# Table of Contents

Copyright statement.........................................................................................................................5

Introducing Symantec Endpoint Threat Defense for Active Directory.................................................6
  About this guide............................................................................................................................................................. 6
  About Symantec Endpoint Threat Defense for Active Directory................................................................................ 6
  Capabilities of Threat Defense for AD...........................................................................................................................7
  Architecture..................................................................................................................................................................... 7
  Getting started with configuring Threat Defense for AD..........................................................................................10
  Where to get more information.................................................................................................................................... 11

About the Symantec Endpoint Threat Defense for Active Directory console............................. 13
  About launching the Threat Defense for AD console............................................................................................13
  Viewing your environment in the Threat Defense for AD console................................................................. 14
  Adding user accounts and roles..................................................................................................................................15
  About the Core server health analytics..................................................................................................................... 16

About the Threat Defense for AD settings..............................................................................................18
  Configuring the notifications from the Notifications tab.....................................................................................20
  Configuring additional settings from the Features tab.........................................................................................22
  Configuring the system AI through the AI tab.........................................................................................................24
  Updating Threat Defense for AD through the System Update tab.........................................................................26
  About the SEPM tab................................................................................................................................................26

Configuring Symantec Endpoint Threat Defense for Active Directory........................................ 28
  About Domains..............................................................................................................................................................28
  Configuring AD sites................................................................................................................................................... 28
  Configuring a deception policy..................................................................................................................................29
    Defining features in a deception policy................................................................................................................30
    Adding deceptive accounts to a deception policy..................................................................................................30
    Defining the exception list in a deception policy..................................................................................................31
  Configuring a Deployment Manager........................................................................................................................32
    Editing a Deployment Manager................................................................................................................................33
    Changing the log method of a Deployment Manager..........................................................................................34

Configuring and deploying Threat Defense for AD with Symantec Endpoint Protection.................... 36
  Configuring SEPM to deploy Memory Manipulation and the deception policy to the SEP agent.................37
  Viewing the Deploy tab..........................................................................................................................................40
  Assigning the Threat Defense for AD policy to SEPM endpoints and groups.............................................42
  Confirm the Memory Manipulation deployment.................................................................................................45

Adding additional SEPM servers..................................................................................................................46
Adding instances to a Deployment Manager.................................................................................................47
Performing test attacks in Symantec Endpoint Threat Defense for Active Directory............. 81
   Testing the Threat Defense for AD environment.............................................................. 81
   User information gathering............................................................................................. 81
   Computer information gathering..................................................................................... 81
   Credential theft using overpass-the-hash....................................................................... 82
   Credential theft using pass-the-hash............................................................................. 83

Troubleshooting Symantec Endpoint Threat Defense for Active Directory......................... 85
   Troubleshooting Threat Defense for AD................................................................. 85
   Issues with log collection and event subscription in Threat Defense for AD................. 85
   Issues with the Threat Defense for AD Core server................................................. 87
   Troubleshooting connectivity issues of a Deployment Manager.............................. 88
   Issues with sites and Memory Manipulation deployment in Threat Defense for AD........ 89
   Replacing web server SSL Certificate........................................................................ 90
   Updating Java................................................................................................................. 90

Frequently Asked Questions (FAQ) in Symantec Endpoint Threat Defense for Active Directory................................................................. 91
   Frequently Asked Questions about the Threat Defense for AD Forensics.................. 91
Copyright statement

Copyright statement

Broadcom, the pulse logo, Connecting everything, and Symantec are among the trademarks of Broadcom.

Copyright ©2020 Broadcom. All Rights Reserved.

The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, please visit www.broadcom.com.

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.
Introducing Symantec Endpoint Threat Defense for Active Directory

About this guide
This guide contains information on the settings that you can configure in Symantec Endpoint Threat Defense for Active Directory. You must have the Administrator role assigned to your account to configure the settings that are mentioned in this guide.

About Symantec Endpoint Threat Defense for Active Directory
Symantec Endpoint Threat Defense for Active Directory (Threat Defense for AD) is a solution that protects the Active Directory. Threat Defense for AD disrupts domain reconnaissance activity, detects an attacker that attempts lateral movement or credential theft, and mitigates intrusion by operations, users, or endpoints. The Artificial Intelligence engine uses Natural Language Processing and creates a false environment on the endpoint. This false environment obfuscates any AD reconnaissance commands that are used regardless of the protocol. This deception results in recognizing attackers when they attack the AD. The intrusion is then automatically mitigated through a deception policy. Threat Defense for AD identifies vulnerabilities, misconfigurations, and possible backdoors within the AD. This identification provides security teams with the opportunity to reduce the AD attack surface, harden the domain, and reduce risk.

Threat Defense for AD protects the integrity of the AD when configured for an endpoint or for a domain. A few security mechanisms can be leveraged to protect the AD from internal or external threats such as access to a domain connected endpoint. The AD stores very important data, and so it is prone to being constantly attacked. Through reconnaissance, lateral movement, and credential theft, an internal or external attacker can own the AD data with ease. Internal Red teams use vulnerabilities in the Kerberos implementation of authentication with AD. Pass-the-hash, Over-pass-the-hash, and Pass-the-ticket are attack methods that are difficult to prevent or even detect. Threat Defense for AD is a post-exploitation security measure that stops these intrusions and protects the AD after the endpoint protection and prevention
mechanisms have failed. Threat Defense for AD exists for the sole purpose of stopping compromises of corporate AD domain environments.

Threat Defense for AD provides security without making any changes to the AD, without deploying anything on the domain controllers, and without the use of an agent on the endpoints. Threat Defense for AD uses Memory Manipulation that is automatically deployed on the endpoints upon authentication. Memory Manipulation does not consume RAM, CPU, or disk space. The Core server automatically deploys the Memory Manipulation without using any deployment tool such as Microsoft System Center Configuration Manager. Threat Defense for AD creates actionable alarms that do not generate noise. An alarm is a high-fidelity event. Forensics are created automatically to generate incident response, and also invoke the automatic or manual mitigation means.

**Capabilities of Threat Defense for AD**

A high-level supported feature list of Threat Defense for AD can help you understand the end-to-end capabilities of the product.

**Table 1: Threat Defense for AD capabilities**

<table>
<thead>
<tr>
<th>Ease of Deployment</th>
<th>Ease of Management</th>
<th>Domain Security for the endpoint</th>
<th>Reduce Attack Surface</th>
<th>Advanced Testing (optional)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simple to install and configure the Core Server</td>
<td>No agent updates or upgrades</td>
<td>Disruption of reconnaissance</td>
<td>Find domain vulnerabilities</td>
<td>Domain attacks prevented from PowerShell Empire</td>
</tr>
<tr>
<td>Simple to deploy on endpoints</td>
<td>No need for Microsoft System Center Configuration Manager or package installer</td>
<td>Infinite scale of deception</td>
<td>Find Domain Misconfigurations</td>
<td>Domain attacks prevented from Metasploit</td>
</tr>
<tr>
<td>Non-disruptive to endpoints (no CPU, RAM, disk space)</td>
<td>Non-disruptive to IT – they do not have to see the deception</td>
<td>Credential Theft lure present in lsass</td>
<td>Find Attacker Persistency</td>
<td>Domain attacks prevented from BloudHound</td>
</tr>
<tr>
<td>No user friction or business impact</td>
<td>Easy to use console</td>
<td>Immediate detection of Lateral Movement attempt</td>
<td>Domain attacks prevented from Deathstar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Domain attacks prevented from Mimikatz</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Pass the Hash detection</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Over Pass the Hash detection</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Pass the Ticket detection</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Silver Ticket – Kerberoasting detection</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Autonomous Forensics</td>
<td></td>
</tr>
</tbody>
</table>

**Architecture**

The Threat Defense for AD architecture includes a Core server that contains a Deployment Manager (DM), Database (DB), and the web-based console. The Core server must run Windows Server 2019 (preferred) or Windows 2016, and can either be a physical computer or virtual machine.
You also require a Symantec Endpoint Protection (SEP) server. Large networks with multiple domains, or with over 20,000 endpoints may need multiple Deployment Managers. Endpoints are Windows clients that are members of the AD domain and are running SEP with the **Full protection policy** deployed. These endpoints run the domain deception as defined by the Threat Defense for AD policy.

**NOTE**

Contact a Broadcom support engineer of Symantec Endpoint Division for assistance with the architecture of standalone Threat Defense for AD. The standalone version has different requirements for a distributed architecture.

The Core server contains the database and the web-based console, as well as the Deployment Manager for the root domain. The Deployment Manager runs an IIS application pool that is used for policy assignment, forensic package deployment, topology gathering, and AD log collection. Additional domains require their own Deployment Manager.

The Deployment Managers can reside on the Core Server or on other dedicated virtual machines, depending on the architecture.

A distributed architecture is required for large networks with multiple domains, and may be used if there are over 20,000 endpoints. A distributed architecture requires a Deployment Manager for every domain. Child domains in a single AD forest have a native transitive trust with the root domain. The child domains can have their Deployment Managers on the Core server. Domains in another forest that have a one-way or two-way trust with the first domain, may each have a Deployment Manager on the Core server in the original Forest\Domain. If no trust exists, the Deployment Managers reside on remote servers or virtual machines in those domains, as long as they are reachable through the network. Deployment Managers can also be used to minimize bandwidth constraints across continents.
Hardware Requirements for Distributed Architecture

Hardware Requirements are based on expected log processing. These numbers are an estimation to be used for planning. Hardware can be added or removed after actual performance metrics are established. Each DM processes the logs for its domain. The preference is to limit the amount of virtual machines and deal with the load by removing or adding resources depending on the load. The main variable is event volume. This is driven by the DC count and velocity of events per domain. The log collection method can also have an effect on processing. Log collection method options are Windows Event Subscription or Syslog Event Forwarding (from another pre-existing syslog tool or SIEM) method.

Minimum Hardware Requirements

- Under 40k endpoints in a domain
  - Core server or DM server with 4 CPUs, 32 GB RAM
- Over 40k endpoints in a domain
  - Large Core server or DM server with 8 CPUs, 40 GB RAM

**NOTE**
If a Forest\Domain is not reachable through the network from the first Forest, then you require a second Core Server and DMs.
## Getting started with configuring Threat Defense for AD

Get started with protecting your AD environment with Threat Defense for AD.

### Table 2: Getting started with configuring Threat Defense for AD

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Complete the Threat Defense for AD Core server installation.</td>
<td>Make sure you have installed Threat Defense for AD Core server as per the guideline mentioned in <em>Symantec Endpoint Threat Defense for Active Directory Installation Guide</em>.</td>
</tr>
<tr>
<td>Step 2 (Optional)</td>
<td>Manage the AD sites.</td>
<td>Edit the AD sites that a Deployment Manager manages to deploy Memory Manipulation on endpoints in that AD site.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuring AD sites</td>
</tr>
<tr>
<td>Step 3</td>
<td>Deploy Memory Manipulation to the SEPM server.</td>
<td>Deploy Memory Manipulation to the SEPM console to assign the Threat Defense for AD policy to the endpoints in the SEPM console.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuring SEPM to deploy Memory Manipulation and the deception policy to the SEP agent</td>
</tr>
<tr>
<td>Step 4</td>
<td>Assign the Threat Defense for AD policy to the endpoints.</td>
<td>Assign the Threat Defense for AD policy to endpoints in the SEPM server and confirm Memory Manipulation deployment to protect the endpoints.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Assigning the Threat Defense for AD policy to SEPM endpoints and groups</td>
</tr>
<tr>
<td>Step 5 (Optional)</td>
<td>Add another SEPM server to Threat Defense for AD</td>
<td>You can add multiple SEPM server per one AD domain to Threat Defense for AD to protect the endpoints in the SEPM server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Adding additional SEPM servers</td>
</tr>
<tr>
<td>Step 6 (Optional)</td>
<td>Configure a new or edit an existing Deployment Manager in Threat Defense for AD.</td>
<td>By default, you configure a Deployment Manager when you add a domain to the Active Directory in Threat Defense for AD. Configure a Deployment Manager to deploy Memory Manipulation on the endpoints in your AD environment. You may need to configure multiple Deployment Managers for larger AD domains.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuring a Deployment Manager</td>
</tr>
<tr>
<td>Step 7 (Optional)</td>
<td>Define a new or edit an existing deception policy.</td>
<td>Define a deception policy to control the components that are deployed to the endpoints and servers in the AD domain. The deception policy can be edited at any time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuring a deception policy</td>
</tr>
<tr>
<td>Step 8 (Optional)</td>
<td>Enable the alarms that you want to be notified of in the Threat Defense for AD console.</td>
<td>Select the types of alarms in the <em>Settings</em> page of the Threat Defense for AD console that you want to be notified of.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>About the Threat Defense for AD settings</td>
</tr>
<tr>
<td>Step 9 (Optional)</td>
<td>Configure the Email Configuration setting.</td>
<td>Configure the Email Configuration settings to receive email notifications of alarms that are generated by Threat Defense for AD.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuring the notifications from the Notifications tab</td>
</tr>
<tr>
<td>Step 10 (Optional)</td>
<td>Add users to Threat Defense for AD to monitor your environment.</td>
<td>Add users to monitor the AD environment and run mitigation whenever necessary.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Adding user accounts and roles</td>
</tr>
<tr>
<td>Step 11 (Optional)</td>
<td>Add an instance to your environment.</td>
<td>You can add and configure multiple instances to manage AD domains that lack a two-way trust relationship.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Adding instances to a Deployment Manager</td>
</tr>
<tr>
<td>Step 12 (Optional)</td>
<td>Add an additional AD domain to your Threat Defense for AD.</td>
<td>You can add an additional AD domain to your Threat Defense for AD environment. Make sure that a two-way trust relationship is established between the domains.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Adding an additional AD domain</td>
</tr>
</tbody>
</table>
Where to get more information

Use the following documentation resources to learn about and use this product.

Table 3: Symantec Endpoint Threat Defense for Active Directory documentation set

<table>
<thead>
<tr>
<th>Document</th>
<th>Description</th>
<th>Location</th>
</tr>
</thead>
</table>
| Symantec Endpoint Threat Defense for Active Directory Release Notes | The release notes provide information about new features and important issues. | • This guide is available on the Endpoint Threat Defense for Active Directory Documentation page.  
• The "Documentation" folder of the Core server: \Program Files\Symantec\Endpoint Threat Defense for AD \Documentation |
| Symantec Endpoint Threat Defense for Active Directory Installation Guide | The installation guide illustrates how to install and configure the Core server. | • This guide is available on the Endpoint Threat Defense for Active Directory Documentation page.  
• The "Documentation" folder of the Core server: \Program Files\Symantec\Endpoint Threat Defense for AD \Documentation |
| Symantec Endpoint Threat Defense for Active Directory Administration Guide | The administration guide illustrates how to perform daily activities within Symantec Endpoint Threat Defense for Active Directory. | • This guide is available on the Endpoint Threat Defense for Active Directory Documentation page.  
• The "Documentation" folder of the Core server: \Program Files\Symantec\Endpoint Threat Defense for AD \Documentation |
| Symantec Endpoint Threat Defense for Active Directory Proof of Concept Guide | The guide describes a typical Symantec Endpoint Threat Defense for Active Directory proof of concept. | • This guide is available on the Endpoint Threat Defense for Active Directory Documentation page. |

The help manuals of Symantec Endpoint Threat Defense for Active Directory have been restructured. Following are the changes that are made to the help manuals:

Table 4: Changes in the help manuals of Symantec Endpoint Threat Defense for Active Directory

<table>
<thead>
<tr>
<th>Original Manual Name</th>
<th>Revised Manual Name</th>
<th>What has changed in the help manual?</th>
</tr>
</thead>
</table>
• Appendix is removed and added to the appropriate chapters. |
| Symantec Endpoint Threat Defense for Active Directory Installation Guide | Symantec Endpoint Threat Defense for Active Directory Installation Guide | • Content from the Symantec Endpoint Threat Defense for Active Directory Prerequisites Checklist Guide is added to this guide.  
• Content from Symantec Endpoint Threat Defense for Active Directory Domain Admin Equivalent Configuration Guide is added to this guide. |
<table>
<thead>
<tr>
<th>Original Manual Name</th>
<th>Revised Manual Name</th>
<th>What has changed in the help manual?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec Endpoint Threat Defense for Active Directory Pre-requisites Appendix</td>
<td>Not Available</td>
<td>Added to the Symantec Endpoint Threat Defense for Active Directory Installation Guide.</td>
</tr>
</tbody>
</table>

For more information on Symantec Endpoint Threat Defense for Active Directory, refer to the following link:

*Endpoint Threat Defense for Active Directory Documentation*
About the Symantec Endpoint Threat Defense for Active Directory console

About launching the Threat Defense for AD console

When you use Threat Defense for AD in an on-premises environment, the console is launched and accessed through the web browser:

https://localhost/ui

To access remotely, use:

https://servername/ui

You can configure Threat Defense for AD only as an Administrator. Use the settings displayed in the left menu of the console to configure Threat Defense for AD.

The icons in the left menu of the console represent the following settings:
Table 5: Icons on the console menu

<table>
<thead>
<tr>
<th>No.</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Overview</td>
<td>The <strong>Overview</strong> icon in the console displays the dashboard in Threat Defense for AD. The dashboard lets you monitor the security levels of your Threat Defense for AD environment. Press the <strong>Overview</strong> icon to view the Threat Defense for AD dashboard. Viewing your environment in the Threat Defense for AD console</td>
</tr>
<tr>
<td>2.</td>
<td>Alarms</td>
<td>The <strong>Alarms</strong> icon lists all the alarms that are generated in Threat Defense for AD. When a misconfiguration or a threat is detected in the Threat Defense for AD protected environment, an alarm is generated. Press the <strong>Alarms</strong> icon to view a list of the generated alarms and dark corners. About Alarms</td>
</tr>
<tr>
<td>3.</td>
<td>Domains</td>
<td>The <strong>Domains</strong> icon lets you configure the required settings to protect your Active Directory. You can configure all the settings that are required to deploy Memory Manipulation on the endpoints in your AD domain. Press the <strong>Domains</strong> icon to configure your Threat Defense for AD environment. About Domains</td>
</tr>
<tr>
<td>4.</td>
<td>Instances</td>
<td>The <strong>Instances</strong> icon lets you add a physical or a virtual machine to Threat Defense for AD. You must add another instance if you want to add a remote Deployment Manager to Threat Defense for AD. Press the <strong>Instances</strong> icon to add a physical or virtual machine to your Threat Defense for AD environment. Adding instances to a Deployment Manager</td>
</tr>
<tr>
<td>5.</td>
<td>Analytics</td>
<td>The <strong>Analytics</strong> icon lets you view the health of the Threat Defense for AD infrastructure. You can determine if the correct information is being collected and view the latest information about the different scans in Threat Defense for AD. Press the <strong>Analytics</strong> icon to view the infrastructure status of your Threat Defense for AD environment. About the Core server health analytics</td>
</tr>
<tr>
<td>6.</td>
<td>Logout</td>
<td>Press the <strong>Logout</strong> icon to log out of the Threat Defense for AD console.</td>
</tr>
<tr>
<td>7.</td>
<td>User Accounts</td>
<td>The <strong>User Accounts</strong> icon lets you add or edit user accounts configured to monitor your Threat Defense for AD environment. You can assign roles to limit the actions that the user accounts can execute. Press the <strong>User Accounts</strong> icon to add or edit user accounts in Threat Defense for AD. Adding user accounts and roles</td>
</tr>
<tr>
<td>8.</td>
<td>Settings</td>
<td>The <strong>Settings</strong> icon contains all the administrative settings of Threat Defense for AD. Press the <strong>Settings</strong> icon to execute administrator configurations of Threat Defense for AD. About the Threat Defense for AD settings</td>
</tr>
</tbody>
</table>

**Viewing your environment in the Threat Defense for AD console**

Access the **Overview** icon in the console menu to display the Threat Defense for AD dashboard. The dashboard provides a snapshot view of the collected Threat Defense for AD data. Press the **Overview** tab in the console to view the following:
Table 6: Data displayed in the Overview tab

<table>
<thead>
<tr>
<th>Data Components</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domains</td>
<td>Displays the domains that are configured. In a complex architecture with multiple domains, you can select the individual domain from a drop-down list, or see all data from all domains consolidated into a single view.</td>
</tr>
</tbody>
</table>
| Alarms         | Displays the alarms generated in Threat Defense for AD. The number on the circles represents the number of alarms generated. Alarms are of following types:  
  • Red circles: Represents alarms that are triggered from AD breach prevention when it detects an interaction with the mask or the credentials.  
  • Black Circles: Represents alarms that are triggered from the AD assessment scan identifies misconfigurations, vulnerabilities, or backdoors in the AD.  
Refer to *Symantec Endpoint Threat Defense for Active Directory Dark Corners Guide* for more information on AD assessment scan. |
| Protected Resources | Displays a list of protected resources on the dashboard that are counters related to Symantec Endpoint Threat Defense for Active Directory. That include:  
  • Number of the workstations that are deployed or protected with Memory Manipulation.  
  • Number of the servers that are deployed or protected with Memory Manipulation.  
  • Number of deceptive accounts that are in use.  
  • Number of subnets that exist within the domain.  
  • Number of domain controllers that are monitored. |
| Detected Dark Corners | Displays a list of dark corners on the dashboard that are counters related to Symantec Endpoint Threat Defense for Active Directory. Dark corners may be found on endpoints, domain controllers, or the domain database. |
| Latest Alarms   | Displays a list of the latest generated alarms on the dashboard. Press on an alarm to view detailed information of the alarm. |
| Latest Dark Corners | Displays a list of the latest generated dark corners on the dashboard. Press on a dark corner to view detailed information of the alarm. |

Adding user accounts and roles

Add user accounts to Threat Defense for AD to monitor your environment. You can assign roles to limit the actions that the user accounts execute. Settings that you configure here can also be configured under the User Management tab in the Settings page.

You can select from three roles that you can assign to a user account. The roles have different permissions:

Table 7: User account roles

<table>
<thead>
<tr>
<th>Roles</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>An administrator account has full access to the console, and can perform all types of actions.</td>
</tr>
<tr>
<td>Read-Only</td>
<td>A read-only account can only view the data on the Overview and Alarms tabs.</td>
</tr>
</tbody>
</table>
| Operator     | An operator account can only view data in the Overview and Alarms console. The operator user account can execute the following actions:  
  • Archive an alarm.  
  • Perform mitigation from the forensics report.  
  • Unmanage a dark corner.  
  • Re-run a dark corner. |
NOTE
Multiple admins, with different AD credentials, can access the Threat Defense for AD console at a time. However, if two admins use the same AD credentials to logon to the console, the session will disconnect for the previously logged on admin.

NOTE
Two administrators cannot work simultaneously on the console. However, operators and read-only users can work simultaneously with one administrator.

To add a user to Threat Defense for AD
1. Navigate to the Accounts page in the console.
2. Press Add User to create a new user in Accounts.
3. In the Account Details dialog box, enter the user name, email address, password, and select a role for the new user.
4. If you have already configured an email method to receive email alerts, assign the Email Method to the account from the drop-down list.
   About the Threat Defense for AD settings
5. Press Save.

About the Core server health analytics
Analytics provides data on the health of the Threat Defense for AD infrastructure.
The Analytics icon displays the following tabs:
- SymETDAD
- Domain Controllers
- Core
- Deployment Manager Name
- Domain Name
- Logs
- Services and Components

SymETDAD
View the health information of the Core server in the SymETDAD tab:
- **DC Log Collect**: Displays the status of log collection from the domain controller. If the Status is shown as failed, then there exists a communication issue for collecting logs from the domain controller.
  Troubleshooting connectivity issues of a Deployment Manager
- **Reset Password**: Displays the time of the last password rotation of deceptive accounts.
- **AD Sites Issues**: Displays domain controllers that have an issue with the deception account. The issues are usually caused because of a replication error in the AD.

The following information is also displayed at the bottom of the page:
- Information on the Last Topology scan for a domain.
- Information on the Last Powerful Objects scan for a domain. This scan searches for users and groups that have rights equivalent to an administrator.
- The Current Obfuscated Data Version of a domain displays the number of times a mask is recreated.
Domain Controllers

This tab has the information about the communication between the Deployment Manager and the domain controllers.

Core

The Core tab combines and displays information from the SymETDAD and Domain Controllers. Information on a disk space, and the time of the previously generated mask is also displayed.

Deployment Manager Name

The tab next to the Core tab is labeled as the name of the Deployment Manager. Determine if the correct event IDs are being collected from the domain controllers in this tab.

The information is distributed across the following sections:

- **Deploy Ids**: Displays the ID generated for Memory Manipulation deployment on endpoints.
- **Active working DCs**: Lists the active domain controllers in your environment from which Threat Defense for AD pulls the logs.
- **DC List**: Lists the information of the connected domain controllers in your environment.
- **Event Info**: Lists the information of the received events and statistics that are collected from the domain controllers.

Domain Name

In a multiple domain environment, a tab for each domain labeled the same as the domain name is displayed. You see the data on the specific Deployment Managers and can determine if you are collecting the correct event IDs from the domain controllers.

Event Info lists the following information:

- All domain controllers.
- The six event IDs collected for every domain controller.
- The number of seconds since the last event was received from a domain controller.

**N/A** on all event IDs may mean that a port is blocked. **N/A** on the same event ID on different domain controller may mean that there is an auditing misconfiguration.

Logs
Collect the logs if you think you may require assistance from the Broadcom Support team. You can edit the types of logs and the time interval for log generation. Deployment Manager logs are most common type of generated logs.

**To collect logs**

1. Navigate to Analytics > Logs tab in the console.
2. Select the type of logs you want to generate from the Log Options list.
3. Use the Select Time Span list to select the time span for which you want to generate the logs. This step is optional.
4. Press Generate.

After the logs are generated, press Download to locally save them to your endpoint. The log files are encrypted and password protected. You will need to upload them to Symantec, either through a location the Symantec Support team provides, or your own system for file sharing over the internet. If you want to review the log files, they are located in the file system in the following path:

\Program Files\Symantec\Endpoint Threat Defense for AD.

There are several locations, depending on which component you want to analyze.

**NOTE**

To upload the logs to cloud, you must configure the firewall rules to allow the Threat Defense for AD network traffic out.

**Services & Components**

**Services:** Lists all server processes and their statuses. Press Restart All Services to restart all the listed services in the console. To restart an individual service, press Restart against the service name.

**Components:** Lists the following components:

- **Active Directory Topology:** Displays the results of the Active Directory Topology. The AI uses this data for mask creation. The AD topology scan generally runs every 24 hours.
- **Dark Corners:** Restarting all components triggers the domain alarms and domain controller dark corners alarms. The scan normally runs according to the defined schedule in the Settings page.
- **Hosts Dark Corners:** Restarting all components triggers the endpoint dark corner alarms. The scan normally runs according to the defined schedule in the Settings page.
- **Obfuscated data:** Generates the mask, usually at installation. The obfuscation data regenerates when the AD topology changes by 2%.

Press the Re-Run option to have the individual components reprocess their data.

**About the Threat Defense for AD settings**

You can perform all administrative tasks from the Settings page of the console.

The Settings page contains the following configurations:
### Table 8: Tabs on the Settings page

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Notifications</strong></td>
<td>You can configure the <strong>Email Methods</strong> and <strong>Email Configurations</strong> settings in this tab to receive email notifications of generated alarms and dark corners.</td>
</tr>
<tr>
<td><strong>Features</strong></td>
<td>You can configure to enable or disable certain features in Threat Defense for AD. You can specify the time interval for scans and reset the password length for deception accounts in this tab.</td>
</tr>
<tr>
<td><strong>AI</strong></td>
<td>You can configure the artificial intelligence to define specification for the mask creation.</td>
</tr>
<tr>
<td><strong>System Update</strong></td>
<td>You can view the system version of Threat Defense for AD in this tab. You can also manually upgrade Threat Defense for AD from this tab.</td>
</tr>
<tr>
<td><strong>User Management</strong></td>
<td>The <strong>User Management</strong> tab has the same functions as the <strong>Accounts</strong> setting.</td>
</tr>
<tr>
<td><strong>Help</strong></td>
<td>The <strong>Help</strong> tab has a link to all Threat Defense for AD documentation on the <a href="https://www.symantec.com">Endpoint Threat Defense for Active Directory Documentation</a> page.</td>
</tr>
<tr>
<td><strong>Advanced</strong></td>
<td>The <strong>Advanced</strong> tab lists all the enabled alarms and dark corners. You may make changes to the list of alarms and dark corners alarms that you receive.</td>
</tr>
<tr>
<td><strong>About</strong></td>
<td>You can locate the Symantec license for Threat Defense for AD in the <strong>About</strong> tab.</td>
</tr>
<tr>
<td>Tab</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| AD Password Policy         | The **AD Password Policy** tab lets you configure and generate password for the deceptive account that meets the complexity requirements of your organization. Edit the password policy of the deceptive account to specify:  
  • Numerical characters with value between 0-20 number  
  • Lower case characters between 0-20 characters  
  • Upper case characters between 0-20 characters  
  • Special characters between 0-20 number  
  • Characters that are not allowed or disabled. These characters must be separated by comma. |

**Reset Password Length**  
Use this drop-down list to select the password length Threat Defense for AD uses when rotating the deception account password. The characters must be between 14-30 characters.

**Configuring the notifications from the Notifications tab**  
Configure the settings in this tab to receive email notifications about the generated alarms and dark corners in your Threat Defense for AD environment.  
**The Notifications tab has the following sections:**  
- **Email Methods**  
  Contains the settings for email and syslog alerts. Threat Defense for AD sends alarms and other alerts to users configured to receive the notifications. To turn off email notifications, set the **Email Forwarding** setting to **OFF**.  
- **Email Configuration**
Configure this setting to add email accounts to receive breach prevention alerts from Threat Defense for AD. You can add additional emails by typing in an email address and pressing the Add option.

1. Email Methods
Configure the Microsoft Email Exchange server to receive email notifications and enable relevant firewall rules between the exchange server and the Deployment Manager. You must configure a mailbox on the exchange server from which Threat Defense for AD can send an email.

To configure a Microsoft Exchange server with a mailbox

a) Navigate to the Settings > Notifications page in the console.
b) Press Add Exchange Config.
c) Enter the Configuration Description for the Microsoft Exchange server in the Add Exchange Config dialog box. For example: Corporate Exchange Server.
d) Enter the Email address to use for sending mails. Threat Defense for AD uses this mailbox on your Microsoft Exchange server to send an email.
e) Enter the Exchange Server name.
f) Enter the Exchange Port. This port is the appropriate port and is usually 25.
g) If you require authentication to the Microsoft Exchange server to send an email, check the Mailbox Password box.
h) Press Add Exchange Config.

If you want to send alerts to syslog, SIEM, or Splunk, you must add a syslog alert to Threat Defense for AD.

To add a Syslog server

a) Navigate to the Settings > Notifications page in the console.
b) Set SymETDAD Syslog Forwarding to ON.
c) Press Add Forwarding. An Add Syslog dialog box is displayed.
d) Select the appropriate protocol from the drop-down list. The commonly used protocol is UDP.
e) Enter the Syslog Server IP address.
f) Press Add Syslog.

A syslog message is sent to you every time an event occurs and is in the standard syslog format. For example:


Where:
- 'WIN-Q171KLF6IHB' is the Core server.
- 'domain:acme.com' is the domain that Threat Defense for AD protects.
- 'hostName:mc-w10-guy.mcdonalds.demo' is the source of the attack.
- 'alarmType:NetComputer' is the alarm type (in this case 'Computer Information Gathering').
- 'destination:MC-DC-3.McDonalds.demo' is the domain controller that generated the alarm.
- 'objectName:win-felicitas$' is the item of the mask that was interacted with.

Table 9: Types of alerts

<table>
<thead>
<tr>
<th>Alert</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NETUSER</td>
<td>User Information Gathering</td>
</tr>
<tr>
<td>xternalNetUser</td>
<td>Brute Force Attempt</td>
</tr>
<tr>
<td>NetComputer</td>
<td>Computer Information Gathering</td>
</tr>
</tbody>
</table>
2. Email Configuration

Add multiple email addresses to receive the breach prevention email alerts.

**To add accounts to receive breach prevention email alerts**

a) Select **Add Email** to enter a destination email address and press **Add**.
b) Under the **Email method** column, select **Exchange server** from the drop-down list.
c) In the **Alerts** column, select the type of breach prevention email alert that you want to receive:
   - **Off**: No email is sent for breach prevention alarms.
   - **Alerts**: You receive an email alert as soon as Threat Defense for AD receives the event log message of the attempted breach.
   - **Alerts + Forensics**: You receive an alert when the forensics report succeeds or fails. The forensics report is attached with the email alert.
   - **Aggregated Alerts + Forensics**: You receive this email alert when the aggregation window closes. All events that are seen in the aggregation window are mentioned and the forensics report is attached.
d) To receive dark corner alerts, press the drop-down list under **Dark Corner** in the console. Select the type of email alert that you want to receive:
   - **Off**: No email is sent for dark corner alarms.
   - **Dark Corners**: The alert is triggered whenever a new dark corner is discovered.
   - **Dark Corners + Report**: A PDF report is added with the details of each dark corner.
e) Repeat the procedure to add multiple email accounts.

Press **Test** to send a test email to the specified email address. The option under the tab turns green to inform you that the test email is sent. Check your mailbox to see if you received the email alert. Press **Remove** to stop an email address from receiving the dark corner alerts.

### Configuring additional settings from the Features tab

You can enable or disable certain settings, generate the forensics report when alarms are triggered and send the server health data to Broadcom Support in the **Features** tab.

You can set the following features to **On** or **Off** under this tab:
- **AD Assessment**: The AD assessment scan looks for misconfigurations, vulnerabilities, and backdoors.
- **Forensics**: Use this setting to disable the forensic analysis that executes on the endpoint after an alarm is generated.
- **Forensics Map Animation**: Enable this option to view the animated version of the forensics report.
- **Block Untrusted LDAP for Clients**: Enable this option if you want Threat Defense for AD to block untrusted LDAP connections with your AD network. Untrusted LDAP connections can let an intruder query the AD to retrieve unauthorized information.
- **Enforce encryption of SAMR queries**: Enable this option to enforce encryption of Security Account Manager (SAM) Remote protocol queries that passes through the Domain Controller to prevent data breaches. The SAMR queries are converted to encrypted LDAP queries such that any breaches in the network does not disclose fake or real objects.

![System Features](image)

- **Enforce encryption of SAMR queries (Requires SEP 14.3 MP1+)**: Enable this option to enforce encryption of Security Account Manager (SAM) Remote Protocol queries towards the DC, to prevent data breaches. The SAMR queries are converted to encrypted LDAP queries such that any breaches in the network does not disclose fake or real objects.
To change time intervals of an AD assessment scan

1. Navigate to the Settings > Features page in the console.
2. Press Advanced to the right of AD Assessment.
3. Enter the time intervals in hours for each dark corner parameter. Different dark corners run against different items in the domain:
   - Domain Dark Corners run against the AD database.
   - DC Dark Corners run against the domain controllers.
   - Host Dark Corners run against the endpoints.
  Refer to the Symantec Endpoint Threat Defense for Active Directory Dark Corners Guide.
4. Press Save

Configuring the system AI through the AI tab

The AI tab on the Settings page contains a wizard to customize the mask creation and Artificial Intelligence (AI). To launch the wizard, press Edit. Press Re-Run to rebuild the mask at any time.
To configure the system AI

1. Navigate to the Settings > AI page in the console.
2. Press Edit in the console.
3. Select the domain from the drop-down list. Press Next till the Add Words to our AI Dictionary page is displayed.
4. In the Add Word space, enter the word that you want to include in the AI dictionary and press Add Word.
   Press X to remove the word.
   This word seeds the AI and is included in the mask that the AI generates.
5. Repeat the process to add multiple words to the AI dictionary and press Next.
   In the Deceptive Data Blacklist page, specify the words that the AI must not use when generating a mask.
6. In the Add Word space, enter a word that you want to add to the blacklist.
7. Press Add Word.
   Select X to remove the word.
8. Repeat the process to add multiple words to the blacklist.
   In the Deceptive Data Multiplication Factor dialog box define the value of the deceptive data generation. The default value is set at 6x.
10. Press on the space where the default value (6x) is mentioned. Select a value from the drop-down list and press Next.
    In the Add Powerful groups dialog box add the powerful groups that must be obfuscated.
11. In the Type Group Name space, enter the name of the group you want to obfuscate.
    Select X to remove the group name.
12. Repeat the step to add multiple group names.
13. Select Save.

The AI automatically re-runs after you save the settings and a progress bar is displayed at the bottom of the page.
Source endpoints from the topology run are ignored from the mask creation if they meet the following conditions:

- Endpoints that have not logged on in over 30 days (stale asset).
- Endpoints that have no "operationSystem" attribute.
- Endpoints that have no "distinguishedName" attribute.
- Endpoints that have no "SAMAccountName" attribute.
- Endpoints that have no DNS record.
- Endpoints accounts that are disabled.
- Endpoints in the OU "Domain Controllers".
- Endpoints that contain words from the deceptive data blacklist.
- Endpoints names that are shorter than 5 letters.
- Endpoints names that are longer than 15 letters (20 letters for users).

**Updating Threat Defense for AD through the System Update tab**

You can view and update the system version in the System Update tab.

- **System Information**: You can view information on the current version number, and other components of the software under this section.

- **Update Version**: You can view the version status of each component of Threat Defense for AD.
  Download the latest update file of Threat Defense for AD from the Broadcom Download Center to the Core server and log on to the Core server. Do not extract the zip file.

  **NOTE**
  For more information on how to download the latest version of Threat Defense for AD, refer to the article here.

**To install a Threat Defense for AD update manually**

1. Navigate to the Settings > System Update page in the console.
2. Press Install Update Manually.

  **NOTE**
  Do not unzip the file that Symantec provides.

3. Browse to the file location and select the zip file.

A message with the status of the file upload is displayed at the bottom of the page. When the file upload is complete, the status changes to Updating and takes several minutes to complete. If successful, the Version number reflects the latest update.

**About the SEPM tab**

The following tabs are seen under the SEPM tab:
Table 10: Columns under the SEPM tab

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entry Name</td>
<td>Displays the name of the SEPM server.</td>
</tr>
<tr>
<td>IP</td>
<td>Displays the IP address of your endpoint.</td>
</tr>
<tr>
<td>Username</td>
<td>Displays your SEPM user name.</td>
</tr>
<tr>
<td>Domain</td>
<td>Displays the domain name that you have connected to SEPM.</td>
</tr>
<tr>
<td>Site</td>
<td>Displays the site name that you have configured with SEPM.</td>
</tr>
<tr>
<td>Port</td>
<td>Displays the web service port number of the endpoint.</td>
</tr>
<tr>
<td>Edit</td>
<td>Press the Edit option to edit the SEPM connection configuration.</td>
</tr>
<tr>
<td>Master</td>
<td>If you have multiple SEPM servers, press the Current Master option of the SEPM server that you want to assign as the master SEPM.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the status of Threat Defense for AD to SEPM health-check. The health-check is run every alternate minute.</td>
</tr>
<tr>
<td>Password Expiration</td>
<td>Displays the password expiration date of the present SEPM password.</td>
</tr>
<tr>
<td>Sync Data</td>
<td>Press Sync Site if you want to restore the old SEPM configuration.</td>
</tr>
<tr>
<td>Unenroll Site</td>
<td>Press Unenroll Site if you want to remove a SEPM server or the entire SEPM site.</td>
</tr>
</tbody>
</table>
Configuring Symantec Endpoint Threat Defense for Active Directory

About Domains
The Domains icon on the menu contains the Deployment Managers that are configured within the application for each domain. To view the information about all the domains that you have added, use the drop-down list that is next to the domain name.

Each domain displays the following:
• At least one defined Deployment Manager.
• A view of sites that are populated based on AD Sites and Services.
• At least one defined deception policy.
• The Deploy tab which provides a view of assignment and deployment of Memory Manipulation on the endpoints.

Configuring AD sites
The Sites tab displays the structure of a specific domain and is populated based on the AD Sites and Services for each domain. Based on this structure, the Deploy tab is populated where you can select the endpoints that Memory Manipulation protects.

The Sites tab has the following columns:

Table 11: Columns displayed in the Sites tab

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site</td>
<td>Displays the site name.</td>
</tr>
<tr>
<td>Coverage</td>
<td>Displays the number of endpoints on which Memory Manipulation is deployed and of the endpoints that are available.</td>
</tr>
<tr>
<td>Subnet</td>
<td>Displays the number of subnets in a site.</td>
</tr>
<tr>
<td>Remove</td>
<td>Lets you remove a specific site from being managed by a Deployment Manager.</td>
</tr>
</tbody>
</table>

You can edit the AD sites that a Deployment Manager manages.

NOTE
You cannot edit a site that has an endpoint with Memory Manipulation deployed on it.
To edit the AD sites managed by a Deployment Manager

1. Navigate to the Domains > DM page in the console.
2. Select the Deployment Manager that you want to edit the sites on and press Edit.
3. The Add Sites to <Deployment Manager Name> dialog box is displayed. Select the sites to edit them from being managed.

A grayed out site has an endpoint with Memory Manipulation deployed and you cannot make changes to this site.

**NOTE**

The changes to the sites that you make here are also reflected in the Domains > Deploy tab.

4. Press Save Changes

**NOTE**

If a site has no domain controller, a scenario is created where the domain and the AD determine an another site's domain controller to manage that site. Symantec recommends selecting all sites to be managed by a domain controller for Threat Defense for AD to have full visibility of a site's activity from the domain controller logs.

The Sites tab is displayed again with the changes reflected in the console. Press Edit next to the site name to view the subnets of each site. You can manage or unmanage the individual subnets.

**Configuring a deception policy**

The Policy tab contains the deception policies and the deceptive users that are available for deployment. Deception policies control the components that are deployed on endpoints and servers. You can have multiple deception policies, but have only one active policy on any given endpoint. The deception policy controls the deceptions that are deployed and make exceptions, if any. You can configure multiple deception users in a policy, and the users are distributed in a repeated rotational order.

When configuring a deception policy, you define information in the following tabs:

**Table 12: Tabs to define in a deception policy**

<table>
<thead>
<tr>
<th>Tab Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Features:</td>
<td>You can change the policy name in this tab. You can make this policy the default policy and enable auto mitigation of attack processes here.</td>
</tr>
<tr>
<td></td>
<td>Defining features in a deception policy</td>
</tr>
<tr>
<td>Deception Accounts:</td>
<td>You can add or remove the deception accounts under this tab. This is the Domain User account created for deception and appears as a Domain Admin to attackers looking in Microsoft's Local Security Authority Subsystem Service (lsass) for credentials.</td>
</tr>
<tr>
<td></td>
<td>Adding deceptive accounts to a deception policy</td>
</tr>
<tr>
<td>Exception List:</td>
<td>The exception list lets you exclude users, groups, or processes from receiving the mask at authentication and should be rarely used.</td>
</tr>
<tr>
<td></td>
<td>Defining the exception list in a deception policy</td>
</tr>
</tbody>
</table>

Around the usage of the Exception List, Symantec recommends the following:

**If you are concerned with IT administrators receiving the mask:**
As per Microsoft recommendations, use a dedicated administration system that has been hardened and is not connected to the Internet. Domain Admins must use this system when logging in as a Domain Admin account (even if you do not have Threat Defense for AD). Exclude this system within Deploy page.

Login into a domain controller and run reconnaissance. Threat Defense for AD does not change the domain controllers in any way.

Make a user exclusion for a user or group of users with policy. You can limit the user exclusion to specific endpoints based on policy assignment on the Deploy page.

If you are concerned about an application that has generated alarms:

- Make a process exclusion with policy. Limit this policy in the Deploy page to specific endpoints that run the application.
- Inform Broadcom Support about these application issues.

### Defining features in a deception policy

You first configure the Features tab when you configure a deception policy.

#### To define features in a deception policy

2. Select Add Deception Policy.
   - To edit an existing policy, press Edit on the existing deception policy.
3. Enter a policy name under the Policy Name space in the New Deception Policy dialog box. The policy name should not have spaces.
   - You can rename an existing policy, or skip this step.
4. Under Policy Settings, do the following:
   a) To make this policy the default deception policy, check the Default Policy box.
   b) To automatically mitigate attack processes, check the Auto Mitigate box.
5. Press Next.

### Adding deceptive accounts to a deception policy

After defining the features, you have to add deceptive accounts to the deception policy.

#### To add deceptive accounts to a deception policy

2. Select Add Deception Policy.
   - To edit an existing policy, press Edit on the existing deception policy.
3. Press Next to view the Add Deceptive Account dialog box.
4. Press Add Account to add a deception account.
5. To use an existing account in the AD, select Existing account in Active Directory from the drop-down list and do the following.
   - Make sure that the accounts are created as per the Prerequisites for installing Threat Defense for AD guidelines mentioned in the Symantec Endpoint Threat Defense for Active Directory Installation Guide.
   a) Enter the username and password of the AD account that you want to use as the deceptive account.
   b) Press Add new Deception Account.
6. To create a new account in the AD, select New account in Active Directory from the drop-down list.
   - The Deployment Manager application pool running as the "Deployment Manager Account" must be a Domain Admin for this function to be successful.
For more information, refer to the *Creating a Domain admin equivalent account* section in the *Symantec Endpoint Threat Defense for Active Directory Installation Guide*.

a) Enter the username and the Organizational Unit (OU). The name should not contain anything similar to “Threat Defense for AD”. Having words like “helpdesk” or “admin” in the username makes the account an attacker's target. The OU is the location in the AD where you want the account to reside. Do not name the OU with any words that would give away the intention of this account.

b) Press **Add new Deception Account**.

7. Press **Next**.

To remove a deceptive account, press X next to the username.

**NOTE**
Be careful to not remove an existing account on accident. If you do, you need to reset the password in the AD before you can add it again.

**Defining the exception list in a deception policy**

After adding the deceptive accounts, you can define the exception list in the deception policy. Exclude a developer, user or group of administrators from the mask for business reasons. Exclude a process when you have an application that needs perform reconnaissance, or one that causes a conflict in memory. Users can be tied to workstations.

**To define the exception list in a deception policy**

1. Navigate to the **Domains > Policy** page in the console.

2. Select **Add Deception Policy**.

   To edit an existing policy, press **Edit** on the existing deception policy.

3. Press **Next** till you see the **Exception List** dialog box.

4. To define the users that you want to exclude, select **User** from the drop-down list on the left and do the following:
   a) Enter the username of the existing AD account you want to exclude from receiving the mask at authentication.
   b) Press **Add User**.
      Press X to remove the user. You can add multiple users.
   c) Press **Done**.

5. To define the groups that you want to exclude, select **Groups** from the drop-down list on the left and do the following:
   a) Enter the group name of the existing account you want to exclude from receiving the mask at authentication.
   b) Press **Add Group**.
      Press X to remove the group. You can add multiple groups.
      You may not select a built-in group. However, you can nest one in a regular user group within the AD, and then select that group. This requirement is due to AD and Kerberos.
   c) Press **Done**.

6. To define the processes that you want to exclude, select **Process** from the drop-down list on the left and do the following:
   a) Enter the process name of the process you want to exclude from receiving the mask at authentication.
   b) Press **Add Process**.
      Press the X to remove the process.
      This exclusion is only supported by process name at present.
c) Press **Done**.

To review the counters under each exception type in the **Add Process to Exception List** dialog box, press **Edit**. If you are done configuring the deception policy, press **Update Deception Policy**. Press **Yes, Update Policy**.

After defining the deception policy, you are navigated to the **Policy** tab. The bottom of the page shows all the configured deceptive users and the deception policies they belong to. If an account is unused, you can press the delete icon in the corner to remove it.

### Configuring a Deployment Manager

You can find the **Deployment Manager** tab in the **Domains** setting. Deployment Managers handle communication between the Core server and the protected endpoints. A Deployment Manager is bound to the domain of the assigned Deployment Manager account that is used to deploy Memory Manipulation on endpoints. The first Deployment Manager runs on the localhost of the Core server. Large environments with multiple domains require additional Deployment Managers. Use additional Deployment Managers for scalability or for multiple Deployment Manager accounts within a specific domain.

**To configure a Deployment Manager in the Threat Defense for AD console**

1. To add a Deployment Manager, do the following:
   a) Navigate to the **Domains > DM** tab in the console.
   b) Press the **Add Deployment Manager** option to the upper right corner of the console. The **Add Deployment Manager** dialog box is displayed.
   c) In the **Create Domain** tab, configure the following:
      - For a multiple domain environment, enter the **Fully Qualified Domain Name** for which you want to configure the Deployment Manager. The domain name is displayed by default in a single domain environment.
      - If you have multiple physical instances configured, enter the name of the physical instance that you want to configure for this Deployment Manager in the **Virtual Machine** space. For the single domain environment, the instance is always the **localhost**.
        
        **NOTE**
        The physical instances need to be configured in Threat Defense for AD before configuring a Deployment Manager.

   **Adding instances to a Deployment Manager**
   - Enter a **Deployment Manager Name** for this Deployment Manager.
     In multiple domain environments, follow a naming convention to reflect the domain in the Deployment Manager name. For example, Domain 1.DM1
     
     **NOTE**
     If you receive an error **invalid validation**, there may be a problem with the domain name entered.
   d) Press **Next**.
   e) In the **Select Log Method** tab, do the following:
      - Select **WMI Collector** from the **Log Method** drop-down list.
• Enter 15 seconds as the **Collection Interval** for log collection. This is the most common method of log collection and time frame. You can change the log collection method to your preferred method.

**Changing the log method of a Deployment Manager**

You can remove a Deployment Manager from the domain it is linked to if you think the Deployment Manager is not required.

**To remove a Deployment Manager**

2. To remove a Deployment Manager, do the following:
   a) Navigate to the **Domains > DM** page in the console.
   b) Press **Remove** next to the Deployment Manager to remove.

   **NOTE**
   If a Deployment Manager has endpoints deployed, do not remove that Deployment Manager.
   c) Press **Remove** on the dialog box to confirm the removal of the Deployment Manager.

   The Deployment Manager is removed from your environment and is not listed under the **DM** tab.

**Editing a Deployment Manager**

You can edit the **DM Identities** and **Log Method** settings of a Deployment Manager after adding it to a domain.
When editing a Deployment Manager, the `<Deployment Manager name> Configuration` dialog box displays the following information:

- **Domain** displays the name of the selected domain.
- **DM Identities** displays the current user account that the IIS application pool uses to deploy Memory Manipulation on endpoints.
- **Log Method** displays the current log collection method that the Deployment Manager uses. Changing the log method of a Deployment Manager

**To edit a Deployment Manager**

1. Navigate to the Domains > DM page in the console.
2. Press **Edit** next to the Deployment Manager that you want to edit.
3. Press **Edit** under **DM Identities**. The **Edit DM Users** dialog box is displayed.
   a) Enter the credentials of the user account that you want to use as the Deployment Manager account.
4. Press **Change** next to the **Log Method** to change the log collection method of the Deployment Manager.
   Changing the log method of a Deployment Manager
5. Press **Save**

**Changing the log method of a Deployment Manager**

A log file records all the events that occur in your Threat Defense for AD environment. When you configure a Deployment Manager, you must define a log collection method to troubleshoot Threat Defense for AD errors or when you require assistance from the Broadcom Support team.

You can select from the following log collection methods for a Deployment Manager and only one type of log collection can be active at any time:
• WMI
• Event Subscription
• Syslog
• None

1. **WMI**

   This is the default type of log collection method. To change the time interval of **WMI Collector**

   **To use WMI as the log method**

   Replace 15 with the desired time interval in seconds.

   a) Navigate to the **Domains > DM** page in the console.
   b) Press **Edit** under the **Config.** column. The `<Deployment Manager name> Configuration` dialog box is displayed.
   c) Press **Change** under **Log Method**. The **Change Log Method** page is displayed.
   d) Select a **Log Method** from the drop-down list.
   e) Enter a numeric value in the **Collection Interval (in seconds)** space.
   f) Press **Save**.

2. **Event Subscription**

   This option provides near real time alerting and deployments within Threat Defense for AD. You must configure event subscription on each domain controller to select this option as a log collection method.

   To use event forwarding, make sure the following prerequisites are met:

   • Enable **Winrm** on all of the domain controllers (`winrm qc`).
     
     **NOTE**
     
     This method enables **winrm** to any requester. Symantec recommends to enable **winrm** in a secure, locked down method in production environments.
   
   • Enable the **Windows Event Collector** on domain controllers and server side (`weutil qc`).
   • On all domain controllers, the **Network Service** must have permission to **Manage** auditing and security log.
   • You must be a member of **Event Log Readers** and **Network Service** to collect logs.
     
     **NOTE**
     
     The user account that is defined to read logs can also be a Deployment Manager user account.
   
   • Enable communication access from the Core server to the domain controllers - 5985, Ports 5986. Restart the **Windows Event Collector Service** on the Core server.

   **To use Event Subscription as the log collection method**

   a) Navigate to the **Domains > DM** page in the console.
   b) Press **Edit** under the **Config.** column. The `<Deployment Manager name> Configuration` dialog box is displayed.
   c) Press **Change** under **Log Method**. The **Change Log Method** page is displayed.
   d) Select **Event Subscription** from the **Select Log Method** drop-down list.
   e) In the **Change Log Method** dialog box, do the following:
      
      • Enter the **Username** and **Password** of the Deployment Manager account.
      • Enter the **Event Path**.
      • Add the **Subscription Hostnames**.
   f) Press **Save**.

3. **Syslog**

   If you are already collecting logs from the domain controllers into a syslog or SIEM, you can have Threat Defense for AD pull those logs. Syslog format must adhere to the Request for Comments (RFC) 5424 standard.
To use Syslog as the log collection method

a) Navigate to the Domains > DM page in the console.
b) Press Edit under Config. column. The `<Deployment Manager name> Configuration` dialog box is displayed.
d) Select Syslog from the Select Log Method drop-down list.
e) Select the Syslog Parser you use from the drop-down list.
f) Enter the IP of the syslog server in Syslog Server’s IP.
g) Enter the Listening Port number that is used. The most common value is 514.
h) Press Save.

4. None
   Select this option only when you have a Deployment Manager that manages endpoint deployments, but does not collect logs. You must have another Deployment Manager that already has a Syslog server configured.

   To use None as the log collection method

   a) Navigate to the Domains > Deployment Manager page in the console.
b) Press Edit under Config. column. The `<Deployment Manager name> Configuration` dialog box is displayed.
d) Select None from the Select Log Method drop-down list.
e) Press Save.

After the settings are implemented, you can change the log collection method in the system and enter a user name and password that is used to collect logs. The system automatically sets up a rule to collect logs from the domain controllers.

Configuring and deploying Threat Defense for AD with Symantec Endpoint Protection

Configure SEPM with Threat Defense for AD to assign the Threat Defense for AD policy to SEPM groups. You must first deploy Memory Manipulation and the deception policy to SEP agent to protect the endpoints in you AD domain. You can then assign the Threat Defense for AD policy to the SEPM groups and endpoints which enables Memory Manipulation and the deception policy that is already deployed to SEPM.

To configure SEPM with Threat Defense for AD, execute the following steps:

- Configuring SEPM to deploy Memory Manipulation and the deception policy to the SEP agent
- Viewing the Deploy tab
- Assigning the Threat Defense for AD policy to SEPM endpoints and groups
- Confirm the Memory Manipulation deployment

If you have configured multiple SEPM groups for one AD domain, select a domain to configure the settings on.

To select a domain in a multiple domain environment

1. Navigate to Domains in the console.
2. Press the domain name to display a drop-down list of all the configure domains in your Threat Defense for AD environment.
3. Select the domain for which you want to configure settings

The Domains settings reflects the data for the selected domain.
Configuring SEPM to deploy Memory Manipulation and the deception policy to the SEP agent

You must first configure SEPM to deploy Threat Defense for AD’s Memory Manipulation and deception policy to the Symantec Endpoint Protection (SEP) agent.

To configure SEPM

1. Navigate to **Admin > Install Packages > Client Install Feature Set** in the SEP console.

   You can select from the following options that contain the Threat Defense for AD policy:

   - **Full protection for Clients**
   - **Full protection for Servers**
   - **Full protection for Active Directory**

   You can also customize your policy to include Threat Defense for AD.

2. Press **Clients** in the menu.

3. Select the group that you want to deploy the Memory Manipulation to. If a group has sub-groups within it, then only select the parent group. Memory Manipulation is deployed to the sub-groups automatically.

   **NOTE**

   Threat Defense for AD policy is not active until the policy is assigned from the Threat Defense for AD console.
4. Press **Install a client**. The **Client Deployment Wizard** window is displayed.

5. Select **New Package Deployment** and then press **Next**.

6. Select a package that includes Threat Defense for AD from the **Install Feature Sets** drop-down list and press **Next**.

7. Enable **Remote Push** and press **Next**.

   Alternatively, you can also select the **Save Package** option and deploy the package with an automation tool.
8. Move the endpoints that you want to assign Memory Manipulation to under **Install Protection Client on**: and press **Next**.

![Computer Selection](image)

Browse or search the network for computers on which you want to install the protection client.

To view the Threat Defense for AD on the SEPM console, double click on a client. The **Edit Properties for "Client name"** is displayed. Press on the **Clients** option on the window.

9. Enter the credentials of the SEP account that you use to deploy the SEP agent in the **Login Credentials** dialog box.

10. Press **Next** till you navigate to the following screen. Press **Finish**.
You can also see the policy that is assigned to a group under the Clients > Policies tab.

Viewing the Deploy tab

**Viewing the Deploy tab**

You manage the AD environment to deploy Memory Manipulation on endpoints in the Deploy tab. You can select from the following 3 options to view the endpoints:
- **SEPM**: Lets you filter the endpoints in your domain as per your SEPM console.
- **OU**: Lets you filter the endpoints in your domain based on the organizational unit in your AD domain.
  This view is a read-only view.
- **Sites**: Lets you filter the endpoints based on the sites you have configured in your environment.
  This view is a read-only view.

You can filter each view using the drop-down list in the left pane. Select a group from the list in the left pane to view the endpoints in that group.

The Deploy tab consists of Filter columns on the right side, each with a counter. The filters are applied to endpoints that exist in the selected domain in the left pane. The filters are:

**Table 13: Filter columns in the Deploy tab**

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>All endpoints that exist within AD.</td>
</tr>
<tr>
<td></td>
<td><strong>The following are not supported and do not appear in the All filter:</strong></td>
</tr>
<tr>
<td></td>
<td>• Domain Controllers</td>
</tr>
<tr>
<td></td>
<td>• Endpoints that belong to a Workgroup and are not on the domain</td>
</tr>
<tr>
<td></td>
<td>• Windows XP, 2000, 2003, any flavor of Linux, or Mac OS X</td>
</tr>
<tr>
<td>Not Assigned</td>
<td>Endpoints eligible for deployment but without a policy assigned.</td>
</tr>
<tr>
<td>Assigned</td>
<td>Endpoints that have a policy assigned and the Memory Manipulation deployed.</td>
</tr>
<tr>
<td>Undeployable</td>
<td><strong>Endpoints that are not eligible for deployment. Those are:</strong></td>
</tr>
<tr>
<td></td>
<td>• Endpoints that have not logged on in the last 30 days.</td>
</tr>
<tr>
<td></td>
<td>• Endpoints that have an unsupported OS.</td>
</tr>
</tbody>
</table>

The following columns are under each Filter column and they display the following data:

**Table 14: Columns under the Filter column**

<table>
<thead>
<tr>
<th>Column</th>
<th>Displayed data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint</td>
<td>Displays the computer name of the endpoint.</td>
</tr>
<tr>
<td>IP address</td>
<td>Displays the endpoint's latest DNS record for the IP address.</td>
</tr>
<tr>
<td>Version</td>
<td>Displays OS version of the endpoint.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the present Memory Manipulation deployment status.</td>
</tr>
<tr>
<td>Policy</td>
<td>Displays the effective policy that is assigned on the endpoint.</td>
</tr>
<tr>
<td>Installed On</td>
<td>Displays the last date and time the endpoint authenticated, and the Memory Manipulation was deployed.</td>
</tr>
<tr>
<td>Identity</td>
<td>Displays the Core server account that manages and deploys on this endpoint.</td>
</tr>
</tbody>
</table>

To apply filters and search for a specific endpoint in the domain

1. Navigate to the **Domains > Deploy** page in the console and select a **Filter**.
2. Press the drop down icon next to the filter name and type the keywords of the endpoint. The endpoints are filtered in real-time.
3. Repeat the step for all the filters that you want to apply to your search. The filter that is applied is shown in blue under the column heading.
   To remove a filter
4. Reselect the drop-down arrow, and delete the text applied.

Assigning the Threat Defense for AD policy to SEPM endpoints and groups

Assigning the Threat Defense for AD policy to SEPM endpoints and groups

When you assign the Threat Defense for AD policy to the SEPM group, Memory Manipulation along with the appropriate policy is enabled in SEPM for that group. If you add a new computer to the network and install the SEP agent with the correct client features, the Threat Defense for AD policy is automatically assigned. You need to deploy the Threat Defense for AD policy from the Threat Defense for AD console to activate it. Assign the policy to SEPM groups to activate Memory Manipulation within the SEP agent with the appropriate policy.

To assign the Threat Defense for AD policy to SEPM groups

1. On the Domains page, select the SEPM filter.
2. Select the SEPM group you want to deploy the policy to on the left pane of the page.
3. Press the Assign option that is below the list of SEPM groups.
4. A pop-up window is displayed on the page. On this window, select the policy you want to deploy from the drop-down list.

5. Press the **Assign** option.

![Policy Selection Window](image)

A pop-up window notifies you that the data is being sent to SEPM. There is a delay before the Threat Defense for AD console reflects the current status of the policy assignment. Threat Defense for AD is dependent on the SEPM schedule for agent communication. If you hover over the SEPM group, you can see that the policy is assigned to that group.

When the deployment is complete, the status of the group changes to **Success**.

To un-assign the Threat Defense for AD policy on SEPM groups
6. On the Domains page, select the SEPM filter.

7. Select the SEPM group that you want to un-assign the policy from the left pane on the page.

8. Press the Un-Assgin option that is below the list of SEPM groups.

9. On the pop-up window that is displayed, press Un-Assgin to confirm the removal of the Threat Defense for AD policy.

The Threat Defense for AD policy is unassigned from the endpoints and the endpoints are listed under the Not Assigned tab.

Confirm the Memory Manipulation deployment
Confirm the Memory Manipulation deployment

To confirm Memory Manipulation is deployed successfully, RDP to the target host. Launch a command prompt and type:

You should see the actual Domain Administrators that are obfuscated by 6x false accounts. This is one example the deception Memory Manipulation creates. To see real accounts, connect to a domain controller and perform the same command.

To confirm that the Memory Manipulation deployment is successful, RDP to the target host. Launch a command prompt and enter the following command:

`net group/domain “domain admins”`

You see the actual Domain Administrators obfuscated by six times the false accounts. This deception is an example of the mask that the Memory Manipulation deploys. To see reality, connect to a domain controller and perform the same command. You can also perform test attacks against your Threat Defense for AD protected AD environment.

Error Codes

These are the status codes that could return from the SEP client which also reflected to the SEPM console:

- 0 = installed without policy (translated to Not Installed on the Core console)
- 1 = running with policy (translated to success on the Core console)
- 2 = error applying policy (translated to Failed on the Core console)
- 3 = getting credentials failed (translated to Partial Success on the Core console)
- 4 = credentials were bad (translated to Partial Success on the Core console)
- 5 = pending deployment (translated to Not Installed on the Core console)
- 6 = running with errors (translated to Partial success on the Core console)

There could be a case where the endpoint restarts after the status of this endpoint is displayed as Success on the console. During that time and the time Threat Defense for AD was starting, SEP reports code “5” meaning “pending deployment” to the SEPM and then Threat Defense for AD does topology. Then, the status Threat Defense for AD shows is Not Installed. On the next topology run, Threat Defense for AD receives the real status that SEPM reports and changes it to either success, fail, or partial.
Adding additional SEPM servers

You can add multiple SEPM servers to Threat Defense for AD to protect the endpoints in the AD domain.

To add an additional SEPM server to Threat Defense for AD
1. Navigate to the Settings > SEPM tab in the console.
2. Press Add a Symantec Endpoint Protection Manager.

3. Provide the following details in the displayed SEPM Connection details dialog box:
   - **Connection Name**
     Provide a suitable connection name for the SEPM server.
   - **IP Address/Hostname**
     Provide the IP address or hostname of the SEPM server.
   - **Web Services Port**
     Provide the web port number of the SEPM server. The default port number is **8446**.
   - **SEPM Sysadmin**
     Provide the sysadmin username of the SEPM server.
   - **SEPM Password**
     Provide the sysadmin password of the SEPM server.
   - **SEPM Domain**
     Provide the SEP domain name. The default name of the domain is **Default**.
   - **Add SEPM SSL Certificate**: You need the SEPM SSL .cert file from the SEPM server to add this server to Threat Defense for AD.
4. Press **Submit**

The SEPM server is added to your Threat Defense for AD environment and is listed under the **Settings > SEPM** tab.

**About the SEPM tab**

**Adding instances to a Deployment Manager**

The **Instances** icon on the menu is where you define either a virtual or a physical computer to run a remote Deployment Manager. Remote Deployment Managers can be used for scalability or to handle multiple domains that lack a two-way trust.

For server specifications, refer to the *Planning and installing* chapter of the *Symantec Endpoint Threat Defense for Active Directory Installation Guide*.

**To add another instance**

1. In your remote computer, open the [https://10.211.149.149/ui/login](https://10.211.149.149/ui/login) using a web browser. Symantec recommends using Google Chrome.

   The **Connect to Symantec TDAD core** dialog box is displayed.
2. Navigate to the **Instances** page in the console in your already configured computer.

3. Press **Add instance** in the console. The **Create new Deployment Manager instance** dialog box appears with the **API Key** and the **Thumbprint** value of the new Deployment Managers.
4. Copy and paste the API Key and the Thumbprint from the Create new Deployment Manager instance dialog box to the Connect to Symantec TDAD core dialog box.

5. Enter the IP address of the remote computer in the Core IP Address space in the Connect to Symantec TDAD core dialog box.

6. Press Submit

When a connection is detected and established, the message Your Deception Manager is ready is displayed on the page. Your remote instance is listed on the Instances page of the Threat Defense for AD console.

Configuring a Deployment Manager

Adding an additional AD domain

You can add multiple AD domains to Threat Defense for AD to deploy Memory Manipulation and protect endpoints in the domain. You can add an additional domain to Threat Defense for AD only if the two AD domains share a trust relationship.

Adding a domain to Threat Defense for AD involves the following steps:

• Making a user from the additional AD domain a local administrator on your computer
  You must make a user from the other AD domain a local administrator on your computer. Use this user account as the Deployment Manager account when you add this domain to Threat Defense for AD.

• Adding the AD domain to Threat Defense for AD
  After you have specified a user as the local administrator on your computer, configure the Threat Defense for AD console to add the new AD domain.

Making a user from the additional AD domain a local administrator on your computer

NOTE
  If you have multiple virtual machines configured, configure the following setting on the virtual machine which will host the additional AD domain.
Adding instances to a Deployment Manager

1. To make a user from the other AD domain a local administrator on your computer, do the following
   a) Click Start and navigate to Computer Management > Local Users and Groups in your computer.
   b) Select Groups and then select Administrators.

The Administrators group lists all the users that are local administrators of the computer.
c) Press **Add** in the **Administrators Properties** dialog box.

d) Press **Locations** in the **Select Users, Computers, Service Accounts, or Groups** dialog box.

e) Select the AD domain that you want to add to Threat Defense for AD from the displayed list in the **Locations** dialog box and press **OK**.

Refer to the **Pre-requisites of installing Threat Defense for AD** section in the **Symantec Endpoint Threat Defense for Active Directory 3.4 Installation Guide**.

f) Specify a user account with the required privileges as the Deployment Manager user account for the AD domain.

g) Press **OK**.

**Adding the AD domain to Threat Defense for AD**
2. To add an additional AD domain to Threat Defense for AD, do the following:
   a) Navigate to the Domains page in the console.
   b) Press the **<Domain Name>** option in the console.
   c) Press **Add Domain** from the displayed drop-down list.
   d) In the **Create Domain** tab, configure the following:
      
      • Provide the **Fully Qualified Domain Name** for which you want to configure the Deployment Manager.
      • If you have multiple physical instances configured, provide the name of the physical instance that you want to configure for this Deployment Manager in the **Virtual Machine** space.
      
      **NOTE**
      
      The physical instances need to be configured in Threat Defense for AD before configuring a Deployment Manager.
• Provide a **Deployment Manager Name** for this Deployment Manager. Symantec recommends to follow a naming convention to reflect the domain in the Deployment Manager name. For example, Domain 1.DM1

  **NOTE**

  If you receive an error **invalid validation**, there may be a problem with the domain name entered.

• Provide the credentials for a Deployment Manager account in the **Privileged Domain Username** and **Password** space.

  To make a user from the other AD domain a local administrator on your computer

e) Press **Next**.
f) In the **Select Log Method** tab, do the following:

  • Select **WMI Collector** from the **Log Method** drop-down list.
Enter 15 seconds as the **Collection Interval** for log collection. This is the most common method of log collection and time frame. You can change the log collection method to your preferred method.

**Changing the log method of a Deployment Manager**

g) Press **Done**.

The domain is added to your Threat Defense for AD environment and is listed in the **Domains** setting.
Configuring Alarms in Symantec Endpoint Threat Defense for Active Directory

About Alarms

An alarm is generated in Threat Defense for AD when a misconfiguration in the AD or a vulnerability is detected. When the same endpoint generates multiple events for the same type of attack within 15 minutes, an alarm is generated. View the alarms, the real-time details of an alarm, and AD assessment results in the Alarms page of the console. You can also navigate to the Alarms page from the Overview page of the console. Press the Alarms icon in the menu to view the Alarms page.

The generated alarms are categorized and listed under the following tabs on the Alarms page:

- **Inbox**
- **Resolved**
- **Archive**

**Inbox**

By default, you view the Inbox tab when you select the Alarms option in the console. The alarms that are generated are listed under the Inbox tab. The two types of alarms that are generated in your Threat Defense for AD environment are as follows:

- **Alarms**
  The breach prevention alarms are listed under this section. On threat detection, the members of your security team are notified through an email, a syslog event is sent to the Security Information and Event Manager (SIEM), and an alarm is generated. An on-demand memory scan is initiated of the endpoint that is compromised, gathering key process and forensic information. Press an alarm to view the details of that alarm.

  Types of breach prevention alarms

- **Dark Corners**
  Dark corner alarms are generated when the AD Assessment scan detects a misconfiguration or a vulnerability in the AD. Press an alarm to view the details of that dark corner alarm.

  Introducing dark corners of the Active Directory

**Resolved**

The dark corner alarms that are remediated are listed under the Resolved tab. A dark corner alarm automatically moves to the resolved tab when you take actions to mitigate that dark corner. For the alarm to list under the Resolved tab, the dark corner scan must be re-run again after mitigation.

  Introducing dark corners of the Active Directory

**Archive**

Alarms that you acknowledge and archive are listed here. You can archive alarm if you decide that the alarm is not relevant anymore, or archive the older alarms that were generated. The Archive tab lists all the archived breach prevention alarms and dark corner alarms.

To archive an alarm, navigate to the Alarms > Inbox page in the console. Select the alarms that you want to archive and press the Archive icon.
To move an archived alarm back to the inbox, navigate to the Alarms > Archived page in the console. Select the alarms that you want to move and press the Inbox icon.

Introducing dark corners of the Active Directory

Responding to an alarm in Threat Defense for AD

When Threat Defense for AD generates an alarm, you need to evaluate the incident and respond.

1. You may want to provide the Forensic JSON file from the Core server if an alarm is generated from a non-testing environment. The file is named the (date\time of the alarm).json and it resides in \Program Files\Symantec \Endpoint Threat Defense for AD\forensicFiles.
2. Check the forensics report and decide if you want to mitigate to contain a process or wait for feedback from Symantec.
3. Determine the effects of disabling the user and endpoint account, or removing the system from the network.
4. Review the Kerberos tickets. You can find the tickets at Forensic Report > Current Status > Kerberos Tickets. Disable the user and the endpoint accounts that actively revoke the tickets inside the suspicious endpoint. Re-enable the accounts and change the password.
5. Evaluate if you can clean the malware from the endpoint, else the endpoint must be wiped or re-imaged.
6. Contact Broadcom Support team of the attack to develop a prevention mechanism to guard against future infections.

Types of breach prevention alarms

When a breach is detected on an endpoint by Threat Defense for AD's Endpoint Trap deception technology, an alarm is generated. The types of breach prevention alarms are as follows:

<table>
<thead>
<tr>
<th>Alarm Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User Information Gathering</strong></td>
<td>This alarm is generated when Endpoint Trap detects user information gathering on an endpoint.</td>
</tr>
<tr>
<td><strong>Computer info Gathering</strong></td>
<td>This alarm is generated when Endpoint Trap detects computer information gathering on an endpoint.</td>
</tr>
<tr>
<td><strong>Credential Theft using Overpass-the-Hash</strong></td>
<td>This alarm is generated when Endpoint Trap detects credential theft using overpass-the-hash to gain a valid Kerberos ticket.</td>
</tr>
<tr>
<td><strong>Credential theft using Pass-the-Hash</strong></td>
<td>This alarm is generated when Endpoint Trap detects credential theft using pass-the-hash to authenticate an user using the NTLM protocol.</td>
</tr>
<tr>
<td><strong>Credential Theft using Pass-the-Ticket</strong></td>
<td>This alarm is generated when Endpoint Trap detects credential theft using pass-the-ticket to gain access to the target endpoint.</td>
</tr>
<tr>
<td><strong>Brute Force Alarm</strong></td>
<td>This alarm is generated when Endpoint Trap detects failed authentication attempts from an endpoint that is outside the AD domain using common usernames. The alarm is generated after 3 failed authentication attempts within 15 minutes.</td>
</tr>
<tr>
<td><strong>Untrusted LDAP Binding</strong></td>
<td>This alarm is generated when Endpoint Trap detects an attempt by an untrusted application to query the AD and perform reconnaissance activities. Investigate the source endpoint for more information.</td>
</tr>
</tbody>
</table>
### Alarm Type: Malicious DCShadow Replication Attack
This alarm is generated when privileged attackers try to imitate a Domain Controller's replication ability to push hidden changes in the domain environment. This allows them to stay stealth while changing AD objects and creating hidden spots without being logged.

### Alarm Type: Malicious DCSync Replication Attack
This alarm is generated when privileged attackers try to imitate Domain Controller's replication ability to perform domain sync directly from the NTDS database. Performing the domain sync lets the attacker potentially obtain every domain accounts' hashes. This may lead to Pass-The-Hash or Golden Ticket attacks using the stolen hashes.

### Alarm Type: Possible Golden Ticket Attack
This alarm is generated when attackers are generating Kerberos tickets using unknown domain principal. This can indicate that an attacker is creating and using a Golden Ticket.

All credential theft alarms have an item that matches the deception accounts. Only a deception account can perform Pass-The-Hash and Over-Pass-The-Hash because no other masked credentials exist in Local Security Authority Subsystem Service (lsass). You can simulate these attacks for testing purposes.

### Testing the Threat Defense for AD environment

#### Over-Pass-The-Hash(OPTH) and Pass-The-Hash(PTH) alarms
The underlying action that generates an event determines the type of alarm that is generated. OPTH is a request for a ticket granting ticket (TGT) from the domain controller and is a Kerberos event. PTH is used to pass the password hash to a service, which the old NTLM protocol accesses.

Depending on the configuration, both OPTH and PTH or either one type of alarms are generated:

#### Table 16: Examples of the OPTH and PTH alarms

<table>
<thead>
<tr>
<th>Alarm type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPTH</td>
<td>This alarm is generated with simple brute force because you fail to logon with the password. The domain controller registered an authentication attempt or TGT request. You could have used a random password or stolen it out of lsass.</td>
</tr>
<tr>
<td>PTH</td>
<td>This alarm is generated if you steal the NTLM hash and perform a PTH in an attempt to go straight for a service, which then fails.</td>
</tr>
<tr>
<td>PTH and OPTH</td>
<td>This alarm is generated if you PTH into another command shell, and then try to gain access to a service. The PTH fails and can be followed by OPTH because an authentication or TGT request can occur depending on what you are attempting to do. OPTH or PTH occurs for a deception account depending on the behavior you exhibit.</td>
</tr>
<tr>
<td>Neither PTH nor OPTH</td>
<td>Except for the deception account, for any masked object you can never have PTH or OPTH because there is no password or hash to steal in Microsoft's Local Security Authority Subsystem Service. These activities are always &quot;User Information Gathering&quot; through a simple brute force. You cannot pass or steal information that is not actually there.</td>
</tr>
</tbody>
</table>

### Viewing the details of an alarm
View the alarms generated in the **Inbox** tab of the **Alarms** page of the console. All the breach prevention and dark corner alarms are listed in this page for you to review. Press an alarm to view the alarm details.

- Alarms displayed in Inbox tab
- Viewing the details of an alarm
- Viewing an alarm on the SEP console

### Alarms displayed in Inbox tab
The following information about the alarms is displayed on the page:

Table 17: Parameters of the alarms listed under the Inbox tab

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Type</td>
<td>Displays the type of attack for which the alarm is generated.</td>
</tr>
<tr>
<td>AD Domain</td>
<td>Displays the attacked endpoint's AD domain name.</td>
</tr>
<tr>
<td>SEPM Domain</td>
<td>Displays the domain name of SEPM.</td>
</tr>
<tr>
<td>Attack Source</td>
<td>Displays the name of the attacked endpoint.</td>
</tr>
<tr>
<td>Forensics</td>
<td>Displays the option to view the forensics report for the attack.</td>
</tr>
<tr>
<td></td>
<td>Note: This option is displayed only if the forensics scan starts when the alarm is generated. You can also run an on-demand forensics scan.</td>
</tr>
<tr>
<td>Risk Severity</td>
<td>Displays the risk severity of the attack.</td>
</tr>
<tr>
<td>The date and time of the alarm.</td>
<td>Displays the full date and the time of the generated alarm.</td>
</tr>
</tbody>
</table>

Press an alarm to view the details of an alarm, which are as follows:
Table 18: Details of an alarm

<table>
<thead>
<tr>
<th>No.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The Alert ID number and the date and time of the generated alarm is displayed.</td>
</tr>
<tr>
<td>2</td>
<td>Information on the endpoint that initiated the attack and the IP address of the endpoint is displayed.</td>
</tr>
<tr>
<td>3</td>
<td>The suspicious processes involved in the attack is displayed. <strong>Note:</strong> Suspicious processes are only displayed if the forensics scan runs automatically after the alarm is generated.</td>
</tr>
<tr>
<td>4</td>
<td>The components and compromised AD objects for which the alarm is generated is displayed.</td>
</tr>
<tr>
<td>5</td>
<td>If multiple endpoints are involved in an attack, then the generated alarm displays a list of the attacked endpoints.</td>
</tr>
<tr>
<td>6</td>
<td>The domain controller from which the events were collected to generate the alarm is displayed.</td>
</tr>
<tr>
<td>7</td>
<td>The options to run a forensics scan or view the forensics report is displayed.</td>
</tr>
<tr>
<td>8</td>
<td>The risk severity of the alarm is displayed. Alarms with <strong>High</strong> risk severity are automatically mitigated if Auto-mitigation is enabled in the deception policy. <strong>Configuring a deception policy</strong></td>
</tr>
<tr>
<td>9</td>
<td>Displays the description of the alarm.</td>
</tr>
<tr>
<td>10</td>
<td>Displays the alarms that this attacked endpoint generated in the last 3 hours.</td>
</tr>
</tbody>
</table>

**Viewing an alarm on the SEP console**

You can view the generated alarms in the SEP console. The alarms are displayed on the **Home Screen > Security Status > View Notifications** page in the SEP console.

**Generating a forensics report**

A few seconds after an alarm is triggered, the forensics report is generated. The report is a snapshot of the endpoint at the time of the attack and runs only after the first event within a 15-minute window, per source endpoint. For example, if the attacker creates multiple events or alarm types from a single endpoint, a new forensic report does not appear until the next event occurs after 15 minutes. The forensic JSON files are stored on the Core server as **report#.json** at the following path:

```
\ Program Files\Symantec\Endpoint Threat Defense for AD\forensicFiles.
```

The forensics report is generated in 3 stages. You can start viewing the forensics report when the first stage of the report generation is complete.

The **Forensics Report** has the following columns:
### Table 19: Columns in the Forensics Report

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory Analysis</td>
<td>The scanned memory map, with detailed malware analysis data about each suspicious process found in user space.</td>
</tr>
<tr>
<td>Persistence and Autoruns</td>
<td>All possible collected persistence methods that are found on the endpoint.</td>
</tr>
<tr>
<td>File System</td>
<td>The latest changes in files stored in the location that often hosts a malware.</td>
</tr>
<tr>
<td>Win Artifacts</td>
<td>Casual OS-related forensics items.</td>
</tr>
<tr>
<td>Current Status</td>
<td>Volatile forensics data collections.</td>
</tr>
<tr>
<td>Authentication Activity</td>
<td>Forensics data that are collected from Windows events logs.</td>
</tr>
<tr>
<td>Evidence of execution</td>
<td>Evidence of executing executables on the endpoint.</td>
</tr>
</tbody>
</table>

### To generate a forensics report

1. Navigate to the **Alarms > Inbox** tab in the console.
2. Press **See Report** or **View Partial Report** next to the alarm for which you want to generate a forensics report.
   
   Or

3. To run an on-demand forensics scan, press on an alarm in the **Inbox** tab and press **View Report** under **Forensics Report**.
   
   **NOTE**
   
   You see the **View Partial Report** option only when you request for an on-demand forensics report.

4. The **Forensics Report** page is displayed. The following information is displayed on the page:
   
   - The type of alarm.
   - The source computer.
   - Timestamp of the alarm.
   - Users that are logged on at the time of the attack.
   - If you are viewing a partial forensics report, you see the message **In Progress** and the status of the forensics report.

5. Press **Pdf** or **JSON** in the console to download the report in the respective format.
   
   **NOTE**
   
   The PDF report contains less data than the console report or the JSON file.
You can re-run a forensics report if a forensics report has an error or is incomplete. The new forensics report overwrites the previous report.

If you have secured boot enabled on your devices, you can download the measured boot logs from this page. Measured boot logs are available on the Forensics page of console in an XML file format. The measured boot logs need to be deciphered to identify any compromises due to rootkits or other malicious tools that may have occurred in the environment. Contact Broadcom support team for assistance.

To re-run a forensics report, navigate to the Alarms > Inbox tab in the console.

- Press on alarm to view the alarm's details.

Components of a forensics report

Alerts in forensics are cross-referenced with numerous malware databases like Virus Total, using smart algorithms and a patent pending memory scan. The engine investigates the endpoint memory to find deception elements or other malicious code that indicates attempts to perform privilege escalation, lateral movement, and reconnaissance. The forensics suite operates with native protocols like WMI and SMB and is completely agentless.

The following columns are seen in the forensics report:
### Table 20: Columns in a forensics report

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Memory Analysis</strong></td>
<td>Lists the suspicious processes in the attacked endpoint’s memory:</td>
</tr>
<tr>
<td></td>
<td>• Threat Overview</td>
</tr>
<tr>
<td></td>
<td>• Mitigating an attack process from the console</td>
</tr>
<tr>
<td></td>
<td>• Indicators of Compromise (IOC)</td>
</tr>
<tr>
<td><strong>Persistence &amp; Autoruns</strong></td>
<td>Lists several areas on the source endpoint that could indicate persistence:</td>
</tr>
<tr>
<td></td>
<td>• Startup Folder Autoruns</td>
</tr>
<tr>
<td></td>
<td>• Local Services</td>
</tr>
<tr>
<td></td>
<td>• WWI Subscriptions</td>
</tr>
<tr>
<td></td>
<td>• Registry Autoruns</td>
</tr>
<tr>
<td></td>
<td>• Scheduled Tasks</td>
</tr>
<tr>
<td></td>
<td>An attacker may manipulate these areas in Windows to have malware or other programs start automatically. Persistence &amp; Autoruns in a forensics report</td>
</tr>
<tr>
<td><strong>File System</strong></td>
<td>Lists several areas on the source endpoint that could indicate malware activity:</td>
</tr>
<tr>
<td></td>
<td>• Last Changed System Files</td>
</tr>
<tr>
<td></td>
<td>• Last Changed Temporary Files</td>
</tr>
<tr>
<td></td>
<td>These represent a location that often hosts a malware.</td>
</tr>
<tr>
<td><strong>Win Artifacts</strong></td>
<td>Lists the Casual Operating System related forensics items:</td>
</tr>
<tr>
<td></td>
<td>• Local User Accounts</td>
</tr>
<tr>
<td></td>
<td>• Connected USB Endpoints</td>
</tr>
<tr>
<td></td>
<td>• Active Network Adapters</td>
</tr>
<tr>
<td></td>
<td>• Run key History</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Office History</td>
</tr>
<tr>
<td></td>
<td>• Host Files</td>
</tr>
<tr>
<td></td>
<td>• USB Endpoints History</td>
</tr>
<tr>
<td></td>
<td>• PowerShell 5 Command-Line History</td>
</tr>
<tr>
<td></td>
<td>• Browser History</td>
</tr>
<tr>
<td></td>
<td>• Download History</td>
</tr>
<tr>
<td></td>
<td>Security responders or investigators may use this information to determine how an infection arrived on the endpoint. Win Artifacts in a forensics report</td>
</tr>
<tr>
<td><strong>Current Status</strong></td>
<td>Lists the ongoing processes and credentials in memory:</td>
</tr>
<tr>
<td></td>
<td>• Process List: Lists every running process at the time of the attack.</td>
</tr>
<tr>
<td></td>
<td>• Advanced Network Statistics: Displays the port of any running process that is connected to a network. This information is helpful to restore Firewall alarms. Current Status in a forensics report</td>
</tr>
<tr>
<td></td>
<td>• Kerberos Tickets in Memory: Informs you of accounts that need to change the passwords.</td>
</tr>
<tr>
<td></td>
<td>• Pass-The-Hash Attempts</td>
</tr>
<tr>
<td><strong>Event Logs</strong></td>
<td>Lists things of interest from the event logs:</td>
</tr>
<tr>
<td></td>
<td>• Windows Event Drivers</td>
</tr>
<tr>
<td></td>
<td>• Windows Event Local Services</td>
</tr>
<tr>
<td></td>
<td>• Windows Event Secclear</td>
</tr>
<tr>
<td></td>
<td>• Windows Event Syscclear</td>
</tr>
<tr>
<td></td>
<td>• Windows Event Software Install</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Evidence of Execution</td>
<td>Lists the records of executables:</td>
</tr>
<tr>
<td></td>
<td>• Shim Cache Entries</td>
</tr>
<tr>
<td></td>
<td>• Amcache Entries</td>
</tr>
<tr>
<td></td>
<td>• Recent File Cache Entries</td>
</tr>
<tr>
<td></td>
<td>• Prefetch Analysis</td>
</tr>
<tr>
<td>Screenshots</td>
<td>Collects a screenshot image of the host endpoint during an attack</td>
</tr>
<tr>
<td></td>
<td>The forensics report automatically collects a screenshot image of the host endpoint at the time of the attack. The Screenshots tab contains columns such as Session ID, Username, and Image. Compressed images not more than 150KB can be embedded through this tab of the report.</td>
</tr>
</tbody>
</table>

Memory Analysis in a forensics report

Memory Analysis in a forensics report

Memory Analysis tab opens by default when you open the Forensics Report console. Memory analysis represents the parent and child processes in the endpoint's memory at the time of the attack. Suspicious processes are highlighted in yellow and red, with red being the process that most likely causes the alarm. Suspicious items may include an Indicator Of Compromise (IOC), or presence of a mask item within the memory space of that process. At the top of the page, the users that were logged on the source endpoint at the time of the attack are listed. Press on the highlighted process for more information.

You see the following in the image:

Table 21: Components displayed in the image

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Memory Analysis</strong>: This tab opens by default when you open the forensics report.</td>
</tr>
<tr>
<td>2</td>
<td>The suspicious process found in the endpoint's memory is displayed. Press the suspicious process to view the Malware Analysis Report. Viewing a Malware Analysis Report</td>
</tr>
<tr>
<td>3</td>
<td><strong>MalRank</strong> displays the probability of this process containing a malicious code.</td>
</tr>
<tr>
<td>4</td>
<td>The indicators of compromise are displayed. Hover over the icons to display what the icons stand for. <strong>Indicators of Compromise (IOC)</strong></td>
</tr>
</tbody>
</table>
The icons listed under IOC are counters seen in the **Memory Analysis**. The counter categories are listed in the following image:

<table>
<thead>
<tr>
<th>Forensic Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Line Shell</td>
<td>A suspicious command shell was executed from a process</td>
</tr>
<tr>
<td>Malware</td>
<td>A known malicious code was identified inside the process</td>
</tr>
<tr>
<td>Deception</td>
<td>Deceptive objects were used inside the process</td>
</tr>
<tr>
<td>Lateral Movement</td>
<td>A lateral movement attempt was detected in the process</td>
</tr>
<tr>
<td>Reconnaissance</td>
<td>Recon attempt was detected inside the process</td>
</tr>
<tr>
<td>Privilege Escalation</td>
<td>Privilege escalation was detected in a process (2 types: local and domain escalations)</td>
</tr>
<tr>
<td>Local Persistence</td>
<td>A persistence was found in the system</td>
</tr>
<tr>
<td>Network Connectivity</td>
<td>Malicious communication was detected from one or to one of the processes</td>
</tr>
</tbody>
</table>

Components of the **Threat Overview** in the forensics report are shown in the following image:
**MalRank:** is the malicious process rank of a threat. Threats with a higher MalRank are automatically mitigated by Threat Defense for AD.

MalRanks of malicious processes are calculated based on the following parameters:

- Yara Rules Analysis
- Deception object from an alarm that resides in the memory sections of an endpoint.
- Recon and lateral movements strings
- Loaded Dynamic-Link Libraries (DLL)
- Executable static analysis (Parent process, Privileges, Parameters, Execution Path)
- Virus Total Hash Lookup
- Active network connections
- Indicators of Compromise (IOC)

**Indicators of Compromise (IOC)**

Suspicious items are highlighted in yellow or red throughout the report, red being more severe threats. Suspicious items may include an IOC or the presence of a mask item within the memory of that process. Items highlighted anywhere within the forensics report are always summarized under the **IOC Triangle** at the bottom of page. Press the IOC triangle at the bottom of the page to view the highlighted summary.

The list of IOCs are as follows:

- Suspicious Arguments
- Double Extensions
- Executable Running from remote / temp path
- Suspicious Strings
- Malicious Processes found by Malware Analysis
- Abnormal Processes
- Obfuscation
- Injected Kerberos Tickets
- Pass-The-Hash Attacks
- Suspicious Loaded DLLs
- Possible Double Extension Filename
Viewing a Malware Analysis Report

Press on a suspicious process on the forensics report page to view the **Malware Analysis Report**. The report has details about the offending processes.

Malware Analysis Report

Overview

<table>
<thead>
<tr>
<th>Process Name</th>
<th>powershell.exe</th>
</tr>
</thead>
<tbody>
<tr>
<td>PID</td>
<td>5696</td>
</tr>
<tr>
<td>PPID</td>
<td>2192</td>
</tr>
<tr>
<td>Path</td>
<td>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</td>
</tr>
<tr>
<td>MDS</td>
<td>DJF8FAD829D287BD596C450MK46E43E7BD</td>
</tr>
<tr>
<td>User Token</td>
<td>KKK4Jyal</td>
</tr>
<tr>
<td>VirusTotal Hash Lookup</td>
<td>0/69</td>
</tr>
<tr>
<td>YARA Malware Rules</td>
<td>0 Rule(s) Match</td>
</tr>
<tr>
<td>Execution Time</td>
<td>December 9th, 2019, 2:25:15 AM</td>
</tr>
<tr>
<td>Description</td>
<td>Windows PowerShell</td>
</tr>
<tr>
<td>Version</td>
<td>16.0.32214.1 (Winbuild.160701.0800)</td>
</tr>
<tr>
<td>Author</td>
<td>Microsoft Corporation</td>
</tr>
</tbody>
</table>

Command Line Parameters

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
```

**VirusTotal Hash Lookup** informs you if the attacking process is a known malware with a hash on Virus Total (crowd sourced known malware repository). This information is not available if the server does not have Internet connectivity.

**YARA Malware Rules** informs you if any activity matched the YARA rules database. The ability to import your own YARA rules will be available in a future release. For Windows console shells, a shell memory dump is included.

**Malware Analysis Report** also collects shell history from all Windows shell consoles, including CMD.exe, PowerShell, and Python. You can view the last commands run in the corresponding shell, and the results that are returned to the attacker scrolling through the **Shell Content**.

Depending on the OS, this information may be stored on the source endpoint in the conhost process. This process may be a child of the shell process, or it may be listed further down the interface at the parent level.

Persistence & Autoruns in a forensics report

Persistence & Autoruns in a forensics report

The forensic engine collects and displays additional information of an attack a few moments after the attack is initiated in the **Persistence & Autoruns** column. This information is hidden and only unique or suspicious findings on the endpoint are displayed. If you still want to view this data, uncheck the **Hide Default Values** option. You can create a query in each column and add custom filters to view the data.
The file Commands.txt is present on the Documents directory of the core server. It contains several examples of other commands and scenarios. Execute these attacks to test your Threat Defense for AD environment.

Path: C:\Program Files\Symantec\Symantec Endpoint Defense for Active Directory\Documentation

This file contains several examples of other commands and attack scenarios. You can execute these attacks to test your Threat Defense for AD environment.

If the results are unexpected, please contact Broadcom Support team for clarification on the attempted attacks and an explanation on the results.

Current Status in a forensics report

The Current Status column in the forensics report displays the on-going processes and credentials in the endpoint's memory. The following components are seen in the Current Status column and can be manipulated:

Table 22: Components of the image

1. **Hide Default Values**: By default, the "Windows Values" is hidden for all components except Memory Analysis in the forensics report. Unchecking the Hide Default Values check box in the upper right-hand corner to restore the values.

2. **Suspicious Values**: Any suspicious values that Threat Defense for AD has retrieved from the forensics scan is marked in red on your suspicious workstation. Items on endpoints can be suspicious for various reasons.

3. **Filtering**: You can filter the results for each tab and timestamp filters for dates. Select each column to apply the filter.

4. **Drop-down icon**: Displays general information about the suspicious item.

Other components displayed in the console are as follows:
Table 23: Other components of the Current Status tab

<table>
<thead>
<tr>
<th>Process List:</th>
<th>Displays the number of running processes at the time of the attack.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Network Statistics:</td>
<td>Shows the ports of any running process that are connected to the network, which is used for reconciling with firewall alarms.</td>
</tr>
<tr>
<td>Kerberos Tickets in Memory:</td>
<td>Informs you of any accounts that need to have the password changed. When all the accounts listed here are compromised, an alarm is generated.</td>
</tr>
</tbody>
</table>

**Mitigating attacks manually**

Attack processes can be contained on an endpoint through mitigation. Use the **Mitigate** option in the forensics report to mitigate an attack. You can also enable the auto-mitigation capability through the deception policy. Mitigation involves copying and executing a file on the source endpoint. Mitigation disables the ability to spawn another process, overwrite a part of the memory, run recon commands, or communicate to the network.

Threat Defense for AD automatically mitigates only the PowerShell.exe, Mimikatz.exe, CMD.exe, PsExecSVC.exe, regsvr32.exe, python27.exe, wce.exe, xcmd.exe processes.

You can mitigate processes manually, or enable the **Auto Mitigate** option when you configure a deception policy. Attack processes are automatically mitigated on any host endpoint after the forensics are completed, if the endpoint is assigned this deception policy.

**Configuring a deception policy**

**To mitigate processes manually**

1. Navigate to the **Alarms** page in the console and press **See Report** next to an alarm.
2. Press **See Report** under **Full Detailed Report** to view the forensics report.
3. Under the **Memory Analysis** tab in the forensics report, press **Mitigate**.
4. Check the boxes against the processes highlighted in red and press **Mitigate Process**

After the mitigation is complete, the process is highlighted in blue and has a lock icon.

You receive an **Access is denied** message when you try to spawn another process, overwrite another part of memory, run recon commands, or communicate out to the network on the source host.
The command completed successfully.

C:\Windows\system32\ping \win31m
ping \win31m could not find host \win31m. Please check the name and try again.

C:\Windows\system32\ping \win31m

C:\Windows\system32\
Dark Corner alarms in Symantec Endpoint Threat Defense for Active Directory

Introducing dark corners of the Active Directory

Dark corners are misconfigurations and vulnerabilities that are found in your environment. The Active Directory (AD) assessment scan searches for these dark corners to protect the AD and reduce attack surface. Learn more about the configurations that are related to dark corners, and the identification of dark corners through AD assessment scan searches. Symantec Endpoint Threat Defense for Active Directory generates dark corner alarms that are listed in the Alarms and Overview pages of the console.

About Active Directory assessment

The AD Assessment generates the dark corner alarms. The assessment scan of an AD detects any misconfigurations, vulnerabilities, or stealth entries into the AD that are known as dark corners. Dark corners can be detected on devices, domain controllers, or the domain databases.

In the Alarms page, press the displayed alarm to open and view the alarm details. The dark corner alarm information contains:

- Explanation of the attack
- Potential threat that the attack can cause
- How to mitigate the attack

If you do not want to take action on a specific dark corner as that is required for the business, you can press the Unmanage option next to the the alarm.

Archived Alarms

Acknowledged alarms are known as archived alarms, and are displayed under the Archived tab of the Alarms page. Unmanaged dark corners are also displayed under the Archived tab.

To restore an archived alarm to inbox

1. To restore an archived alarm to inbox, do the following:
   a) In the Alarms page of the console, press the Archived tab.
   b) Under Source Element, select the alarm that you want to restore to the Inbox.
   c) Press the Manage.
      The managed alarm is listed under the Inbox tab.

Re-running a dark corner

The dark corners can highlight accounts that can be compromised. For privileged accounts, an attacker has considerable time to steal the credentials as the passwords of these accounts do not expire. You must change your passwords of the privileged accounts to prevent credential theft. After changing the passwords, re-run the dark corner scans manually, if the scan does not run automatically.
2. To re-run a dark corner scan manually, do the following:
   a) Press the Re-Run Dark Corner option on the Alarms page.
   b) In the console menu, press the Analytics icon.
   c) Press the Service and Components tab on the console.
   d) Under Components, search for Dark Corners.
   e) Press the Re-Run option for dark corners

All dark corners run again and the updated events are displayed in the console. A remediated dark corner is moved and is listed under the Resolved tab.

Resolved Alarms
When an event that triggered an alarm is remediated, the alarm moves under the Resolved tab. Press the alarm to view the information on the event that triggered the alarm.

Domain dark corners
The AD assessment scan looks for misconfigurations in the AD database. The misconfigurations detected in the AD database trigger the domain dark corner alarms.

SYSVOL Attack
When a user logs on, Group Policy Preferences (GPP) allows an administrator to configure local administrator accounts, schedule tasks, and mount network drives with specified credentials. GPPs are written to the SYSVOL share of the domain controllers. An attacker can gain access to the GPP xml files inside the SYSVOL share and extract the specified credentials that are stored in the GPP.

Potential threat
An attacker can gain the same privileges of the accounts it extracts from the GPPs. Accounts that are used for the GPPs typically have local admin user rights for every computer.
To mitigate
1. Disable risk-prone features from the Microsoft RSAT using MS14-025.
2. Review the active GPPs list and make sure to delete them.
3. Maintain password rotation using Invoke-PasswordRoll script

Hidden Security Identifier (SID)
Abuse of an AD "SID History" object enables an attacker to inherit permissions from other high-privileged SID accounts or groups without any trace of additional group membership for the user.

Potential threat
Using a "Hidden SID" attribute can indicate that the attacker is trying to hide high-privileged group membership in a low-privileged account to conceal a post-exploitation, domain persistence backdoor.

To mitigate
1. Delete the suspicious object to remove the persistence.
2. Delete the SID History attribute of the suspicious user:
   

Golden Ticket
If an attacker has the long-term key for the "krbtgt" account, they can forge a logon TGT with any user rights. The ticket can contain a fictitious username with domain admin membership or any other membership that the attacker chooses.

Potential threat
An attacker can gain any type of privileges for any service or computer in the network and can use it everywhere. These privileges can last as long as the “krbtgt” account is not reset.

To mitigate
1. Reset the long-term key for the ‘krbtgt’ account after every six months.
2. To reset the krbtgt account immediately, press the following link:

DCSync/DCShadow Backdoor Account
Adding a low-privileged user to the domain replication object gives them access to all domain sensitive data without being a high-privileged user. Replication permissions must be assigned to AD objects because certain domain services require domain replication capabilities.

Potential threat
An attacker can gain full access to the entire domain user account database.

Remove the suspicious user from the domain replication object.

https://support.microsoft.com/en-us/kb/303972

Unprivileged Admin Holder ACL
Attackers can abuse the AdminSDHolder ACLs by adding unprivileged users to the AdminSDHolder security object with full control or write permissions. On receiving this access, the unprivileged user is able to add themself or other users to powerful groups, such as Domain Admins, without having high-privileges.

Potential threat
Enabling and modifying this feature would allow an attacker to leave hidden administrator privileges on the domain controller, without using domain accounts.

Remove the suspicious user from the AdminSDHolder security object.

https://support.microsoft.com/en-us/kb/817433

**Power User Enumeration**

Authenticated users can enumerate any object in the domain. Enumerating users have a password that never expires, and could reveal high-privileged users in the domain.

**Potential threat**

These credentials allow an attacker to gain access to high privileges in the network that can last for a very long time.

**To mitigate**

1. High-privileged users must change passwords more frequently.
2. **Domain Admins** must also be protected with complicated passwords.
3. The password should have at least 14 characters, include lowercase and uppercase letters, numbers, and symbols.

**Anonymous LDAP Binding**

Unmanaged endpoints can create queries in the AD and gather information on the domain environment without authentication.

**Potential threat**

Attackers can view the entire directory structure and permissions from an unauthenticated user and computer with a network connection.

**To mitigate**

1. In ADSI edit tool, change the properties of the object to:

   "CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=[yourdomain]".

2. Replace the attribute value of “dSHeuristics” without 2 with 0 on the 7th digit

**AS-REP Roasting**

Attackers can look up for privileged accounts with the **Do not use Kerberos pre-authentication** attribute enabled. They can receive an AS-REP ticket with weak encryption that they can decode offline and receive the password of this account, using tools such as ASREPRoast by Harmj0y.

**Potential Threat**

Kerberos pre-authentication prevents offline password guessing. While the AS-REP ticket itself is encrypted with the service key, the AS-REP "encrypted part" is signed with the key of the user we send an AS-REQ (client key). If pre-authentication is not enabled, an attacker can send an AS-REQ for any user that does not have pre-authentication required. The attacker receives a bit of encrypted material back that can be cracked offline to reveal the target user’s password, without any domain controller involved in the process.

**To mitigate**

1. In ADSI Edit tool, change the properties of the object:

   "CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=[yourdomain]".
2. Replace the attribute value of “dSHeuristics” without 2 with 0 on the 7th digit.

**Cached Privileged Account in RODC**

Attackers might compromise the whole domain from an unsecured site covered with Read-Only Domain Controller (RODC). The attack is executed by dumping the secrets of the cached privileged accounts in the RODC NTDS, or using DCSync towards the read-only domain controller. If those secrets are exposed, attackers can perform lateral movement in the whole domain.

**Potential Threat**

Read-only domain controllers are usually deployed in unsecured sites and are considered untrusted. Therefore, privileged accounts secrets should not be saved in the RODC NTDS AD database. Once the untrusted site is compromised, existence of cached AD privileged accounts secrets does not limit the attacker to the untrusted site. They can dump the read-only domain controller cached secrets and compromise the whole domain.

**To mitigate**

1. Open the **Active Directory Users and Computers** console.
2. Go to the **Domain Controllers** container.
3. Right click on your **RODC**, go to **Password Replication Policy**.
4. Select the vulnerable privileged account.
5. Press **Remove**.
6. Press **Yes**

**Trusted Domains**

Attackers can infiltrate into your network through trusted domains. Verify that you trust and know all the domains and try to limit the number of trusted domains with transitive trust.

**Potential Threat**

Understanding the connections in your domain is crucial to determine the risk that is included in trusting other forests and domains. Compromising a trusted domain could lead to compromise the whole trust network. When trusting a domain, you might also trust the domains that it is trusting, making a possible unwanted connection.

Limit the bidirectional trusts in your domain network.

**SID Filtering Disabled For Domain Trusts**

SID Filtering between trusting domains is a mechanism that denies unwanted access by users from one domain to another. If SID filtering is disabled, an account can mimic the privileges of any account from the trusting domain through the "SIDHistory" attribute, elevate their privileges and compromise the trusting domain. Once the trusted domain has been compromised, the trusting domain can be easily compromised as well. SID Filtering should never be disabled, except for in rare cases during the migration of the domain.

**Potential Threat**

Once the trusted domain has been compromised, if SID Filtering is disabled, the trusting domain can be easily compromised as well.

From the trusting domain, type this command using high privileges:

```
Netdom trust [TrustingDomain] /domain:[TrustedDomain] /enablesidhistory:no
```
Privileged Foreign Account
Attacks who have compromised a "foreign trusted domain" can use this account to perform a privileged lateral movement from a trusted domain to the current domain.

Potential Threat
The perimeter of your AD domain network is breached. Using these accounts, attackers can easily navigate from a foreign trusted domain to your domain and compromise it.

To mitigate
1. Open the Active Directory Users and Computers console.
2. Go to the mentioned group.
3. Remove the mentioned foreign user from that list

DNS MITM
Attack explanation
Attackers can leverage DNS wildcards to register a record that responds to any unknown host resolution attempts and performs MITM attack. Discover wildcard DNS records that respond with the IP address to any unresolved DNS request. Anyone in the domain can create a record of this type and put your endpoint at risk with MITM scenarios.

Potential threat
Every endpoint in the network is exposed to MITM scenarios.

To mitigate
1. Open the DNS Manager console in your DNS server.
2. Go to the Forward Lookup Zone and the relevant zone.
3. Find the wildcard record and delete it

Hidden ACL
Attackers might gain control over privileged Domain Users, groups, and computers using a weak object. Discover abnormal aces that allow high privileged access using normal, weak accounts, over privileged accounts. In the v3.3 release, the discovery is limited to users only.

Potential threat
Attackers have hidden paths to hunt administrators and gain privileged access in your domain.

Examine the vulnerable objects security configuration using the Active Directory Users and Computers tool. Delete or modify the relevant ACL entry and limit the permissions.

Domain controller dark corners
AD assessment scans the domain controller and looks for misconfigurations. The misconfigurations detected in the domain controllers generate the domain controller dark corner alarms.

Vulnerable Domain Controller MS14-068
The remote privilege elevation vulnerability MS14-068 exists in implementations of Kerberos KDC in Microsoft Windows. The vulnerability arises when the Microsoft Kerberos KDC implementations fail to validate signatures properly. The improper validation of signatures lets an attacker to modify an existing valid domain user logon token. For example, adding false statements that the user is a member of domain groups such as Domain Admins.
Threat Defense for AD may not detect this dark corner if you configure a Domain Admin equivalent account.

**Potential threat**

This vulnerability lets an attacker to elevate privileges from any unprivileged domain user account to a domain administrator account.

**To mitigate**

- MS14-068 update addresses the vulnerability by correcting signature verification behavior in Windows implementations of Kerberos.

This update must be installed on all domain controllers in the enterprise.

**DSRM logon Enabled**

DSRM is a special boot mode for repairing or recovering the AD when the directory services are down. Enabling and modifying this feature allows an attacker to leave hidden administrator privileges by a backdoor on the domain controller without using any domain accounts.

**NOTE**

Threat Defense for AD may not detect this dark corner if you configure a Domain Admin equivalent account.

**Potential threat**

The attacker gains full control of and access to the domain controllers of the organization.

**To mitigate**

1. Change your domain controller's DSRM password:
3. Change your current DSRM configuration to disallow this backdoor by modifying: "HKLM\System\CurrentControlSet\Control\Lsa\DSRMAdminLogonBehavior" registrykeyvalueto0or1

**Unsupported AES encryption**

The Skeleton Key attacks an in-memory patch of the domain controller security system, that enables a master password to be accepted for any domain user. This enables the attacker to impersonate and log on as any domain user with the master password the Skeleton Key creates. Therefore, he can log on with any user using just one password.

The skeleton key attacks an in-memory patch of the domain controller security system, that enables a master password to be accepted for any domain user. The attacker is able to impersonate and log on as any domain user with the master password that the skeleton key generates creates. The attacker is able to log on as any user using one password.

**Potential threat**

Using the skeleton key allows the attacker to impersonate and log on to any user, e.g. high-privileged admins, once they have compromised the Domain Controller. This attack provides hidden, unlimited, and unmonitored backdoor entry into the domain environment.

After the domain controller is compromised, the skeleton key lets the attacker to impersonate and log on to any user. This type of attack provides hidden, unlimited, and unmonitored backdoor entry into the domain environment.
To mitigate

1. Investigate the existence of a malware on the suspicious domain controller.
2. Restart the suspicious domain controller if no malware persistence is found (the skeleton key lives in-memory).
3. Consider additional logging on your domain controllers and LSA protection.


Unknown Security Provider

The attacker can add a new method of authentication after gaining high domain privileges. The attacker has complete control over the new method of authentication and can log on directly to the domain controller without domain credentials.

NOTE

Threat Defense for AD may not detect this dark corner if you configure a Domain Admin equivalent account.

Potential threat

Attackers might have created a backdoor method of authentication directly to the domain controller, bypassing any AD security.

To mitigate

1. Delete the suspicious security provider from the following registry key in the infected domain controller: HKLM\System\CurrentControlSet\Control\LSA\Security Packages
2. Investigate the domain controller for existence of malware

DC Net Session Enumeration

With this configuration, any user without privileges can enumerate sessions that are currently running on all computers connected to that domain. In a domain controller, this configuration enables an attacker to reveal users that are privileged and can connect to a domain controller.

Potential Threat

The attacker can reveal and enumerate privileged accounts in your domain.

To mitigate

1. Download Microsoft’s PowerShell Script NetCease by Microsoft, and run it on affected domain controllers.
2. Restart the Server service

Endpoint dark corners

The misconfigurations that the AD assessment scan detects in the endpoints generates the endpoint dark corner alarms.

Local Admin Traversal

Since many companies use imaging software, the local administrator password is frequently the same across the entire enterprise. An attacker stealing local administrator credentials from a local computer in the network can pass the local admin long-term key to a remote machine to authenticate itself.

The local administrator password is usually the same across the entire enterprise. An attacker with stolen admin credentials can pass the local admin long-term key to a remote machine to get authenticated access.

Potential threat

An attacker, once he obtains local admin credentials on one computer, can spread laterally and obtain access to every computer in the network with the same local admin password.
An attacker can access every computer in a network with the local admin credentials obtained on one computer in that network.

To mitigate
1. Download and install the following security update on workstations:
   https://support.microsoft.com/en-us/kb/2871997
2. Enable local admin traversal through GPO:
   ```
   windowssettings\securitysettings\localpolicies\userrightsassignment\denyaccesstothiscomputerfromthenetwork
   ```
   Add this user RID to the list:
   ```
   "*S-1-5-113"
   ```
   This RID represents every local user account in a Windows station.

Saved Sensitive Credentials

Saved credentials with high privileged groups were found in one of your endpoints. The credentials are "secured" and managed in the Local Credentials Manager, but they're actually exposed easily with any Credentials Theft Software such as Mimikatz and WCE. Those credentials are persistent and saved even after restart.

In this attack, saved credentials along with high privileged groups are found in one of your endpoints. Credentials are secured and managed in the Local Credentials Manager, but can be easily exposed by credentials theft software like Mimikatz and WCE. The credentials are persistent and are saved even after a restart.

Potential threat

Attackers can easily access these sensitive credentials once they've compromised endpoints containing the saved credentials. This dark corner alerts only if the saved credentials contain high privileges.

Attackers can easily access saved sensitive credentials on an endpoint, after compromising that endpoint. This dark corner alert generates only when the saved credentials contain high privileges.

To mitigate
1. Define "Network Access: Do not allow storage of passwords and credentials"; GPO Policy as "Disabled".
   Set Network Access as Do not allow storage of passwords and credentials. Disable the GPO Policy.
2. Remove the saved sensitive credentials from the credentials manager manually.

Unconstrained Delegation

Computer accounts with unconstrained delegation force users, who request services to that computer, to present their TGT instead of TGS to support single sign-on to specific services. Enabling sensitive accounts to connect to computers with unconstrained delegation allows attackers to steal their TGT and abuse their high-privileged permissions for malicious activity.

When users request services to a computer account with unconstrained delegation, they are forced to present their TGT to support single sign-on to specific services. Connecting sensitive accounts to computers with unconstrained delegations allows an attacker to steal their TGT and misuse high-privileged permissions for malicious activity.

Attackers may try to lure high-privileged accounts to connect to their compromised computer with unconstrained delegation, and then steal the permissions to achieve high-privileged lateral movement in the domain environment.
To mitigate
1. Configure the computer account properties in **Delegation** tab to use the option: **Do not trust this computer for delegation**.
2. Try to investigate who may have changed the configuration.

**LLMNR Enabled**

LLMNR protocol is exposed to credentials theft and local LAN reconnaissance. Attackers grab NTLM hashes over the wire using MITM on LLMNR protocol by intercepting and faking responses of DNS multicast requests. From this point, the attacker asks for credentials from the remote station.

LLMNR protocol is exposed to credentials theft and local LAN reconnaissance. Attackers intercept and deliver fake responses of DNS multicast requests to obtain NTLM hashes over the wire using MITM on LLMNR protocol. The attacker then asks for credentials from the remote station.

**Potential threat**

Attacker might attack their segment, intercept DNS resolving requests, and perform MITM attack on the endpoints to steal sensitive credentials.

**To mitigate**

Set the **Turn Off Multicast Name Resolution** GPO policy as **Enabled**

**Vulnerable Host MS17-010**

This vulnerability in SMBv1 service can be exploited remotely with a specially crafted packet to execute a code on target server, as long it has open SMB 445 connection.

This vulnerability was leaked from the NSA's 0-day pool at 2017.

**NOTE**

Threat Defense for AD may not detect this dark corner if you configure a Domain Admin equivalent account.

**Potential Threat**

Attacker will be able to execute the code remotely on vulnerable endpoints without being authenticated, and compromise your environment.

**To mitigate**

1. **MS17-010** update addresses the vulnerability.
   - This update must be installed on all servers, workstations, and domain controller.
     - Installing MS17-012 is highly recommended as well.
   2. Alternatively, you can disable SMB v1 through your GPO Policy (Not recommended).

**Permissions**

Most dark corners can be discovered without any special domain privileges. However, the following dark corners require Domain Admin privileges.

The following dark corners may not execute if you choose to use a Domain Admin equivalent account:

- **DSRM Logon** Enabled
  - **DSRM logon Enabled**
- **Vulnerable Host MS17-010**
  - (To discover vulnerable domain controllers and not hosts.)
Vulnerable Host MS17-010
• Unknown Security Provider
  Unknown Security Provider
• Vulnerable Domain Controller MS14-068
  Vulnerable Domain Controller MS14-068
Performing test attacks in Symantec Endpoint Threat Defense for Active Directory

Testing the Threat Defense for AD environment

You can perform the following test attacks against your Threat Defense for AD protected AD environment:

- User information gathering
- Computer information gathering
- Credential theft using overpass-the-hash
- Credential theft using pass-the-hash

User information gathering

This alert is triggered when a fake user account is used within the mask. These fake user accounts generate when reconnaissance commands are run on protected endpoints. The accounts are created in the groups that contain privileged users, such as Domain Administrators.

This type of attack often occurs in Advanced Persistent Threat scenarios. The attacker tries to detect and steal a high-privileged user by attempting to move laterally in the victim’s environment. The alert occurs in the first attempt of the attacker trying to brute-force these users.

To perform the attack

1. Connect to an endpoint on which Threat Defense for AD is deployed.
2. Open CMD Shell or PowerShell.
3. Run the following command:
   ```
   Net group "domain admins" /domain or net users /domain.
   ```
4. A list of Domain Administrators and users that do no belong to your environment are displayed. Identify a deceptive Domain Administrator or user. Compare and detect the fake accounts from the results with an endpoint on which Threat Defense for AD is not deployed.
5. Run any lateral movement commands with the fake user and any password:
   a. Runas /u: DomainName.com\FakeUser notepad.exe
   b. Net use z:\Your_DC_Name\C$ /user: DomainName.com\FakeUser password
6. A few moments after running the lateral movement commands, an alert is listed under Alarms > Inbox.

Computer information gathering

This alert is triggered when Threat Defense for AD detects a movement attempt towards one of the fake computers or servers. Reconnaissance commands performed on a protected endpoint results in the generation of fake computers or servers.

This attack often occurs in Advanced Persistent Threat scenarios. The attacker tries to detect high-valued endpoints or servers in the domain to move laterally in the victim’s environment and attempt to attack endpoints or servers. The alert is triggered in the attacker’s first attempt to move laterally towards one of those fake targets.
To perform the attack

1. Connect to an endpoint on which Threat Defense for AD is deployed.
2. Open CMD Shell or PowerShell.
3. Run the following command:
   ```
   Net group "domain Computers" /domain
   ```
4. A list of computers and servers that do not belong in your environment are displayed. Identify a deceptive computer or server. Compare and detect the fake computers from the results with an endpoint on which Threat Defense for AD is not deployed.
5. Run any lateral movement commands with the fake computer: (Red color indicates the fake deception computer – “c2-info”).
   a. `dir \FakeComputer\c$`
   b. `Net use Z: \ FakeComputer \c$
   c. `Psexec \ FakeComputer -s cmd`
6. A few moments after running the lateral movement commands, an alert is listed under Alarms > Inbox.

**Credential theft using overpass-the-hash**

This alert is triggered when Threat Defense for AD detects an attempt to steal and use a deceptive user account that is injected into the memory of the protected endpoints. Credentials theft tools such as WCE and Mimikatz expose credentials of these deceptive user accounts. These user accounts appear to have Domain Admin privileges, tricking the attacker into thinking they are legitimate when the attacker runs reconnaissance commands on them.

This attack often occurs in Advanced Persistent Threat scenarios. The attacker tries to steal high-privileged user accounts to escalate privileges to move laterally in the victim’s environment. The alert is generated in the first attempt to compromise one of high privileged users.

To perform the attack

1. Connect to an endpoint on which Threat Defense for AD is deployed.
2. Open PowerShell with administrator privileges.
3. Run the following command:
   ```powershell
   ```
4. You can see all the credentials that are stored in the memory. Copy the password of the injected deception user. Use this user credentials in the deception policy.
5. Perform any lateral movement command with the fake user name and password:
   a. `Run as /u: DomainName.com\FakeAdmin cmd.exe`
   b. `Net use z:\YOUR_DC_NAME\C$/User:DomainName. com\FakeAdmin password.`
6. A few moments after running the lateral movement commands, an alert is listed under **Alarms > Inbox**.

### Credential theft using pass-the-hash

This alert is triggered when the Threat Defense for AD detects an attempt to steal and use one of the deceptive user accounts that are injected into the memory of the protected endpoints (within lsass.exe). Credentials theft tools such as WCE and Mimikatz expose the credentials of these deceptive user accounts. These user accounts appear to have Domain Admin privileges, tricking the attacker into thinking they are legitimate when the attacker runs reconnaissance commands on them.

This attack often occurs in Advanced Persistent Threat scenarios. The attacker tries to steal high-privileged user accounts to escalate privileges to move laterally in the victim’s environment. The alert occurs in the first attempt to compromise one of those users.

**To perform the attack**

1. Connect to an endpoint where Threat Defense for AD is deployed.
2. Open Mimikatz with Administrator Privileges.  
   
   [GitHub repository link](https://github.com/gentilkiwi/mimikatz/releases)
3. Run the following commands:
   a. `Privilege::debug`
   b. `Sekurlsa::logonpasswords`
4. Copy the NTLM hash of the injected deception user that you chose in your deception policy.
5. Run the following command with your relevant parameters:
   
   `sekurlsa::pth /user:FakeAdmin /ntlm:YourNTLMHashValue /domain:YourDomain.com`
6. A new CMD shell opens after running the commands in Step 5. To perform a lateral movement using the NTLM hash (AKA pass-the-hash), an IP address should be used instead of the DNS name.

   For example: `DIR \192.168.1.1\c$`
7. A few moments after running the lateral movement commands, an alert is listed under **Alarms > Inbox**.
Troubleshooting Symantec Endpoint Threat Defense for Active Directory

Troubleshooting Threat Defense for AD

The deployment of Threat Defense for AD is straightforward. However, sometimes you may have issues. Here are several categories to refer to if you have issues. Contact anytime you need assistance. Broadcom Support

If you require assistance from the Broadcom Support team, collect the logs.

To collect logs

Issues with log collection and event subscription in Threat Defense for AD

Issues with Log Collection

You could face issues with log collection for the following reasons:

• You may have a connectivity issue and so, RPC is unavailable.
• The host may have the firewall on. Check the firewall settings on the host endpoint.

To confirm that the host endpoint or the AD is configured correctly
1. Go to the Core Server and select Event Viewer.
2. In the left pane, right-click on Event Viewer and select Connect to another endpoint from the list.
3. The **Select Computer** dialog box is displayed. Browse to the "Domain controller". Check the **Connect as another user** box.

4. Press the **Set User** option. Enter the credentials of the "Deployment Manager" Account.

5. Press **OK**.

When this works, you can see the domain controller that is listed at the top of the **Event Viewer** dialog box. You can also verify that the correct event IDs are generated:

- 4624 - A new Kerberos ticket created.
- 4768 - A Kerberos authentication ticket (Ticket Generating Ticket) was requested.
- 4769 - A Kerberos service ticket (Ticket Granting Service) was requested.
- 4771 - Kerberos pre-authentication failed.
- 4776 – NTLM events.

![Event Viewer Dialog Box](image)

**Trouble with event subscription**

When the infrastructure is concerned, verify that a subscription is set correctly. To verify, do the following:

- Enable **winrm** on the Threat Defense for AD server and all of the domain controllers - (winrm qc).
- Enable **Windows Event Collector** on the Threat Defense for AD and on all of the domain controllers (wecutil qc).
- Network Service should have the right to **Manage auditing and security log** on all of the domain controllers.
- Network Service and the account that you inserted at the log collection definition in Threat Defense for AD console should be members of the Event Log Readers group.
- Allow access from the Threat Defense for AD server to all of the DCs at ports: 5986, 5985.
- After verifying, restart the Threat Defense for AD server.

If there is a problem getting the logs from one of the domain controllers:

- On the problematic domain controller, verify:
  - The key: HKLM/SYSTEM/CurrentControlSet/Services/EventLog/Security Value: CustomSD
  - Contains the following:
    - (A;;0x1;;;NS)
    - Or
    - (A;;0x1;;;S-1-5-20)
- If not, you should add them manually and it should be done on all of the problematic domain controllers:
  - Open cmd:
    - `wevtutil gl security`
Copy the security descriptor to a new text document. The descriptor should be similar to the following:

O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)

Add the following string to the security descriptor:

(A;;0x1;;;S-1-5-20)

It should now be similar to this:

O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)(A;;0x1;;;S-1-5-20)

To apply the new security descriptor, run the following command. Make sure to use the security descriptor that you previously created:

wevtutil sl security /ca:O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)(A;;0x1;;;S-1-5-20)

Issues with the Threat Defense for AD Core server

Core Server installation failure

A Core server installation failure usually occurs when the minimum specifications are not correctly followed.

Refer to the Prerequisites chapter of Symantec Endpoint Threat Defense for Active Directory Installation Guide.

Prerequisites for installing Threat Defense for AD

The residual files from other products that are removed from the image may cause issues when installing the Core server.

• To find the cause of the failure, refer to "Symantec_install.log" file.
• The install log is located in "\Users\$username$\appdata\local\temp".
  $username$ is the actual user who is logged on Threat Defense for AD.
  Send this log to Symantec if you cannot find the issue.

If you find a problem with a specific component:

• Run that component from a command line: "C:\Users\$username$\AppData\Local\Temp\Core\$component$.msi".
  $username$ is the actual user who is logged on Threat Defense for AD.
  $component$ is the name of the component that failed in the file.
  Send a screen shot of the command-line window to the https://support.symantec.com/us/en/contact-us.html if you cannot find the issue.

Core Server configuration failure

The following failures usually occur when the minimum specifications are not correctly followed.

Refer to the Prerequisites chapter of Symantec Endpoint Threat Defense for Active Directory Installation Guide.

Prerequisites for installing Threat Defense for AD

Deployment Manager configuration failure:

• There may be an issue with the password of the Deployment Manager account. Reset the domain password of the Deployment Manager account, without the unusual characters, and re-enter the password in the console.

Adding a deceptive account fails:

• There may be an issue with the password of the deception account. Reset the domain password of the deception account, without the unusual characters, and re-enter the password in the console.
• Make sure that the account is not locked.
• The account properties should not have User must change password at next login checked.

Alarms do not generate:
• Navigate to the Analytics icon > specific "Deployment Manager" tab and check the settings.
• You should see a lower number under Seconds Since Received. These are listed per domain controller and per Event ID.
• If you see some event IDs with NA, then you may have an issue with your Domain Controller Domain Audit Policy.
• If you do not see any event IDs with a lower number, you may have an issue with log collection.

**Troubleshooting connectivity issues of a Deployment Manager**

An endpoint is listed under the No Connectivity tab when the Deployment Manager is unable to communicate with the endpoint.

The possible resolutions are:

• Make sure that the endpoint is online.
• Make sure that a network route is available.
• Make sure that correct firewall rules are in place if a network firewall is between the Deployment Manager and the endpoint.
• Make sure that the endpoint firewall is on. If so, apply the correct firewall rules locally or through a GPO.
• If the connection is through a VPN, check firewall rules of the VPN client.

**Table 24: Firewall rules of the VPN client**

<table>
<thead>
<tr>
<th>Access Type</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal or VPN</td>
<td>Core</td>
<td>Endpoint</td>
<td>445 (SMB), 135-139 (RPC)</td>
</tr>
</tbody>
</table>

Also, try to map a drive to the administrator share “C$” on the target host using the run as command with the “Deployment Manager” Account, which must be successful to deploy the Memory Manipulation.

Failed: Partial success is usually an issue with the <Deception Account>. Possibly another Domain Admin user made a change to the account or there is a replication issue with the account.

Refer to the Prerequisites Checklist chapter in the Symantec Endpoint Threat Defense for Active Directory Installation Guide.

To confirm Memory Manipulation is deployed successfully, RDP to the target host. Launch a command prompt and type: net group /domain “domain admins”.

You should see the actual Domain Admins that are obfuscated by 6x false accounts. This is one example of the mask that Memory Manipulation deploys and is a deception. To see real accounts, connect to a domain controller and execute the same command. You can also perform test attacks on your Symantec Endpoint Threat Defense for Active Directory protected AD environment.
Issues with sites and Memory Manipulation deployment in Threat Defense for AD

Errors under AD Sites Issues

Navigate to the Analytics > Core > AD Sites Issues section in the console. If any of the following listed errors is displayed, the Core server experiences a failure.

- **userNotExistDcs** - The deceptive user does not exist on the domain controller.
- **userDisabledDcs** - The deceptive user is disabled on the domain controller, Deployment Manager service account cannot enable it.
- **userLockedDcs** - The deceptive user is locked on the domain controller, Deployment Manager service account cannot unlock it.
- **faildResetPasswordIssue** - Reset password of the deceptive account is not working - could be password complexity not met or Deployment Manager service account does not have permission to reset the deceptive account password.
- **connectivityIssue** - The Core server cannot reach the domain controller.

RODC (Read-only Domain Controller) issues:

- **User replication issues** - Deceptive account does not replicate to the RODC.
- **Server connectivity issues** - Core server cannot reach out the RODC to replicate deceptive account.

Memory Manipulation Deployment

The following deployment failures usually occur when the minimum specifications are not correctly followed:

Deployment Fails - No connectivity:

- Check the ports, there may be a routing issue or local firewall issue.
- Try to map a drive to the admin share “C$” on the target host using the `runas` command with the “Deployment Manager” Account. This must be successful for us to deploy the Memory Manipulation.

Deployment Fails – Partial Success:

- There may be an issue with the credentials of the deception account.
  Sometimes, this message is displayed if there is a replication issue in the AD, or if the replication has not occurred since the account was created or the password changed.

Refer to the Prerequisites Checklist chapter in the Symantec Endpoint Threat Defense for Active Directory Installation Guide.
Replacing web server SSL Certificate

If you receive a web browser error, you need to replace the SSL certificate on the Core web browser. You can update the web server console with your own SSL certificate or key, that removes SSL warnings in the web browser. Contact Broadcom Support for assistance.

To replace SSL certificate or key for the console

1. On the Core server, launch Control Panel > System and Security > Administration Tools > Services. Right Click on Javelin Apache and press the Stop option.
2. Open Windows File Explorer. Navigate to C:\Program Files\Symantec\Threat Defense for AD.
3. In this window, replace these 2 files: device.key and device.crt with the new certificates.
5. Access the https://localhost/ui through a web browser. You should not receive a warning.

Updating Java

Symantec Endpoint Threat Defense for Active Directory by default manages the Java version. If you want to upgrade the Java version manually, or use an automation method, you can configure the Tomcat application where the new instance of Java is located. Contact Broadcom Support if you have any questions.

To update the Java version

1. Open Windows Explorer. Right click on This PC > Properties.
2. Press Advanced System Settings.
3. Press Environment Variables.
5. Enter the new location to Java for "Variable Value".
6. Press Ok on the next three windows.
7. Launch Control Panel > Local Services.
8. Restart Apache Tomcat and Symantec Apache services
Frequently Asked Questions (FAQ) in Symantec Endpoint Threat Defense for Active Directory

Frequently Asked Questions about the Threat Defense for AD Forensics

How do the forensics work?

The forensics run after an Threat Defense for AD alarm is triggered on the attacked endpoint. After detection, a named pipe process installs remotely and receives instructions from the Deployment Manager servers about the items to export from the compromised workstation. The actual processing of the data occurs on the Deployment Manager.

Here's the process of how the forensics are collected:

• After the host receives an alert, the Deployment Manager copies the remote forensics agent (raXXX.exe, XXX is the version of the .NET framework) over Server Message Block (SMB).
• Then, the Deployment Manager starts up the remote agent by creating a service remotely by SMB.
• The service opens a named pipe and listens to this named pipe.
• The Deployment Manager communicates and tells the items to collect to this named pipe remotely using SMB.
• The host locally executes name resolution to translate addresses of the current network connections.
• The results of the collections are also saved in the named pipe and the Deployment Manager collects them.
• The named pipe is encrypted with DHEC.

What's the purpose of forensics and how is it different from another forensics software?

Forensics are oriented to detect post breach AD attacks, focusing on detecting the actual Reconnaissance, Credential Theft, and Lateral Movement phases performed by an attacker. Forensics help identify the malware that is involved in the attack, and the other items on the infected workstation that could have been involved in the attack.

How quickly do I get the forensics report back after launching it?

You receive the forensics report within one to five minutes, depending on environment latency, local resources, and the amount of data to process.

Can forensics recover lost and deleted files from the hard drive?

No, it only analyzes the metadata of the workstation. We do not process the entire hard drive.

How does forensics perform memory analysis?

From the forensics report we already know the following:

• The attack method attempted on an endpoint.
• The fake object the attacker attempted to interact with.
• If a fake endpoint or a fake credential was used to interact.

The infected workstation memory is analyzed and any process that contains our fake data is retrieved. Apart from that, memory analysis uses the YARA project to analyze the endpoint's memory, the open-sourced project PE-sieve, and many more actual rules that we have developed to detect any indicators of compromise.