



# codima

toolbox

redefining the art of network management

## CHECK LIST : Codima Discovery Engine

Available in the following Toolboxes:-

- Codima Toolbox – All in One
- IT Inventory and Mapping Toolbox
- IT Engineer Toolbox
- VoIP Readiness Toolbox

To successfully provide :-

- o Topology drawings (autoMap/Visio View tree branches)
- o Asset inventory reports (autoMap/Asset View and Asset Reports tree branches)
- o Information to set SNMP Polling Policy (autoMonitor/SNMP Poll Manager tree branch)
- o Information for Pinger list (autoPinger tree branch)

You will need to ensure the following:-

1. That a full copy of Microsoft® Office Visio® 2010 or 2007 Professional is installed on the Host PC (Visio® 2003 is supported for drawing production, however that software level does not have the real time data graphic facilities need to support the full Toolbox functionality).
2. That there are active SNMP Agents on the network? – Obtain a list if possible.
3. That you have the IP address of a Router or Switch, which has an active SNMP Agent. This address can be used as a start point for the discovery by including it in the Seed List.
4. That you have the required SNMP information needed to start the discovery, i.e., Read Community strings or, authentication and privacy information – range subject to SNMP version.
5. That you have an IP address for the Host PC - one that will be classed as a trusted IP address by the network firewalls (this is required to enable us to extend the discovery process beyond the local site to discover remote network assets).
6. That you have a list of IP addresses that should be included in the discovery - used to create the Seed List used by the discovery process (optional)
7. That you have a login for the Microsoft® network domain with Administrator rights : *Optional – only required if you wish to use WMI to obtain information from Microsoft® devices*).
8. **That Site planning is undertaken prior to starting the discovery, to ensure the most efficient discovery results - see Site Planning and Scale of Discovery check lists (Appendix 1 and 2)**
9. That you will be able to attach the Host PC to an SNMP compliant Router or Switch using a port that is on the network management VLAN (if the site uses VLANs).
10. That you configure the Toolbox Host PC with the required start parameters for the discovery, i.e., Seed List, SNMP Information.
11. That you test that some of the addresses in the Seed List responds to SNMP : Use the Test Seed List button in the Start Discovery dialog for an automatic check.
12. That hibernation/standby on the Toolbox Host PC is disabled and that windows automatic update is disabled to stop the system being restarted..

## Appendix 1 : Site Planning Check list

The Codima Discovery Engine can use a number of protocols/methods including SNMP, SIP Queries, CDP, ICMP, WMI, and NetBIOS in the discovery and inventory process. For the most complete inventory, the users need to ensure that the network devices are correctly enabled to use these technologies - see SNMP and WMI Planning entries below.

### SNMP Planning

It is important that all devices that are going to rely on SNMP as the main discovery protocol are configured correctly for IP and have SNMP Agents installed.

#### Check list:-

- **SNMP support** – Key devices need to have an SNMP Agent installed.
- **SNMP access** - You must be able to browse the discovery start point (Address in Seed List)
- **SNMP information** - The correct range of SNMP read communities/authentication/ privacy information must be included in the start up parameters
  - SNMP information required is subject to SNMP version:-
    - *SNMPv1 and v2* - Read community strings for the network (multiple Read community strings are supported).
    - *SNMPv3* – authentication and privacy information
- **VLAN** - The Toolbox Host PC must be on the management VLAN.
- **Access restrictions** - Devices should be checked to ensure they are not configured with filters or “Access Lists” restricting which administration addresses are allowed.
- **Firewalls** - For the discovery to work, the Firewall needs to be configured to allow the Toolbox Host PC to transmit and receive as a trusted user, i.e., to allow SIP, ICMP and SNMP source and destination packets etc through the Firewall. If running on a PC with XP service pack 2 that uses the XP system embedded firewall, ensure that you open the SNMP Ports.

### Device Library

You can also check the device type list used by the discovery process (*see Note 1*) prior to running a discovery, as it will help you establish if the key device types on your network have already been incorporated in to the Codima Discovery Engine. This way you will know in advance that some customization will be needed to add in unknown device types.

*Note 1: The Discovery Menu option titled Manage Device Library provides access to the device type list – for full information see Help entry titled “How to use Device Library”.*

### MIB Support

You can also check the latest MIB support by accessing the following url

- [www.codimatech.com/dl/extranet/TechnicalSupportFAQ/Linked\\_Documents/Codima\\_Toolbox\\_SNMP\\_MIB\\_List.zip](http://www.codimatech.com/dl/extranet/TechnicalSupportFAQ/Linked_Documents/Codima_Toolbox_SNMP_MIB_List.zip)

This is particularly relevant when using the **IT Engineer Toolbox**, as it provides a means of checking if performance information can be gathered from specific devices.

## WMI Planning

Microsoft® WMI is implemented and enabled, by default, on all Windows 2000, XP, 2003 and Vista systems.

### Check list :-

- **Domain Administrator** - The discovery engine must be run from a Domain Administrator account
- **WMI Support**
  - WMI discovery must be ticked in the Start Discovery dialog – it is an option under the *Start Discovery Advance Settings* Tab.
  - Network devices must support WMI.

The Discovery Engine will identify all WMI supported machines logged on that Domain

Can obtain WMI from:-

- Windows 2000 (SP4 or later)
- Windows XP
- Windows 2003
- Vista

Can NOT obtain WMI from:-

- Windows 95
- Windows 98
- Windows NT (pre SP6)

Microsoft® recommends the latest service pack when using WMI on NT.

## Appendix 2 : Scale of discovery - Check list

- **Have you allowed sufficient time for the discovery?**

Do you know how long the discovery could take - ensure you know roughly the number of devices involved in the discovery and roughly the number of Routers and Switches. The duration of an inventory/discovery varies with:

- The configuration parameters used when setting up discovery
  - Using the default settings makes SNMP the only management protocol and provides a fast discovery.
  - Using the optional advanced settings (associated with the Start Discovery Advance Settings Tab) instead will slow the discovery down, as they can include options to add Ping Scans and additional protocols to the discovery process.
- The size of the network
- The number of devices
- The type of devices
- The bandwidth available
- The complexity of the network configuration – for example will take longer if you have lots of VLANs, Subnets, or spanning trees and if you have multiple SNMP community strings.

Information on how long discovery should take is provided in the Codima Help, the Toolbox FAQs and Technical Bulletin 11.

- **Would the network discovery be best served if split into smaller discovery runs?.**

For example:

- To save time/get quicker more manageable results
- To enable end results to be “viewable” for example if the Layer 2 Topology drawing had over 100,000 objects in it, it would just be too complex to visualize. It is a much more realistic approach to produce a database for each network subnet, or divide up the discoveries according to your subnets
- To handle situations where you have multiple private networks with the same subnet.

- **Should you make use of the Merge discovery facility, undertaking multiple discovery runs and merging discovery results prior to the drawing production or generation of the asset report?**

For example:

- To handle firewalls that you are not allowed to breach, i.e., you can do an initial discovery run which stops at the firewall, then move the Host PC to the other side of the firewall and restart the discovery run adding the results to the same database (Use Discovery Menu item Rediscover Current Network – this will ensure the currently loaded discovery database is used in the new discovery).
- To handle devices with different SNMP Read community strings

For more information see Technical Bulletins 9 and 11, they provide guidance on improving discovery efficiency and scaling discovery for use on larger networks.