

### User Agent 1.1.5

## Preparing the Windows Environment and Installing the User Agent

How-To



### CONTENTS

Introduction to the User Agent	2
Selecting the User Account to Run the User Agent	3
Setting Access Rights on the Domain Controller	4
Verifying that DCOM is Allowed on the Domain Controller $\ \ldots$	5
Editing COM Security Permissions on the Domain Controller .	6
Auditing Successful Login Events	7
Allowing Security Leg Queries on the Domain Controller	8
Allowing Security Log Queries on the Domain Controller	0
Configuring WMI Permissions on the Domain Controller	9
Configuring WMI Permissions on the Domain Controller Installing the User Agent Software	9 11

The User Agent is an optional software component that can be installed either locally on Domain Controller or on another Windows system in the domain to associate users with IP addresses.





- 1. The Stonesoft Management Server sends the IP address of the User Agent, and the account name, password and IP address of the Domain Controller to the Stonesoft Firewall.
- 2. The Stonesoft Firewall sends the configuration information to the User Agent.
- 3. The User Agent queries the Controller Domain about log-on events from hosts in the domain to keep track of when a user logs on or logs off, a user's IP address changes, or a user acquires the same IP address that was previously associated with another user.
  - The User Agent can optionally be set to periodically send ICMP echo (ping) requests to users' workstations to monitor which users are active. If a user's workstation does not respond, the user is removed from the list of IP addresses. In cases where ping requests to workstations are not allowed or are unreliable, users' connections may be incorrectly closed. In these cases, workstation monitoring should not be enabled.
- 4. The Domain Controller replies to the User Agent.
  - Users are associated with IP addresses based on logs collected by the Active Directory Domain Controller. For this reason, it is only possible to associate one user with each IP address from a client computer. It is not recommended to use the User Agent with domains that include terminal servers or other computers that have many users logged on at the same time.
- 5. The User Agent verifies the information received from the Domain Controller and sends information about the user, IP address, and timestamp of log-on events to the Stonesoft Firewall.

#### **Configuration Overview**

- 1. Plan whether you will install the User Agent software locally on the Domain Controller or on another Windows system in the domain.
  - If there is only one Domain Controller it is recommended to install the User Agent on the same server for more efficient communication.
- 2. Configure the necessary elements in the Stonesoft Management Center as instructed in the section titled **Enabling Access Control by User** in the Stonesoft Administrator's Guide or the Management Client Online Help.
- 3. Configure the Windows system and the Domain Controller as instructed in this How-To document.
- 4. Install the User Agent software as instructed in Installing the User Agent Software (page 11).
- 5. (*Optional*) Enable Workstation Monitoring to monitor which users are active. See Workstation Monitoring (page 11).

#### Selecting the User Account to Run the User Agent

Usually administrator privileges are sufficient for the user account that runs the User Agent. However, depending on settings in the Windows environment, the User Agent user may need Domain Administrator privileges. If the User Agent is installed on a different server than the Domain Controller or if the User Agent needs to contact a remote Domain Controller, Domain Administrator privileges are always needed.

**1.** On the Windows system where you will install the User Agent, select **Control Panel**→**System Security**→**Administrative tools**→**Services**.



Note – In older Windows versions, select Control Panel  $\rightarrow$  Administrative tools  $\rightarrow$  Services.

- 2. Right-click the Stonesoft User Agent Service and select Properties.
- 3. Switch to the Log On tab.
- **4.** Select **This account** and type in the username of the user that has rights to connect to the Domain Controller.

#### Setting Access Rights on the Domain Controller

- **1.** On the Domain Controller, select Windows Server→Start→Administrative tools→Active Directory Users and Computers→Users.
- 2. Select an existing user or create a new user. Open the user properties.
- **3.** Switch to the **Member Of** tab.

Security	Env	vironment			Session	IS
Remote control	i l	Remote	Desktop !	Servic	es Profil	e
Personal Virtual De	esktop	COM+		Att	tribute E	ditor
General Address	Account	Profile	Teleph	ones	Orga	anization
Published Certificates	Member Of	Password	Replicati	on 📋	Dial-in	Objec
Name Administrators Distributed COM Use	Active [ example rs example	Directory Do com/Builtin com/Builtin	main Serv	vices I	Folder	-
Name Administrators Distributed COM Use Domain Users	Active I example rs example example	Directory Do .com/Builtin .com/Builtin e.com/Global	main Serv /Groups	vices I	Folder	
Name Administrators Distributed COM Use Domain Users	Active [ example rs example example	Directory Do com/Builtin com/Builtin com/Global	main Serv /Groups	vices I	Folder	
Name Administrators Distributed COM Use Domain Users	Active [ example rs example example	Directory Do e.com/Builtin e.com/Builtin e.com/Global	main Serv /Groups	vices I	Folder	
Name Administrators Distributed COM Use Domain Users	Active I example rs example example	Directory Do com/Builtin com/Builtin e.com/Global	main Serv /Groups	vices I	Folder	

4. Click Add. The Select Groups dialog opens.

Groups or Built-in security prin	ncipals	Object Types.
from this location:		
example.com		Locations
nter the object names to sele	ect ( <u>examples)</u> :	
		Check Name

- 5. Select Advanced and click Find Now.
- 6. Select and double-click the **Distributed COM Users** group.
- **7.** Click **OK**.
- 8. Repeat Step 4 to Step 7 to add the user to the following groups:
  - Administrators
  - Domain Users
- 9. Click OK to close the user properties.

4

## Verifying that DCOM is Allowed on the Domain Controller

- **1.** On the Domain Controller, select Start → Administrative tools → Component Services.
- 2. Browse to Component Services→Computers.
- 3. Right-click My Computer and select Properties. The My Computer Properties dialog opens.

Derduit Frotocois	COM Se	curity Ì	MSDTC
General	Options	Defau	It Properties
Enable Distributed C(	DM on this compute	r	
Enable COM Internet	Services on this co	mouter	
Enable Committeened	COCIVICES OF THIS CC	mpacer	
Default Distributed COM	M Communication P	roperties	
The Authentication Le	vel specifies security	y at the packe	t level.
Default Authenticatio	on Level:		
Connect		-	
Joonnood			
Jedinider			
The impersonation leve	el specifies whether	applications c	an determine
The impersonation leve who is calling them, an using the client's identi	el specifies whether id whether the appli ty.	applications c cation can do	an determine operations
The impersonation leve who is calling them, an using the client's identi	el specifies whether Id whether the appli ty.	applications c cation can do	an determine operations
The impersonation leve who is calling them, an using the client's identi Default Impersonatio	el specifies whether id whether the appli ty. n Level:	applications c	an determine operations
The impersonation leve who is calling them, an using the client's identi Default Impersonatio Identify	el specifies whether id whether the appli ty. n Level:	applications c cation can do	an determine operations
The impersonation leve who is calling them, an using the client's identi Default Impersonatio Identify	el specifies whether Id whether the appli ty. In Level:	applications c cation can do	an determine operations
The impersonation leve who is calling them, an using the client's identi Default Impersonatio Identify Security for reference t and that the default imp	el specifies whether Id whether the appli In Level: tracking can be prov personation level is	applications c cation can do vided if authen not anonymou	an determine operations tication is use s.

**4.** Switch to the **Default Properties** tab and make sure that **Enable Distributed COM on this computer** is selected.

# Editing COM Security Permissions on the Domain Controller

1. Switch to the COM Security tab.



- 2. Click Edit Default in the Access Permissions section. The Access Permission dialog opens.
- 3. Click Add and select the user that is used to connect to the Domain Controller.
- 4. Select Allow for the following permissions:
  - Local Access.
  - Remote Access.
- 5. Click OK to close the Access Permission dialog.



- **6.** Click **Edit Default** in the Launch and Activation Permissions section. The Launch and Activation Permission dialog opens.
- 7. Click Add and select the user that is used to connect to the Domain Controller.
- 8. Select Allow for the following permissions:
  - Local Launch.
  - Remote Launch.
  - Local Activation.
  - Remote Activation.
- 9. Click OK to close the Launch and Activation Permission dialog.

10.Click OK to close the My Computer Properties dialog.

#### Auditing Successful Login Events

- **1.** On the Domain Controller, select  $Start \rightarrow Administrative tools \rightarrow Group Policy Management.$
- 2. Browse to Group Policy Objects and select the Default Domain Controllers Policy.
- 3. Switch to the Settings tab in the right panel.
- 4. Right-click Default Domain Controllers Policy in the left panel and select Edit.



- 5. Browse to Computer Configuration→Policies→Windows Settings→ Security Settings→Local Policies→Audit Policy.
- 6. Right-click Audit account logon events and select Properties. The Audit Account Logon Events Properties dialog opens.



7. Select Success and click OK to close the Audit Account Logon Events Properties dialog.



Note – Depending on your existing configuration, auditing of Failure events may also be enabled. This does not affect the functioning of the User Agent.

#### Allowing Security Log Queries on the Domain Controller

1. Browse to Computer Configuration→Policies→Windows Settings→ Security Settings→Local Policies→User Rights Assignment.



2. Right-click Manage Auditing and Security Log and select Properties. The Manage Auditing and Security Log Properties dialog opens.

anage additing and secondy log ropercies	? ×
Security Policy Setting Explain	
Manage auditing and security log	
Define these policy settings: Administrators	
EXAMPLE\Exchange Servers EXAMPLE\user_agent	
2. 0.703452 · ·	
2 10000	

- **3.** Click **Add User or Group** and select the user that is used to connect to the Domain Controller.
- 4. Click **OK** to close the Manage Auditing and Security Log Properties dialog.

#### **Configuring WMI Permissions on the Domain Controller**

- **1.** On the Domain Controller, select **Start** $\rightarrow$ **Run**.
- 2. Type wmimgmt.msc and click OK. The WMI Control console opens.
- **3.** Right-click **WMI Control** and select **Properties**. The WMI Control (Local) Properties dialog opens.

amespace navigation allows you to set namespa	ace specific security.
E D Root	<u> </u>
ter la aspnet	
+ directory	
🗄 🧓 Hardware	
🗄 🧓 Interop	
庄 與 Microsoft	
🔁 🕖 MicrosoftActiveDirectory	
HicrosoftDfs	
🕀 🔛 nap	
	_
	(6

- 4. Switch to the Security tab.
- **5.** Browse to **Root** $\rightarrow$ **CiMV2**.
- 6. Click the Security button. The Security for Root\CIMV2 dialog opens.

curity		
iroup or user names:		
Authenticated Users LOCAL SERVICE		
USER_AGENT (user_agent@	Dexample.com)	
(a)	ministrators)	
Maministrators (EXAMPLE)Ad	7	)
🗠 Administrators (EXAMPLE)Ad	Add	Remove
Administrators (EXAMPLE)Ad	Add	Remove Deny
Administrators (EXAMPLE) Administrators (EXAMPLE) Administrators for USER_AGENT Execute Methods	Add	Remove
Administrators (EXAMPLE)Ad ermissions for USER_AGENT Execute Methods Full Write	Add	Remove
Administrators (EXAMPLE) Administrators (EXAMPLE) Administrators for USER_AGENT Execute Methods Full Write Partial Write	Add	Remove
Administrators (EXAMPLE) Administrators (EXAMPLE) Administrators for USER_AGENT Execute Methods Full Write Partial Write Provider Write	Add	Remove

- **7.** Click **Add** and type in or find the username of the user that is used to connect to the Domain Controller.
- 8. Select the following permissions for the user:
  - Execute Methods.
  - Provider Write.
  - Enable Account.
  - Remote Enable.
  - Read Security.
- 9. Click OK to close the Security for Root\CIMV2 dialog.

10.Click OK to close the WMI Control (Local) Properties dialog.



Note – Depending on your existing configuration, there may be other settings that override the settings you configure here to allow the User Agent to query the Domain Controller, or to allow the Domain Controller to create security log entries on user logon events.

User Agent installation requires administrator rights on the Windows system. After installation, the User Agent service must run with sufficient permissions to allow it to monitor the domain controller's Security Event Log.

#### ▼ To install a User Agent

- **1.** Log in to the system where you are installing the User Agent with the user account you configured to run the User Agent.
- 2. Transfer the User Agent installation files and the configuration.zip file to the computer.
- 3. Run UIA\_Installer.exe. The installation wizard starts.
- 4. Click Next. The License Agreement opens.
- 5. Click I Agree to accept the license.
- 6. (Optional) Click Browse and select the installation folder.
- **7.** Click **Install**. You may be prompted to install additional components that the User Agent requires.
- 8. Install any additional components as instructed in the installation wizards for those components. When the installation returns to the User Agent installation wizard, click **Next**.
- 9. Click Finish. The User Agent properties open.
- 10.Click Import Configuration and select the configuration.zip file.
- 11.Click OK.

#### Workstation Monitoring

The User Agent can optionally be set to periodically send ICMP echo (ping) requests to users' workstations to monitor which users are active.



Note – If a user's workstation does not respond, the user is removed from the list of IP addresses. In cases where ping requests to workstations are not allowed or are unreliable, users' connections may be incorrectly closed. In these cases, workstation monitoring should not be enabled.

#### **Stonesoft Guides**

Administrator's Guides - step-by-step instructions for configuring and managing the system.

Installation Guides - step-by-step instructions for installing and upgrading the system.

Reference Guides - system and feature descriptions with overviews to configuration tasks.

User's Guides - step-by-step instructions for end-users.

For more documentation, visit www.stonesoft.com/support/

**Stonesoft Corporation** 

ltälahdenkatu 22 A FI-00210 Helsinki Finland

Tel. +358 9 476 711 Fax +358 9 4767 1349

#### Stonesoft Inc.

1050 Crown Pointe Parkway Suite 900 Atlanta, GA 30338 USA Tel. +1 770 668 1125 Fax +1 770 668 1131

Copyright 2014 Stonesoft Corporation. All rights reserved. All specifications are subject to change.