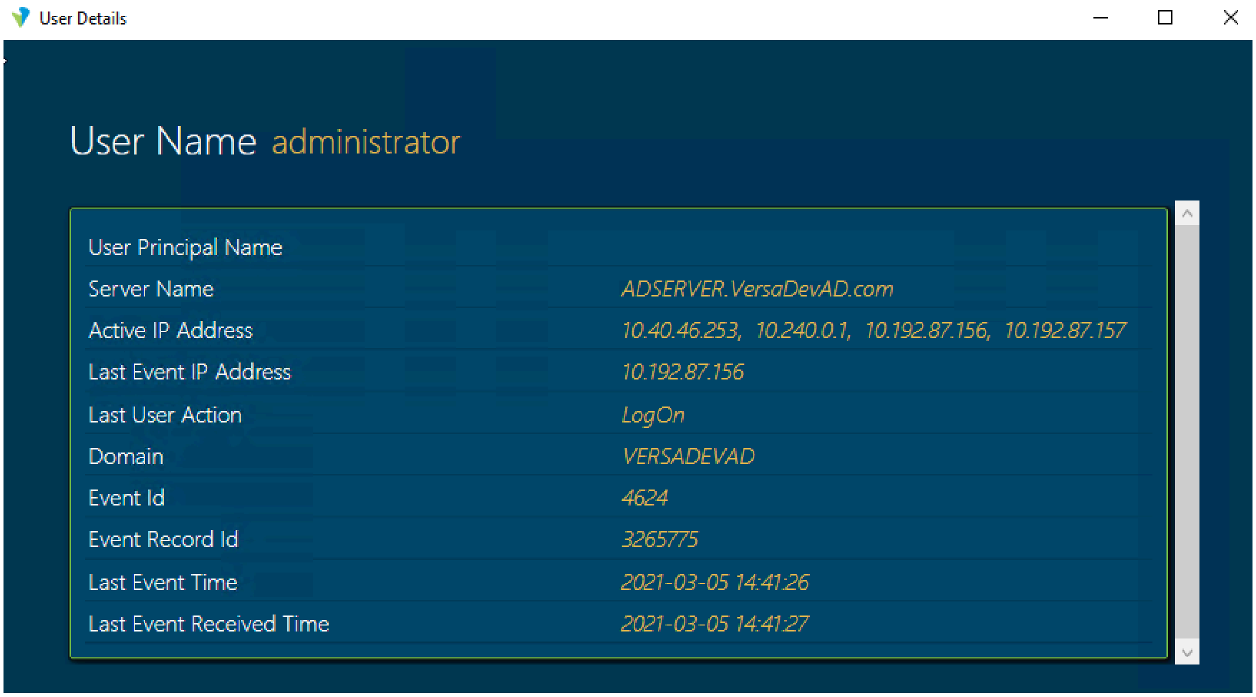


Users Count 2

Search Filter ON OFF

User Name	Server Name	Active IP Address	Last Event IP Address	Last User Action	Last Event Time	Details
administrator	ADSERVER.VersaDevAD.com	10.40.46.253, 10.240.0.1, 10.192.87.156, 10.192.87.157	10.192.87.156	LogOn	2021-03-05 14:40:26	View Details
user1	ADSERVER.VersaDevAD.com		10.192.87.157	LogOff	2021-03-05 14:08:05	View Details

2. To export user records to an excel (.xls) file, click Export.
3. Click View Details to view more information about a user.



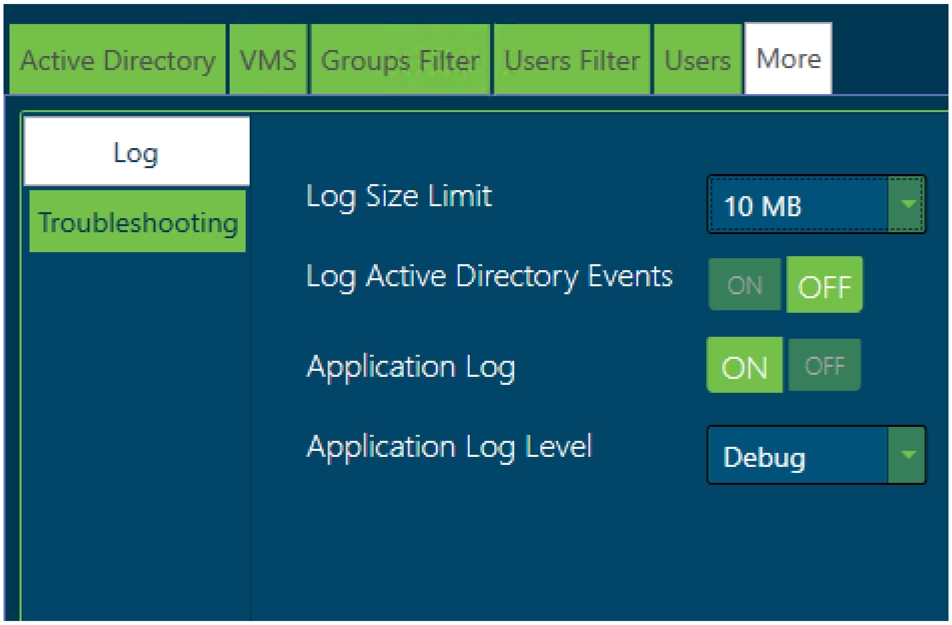
User Name administrator

User Principal Name	
Server Name	ADSERVER.VersaDevAD.com
Active IP Address	10.40.46.253, 10.240.0.1, 10.192.87.156, 10.192.87.157
Last Event IP Address	10.192.87.156
Last User Action	LogOn
Domain	VERSADEVAD
Event Id	4624
Event Record Id	3265775
Last Event Time	2021-03-05 14:41:26
Last Event Received Time	2021-03-05 14:41:27

Configure Log Parameters

To configure log parameters for the WMI agent:

1. In the WMI agent main window, select the More tab.
2. Select Log in the left navigation bar, and enter information for the following fields.



Log Size Limit: 10 MB

Log Active Directory Events: ON [✓ OFF]

Application Log: [✓ ON] OFF

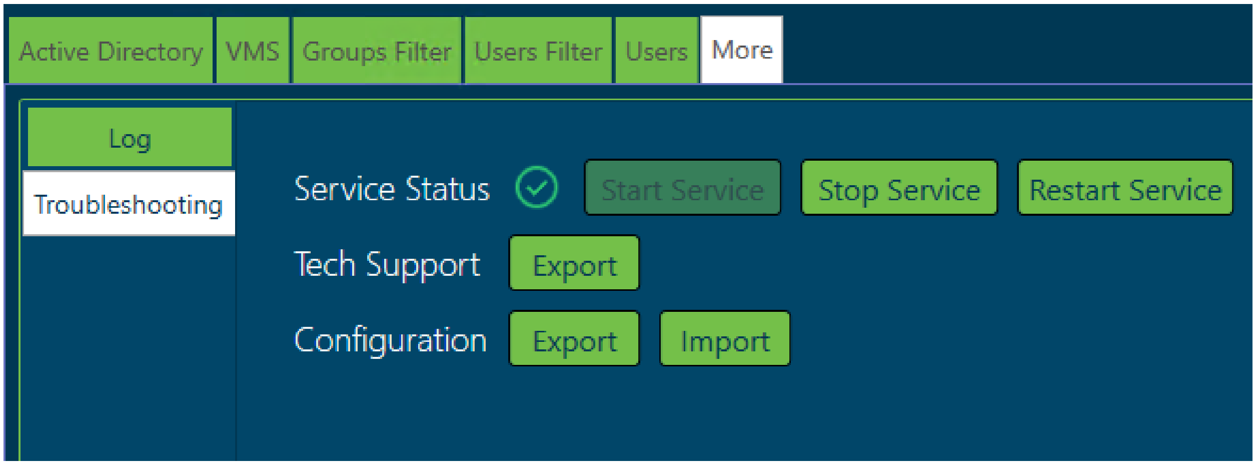
Application Log Level: Debug

Field	**Description**
Log Size Limit	Select maximum size for log files: ◦ 10 MB ◦ 25 MB ◦ 50 MB ◦ 100 MB
Log Active Directory Events	Click On to create logs for active director events.
Application Log	Click On to enable logging for application events.
Application Log Level	Select the severity level to apply to application logs: ◦ Debug—Application log requires debugging. ◦ Error—Log event is an error. ◦ Info—Log event is for informational purposes. ◦ Verbose—Show additional information during the interaction with the client user interface. ◦ Warn—Log event is a warning. *Default*: Debug

Troubleshoot WMI Service Issues

To check WMI service status and to start, stop, or restart the service:

1. In the WMI agent main window, select the More tab.
2. Select Troubleshooting in the left navigation bar to view the running status of the WMI service.



- ✓ indicates that the WMI service is running.
- ⊗ indicates that the WMI service has stopped. Click Restart Service to try to restart the service.

3. If the WMI service is not running, click Start Service to start it.
4. To stop the service, click Stop Service.
5. To save log records to share with Versa Networks Customer Support, click Export. The log records are saved as a .zip file.
6. To save a configuration record (.zip file) to your local disk, click Export. All configuration details except the password of the account used for listening to Active Directory events are saved.
7. To import a saved configuration record (.zip file) from your local disk, click Import and select the file to import.

Supported Software Information

Releases 21.2.1 and later support all content described in this article.

Additional Information

[Configure Passive Authentication for VMS]
[Install the Versa Messaging Service]